UNIVERSITÀ
DEGLI STUDI
FIRENZE

University of Florence
Department of Industrial Engineering (DIEF)
Curriculum: Industrial and Reliability Engineering

A thesis presented for the degree of Doctor of Philosophy

The Importance Of Human Factor And Maintenance Activities In Risk Assessment For Railway Applications

Candidate:
Dr. Giulia Guidi

Supervisors:
Prof. Marcantonio Catelani
Prof. Lorenzo Ciani

PhD Coordinator:
Prof. Giampaolo Manfrida

Academic Discipline : ING - INF/07

Cycle XXXIV Years: 2018-2022

University of Florence, Department of Industrial Engineering (DIEF)

Thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Industrial Engineering.

A mio babbo, che mi ha sempre
insegnato che a fare l'ingegnere ci
deve andare chi non sa fare altro

Acknowledgements

Mi è doveroso dedicare questo spazio del mio elaborato alle persone che hanno contribuito, con il loro instancabile supporto, alla realizzazione di questo lavoro.

In primis, un ringraziamento speciale ai miei supervisors Marcantonio Catelani e Lorenzo Ciani, per la loro immensa pazienza, per gli indispensabili consigli, per le conoscenze trasmesse durante tutto il lavoro di ricerca.

Vorrei ringraziare la mia famiglia per la vicinanza ed il supporto che mi hanno dato. In particolare, spero che i miei genitori siano orgogliosi di questo mio traguardo che segna l'inizio di un nuovo percorso lavorativo.

Ringrazio tutti/e quelli/e che con un sorriso, una risata o un piccolo gesto mi ha sostenuto in questi ultimi tre anni, soprattutto nei momenti di sconforto e mi ha permesso di essere qui adesso.

Ringrazio infinitamente Gabriele, per aver condiviso con me tutto questo lungo percorso che ci ha condotto insieme a questa nuova meta. Lo ringrazio per essere stato sempre al mio fianco, pronto ad aiutarmi in qualsiasi cosa e a rendere più leggeri anni di studi e giornate al computer.

CONTENTS

Contents vii

Abstract xi

List of Figures xiii

List of Tables xix

Abbreviations & Acronyms xxi

Reliability and Maintenance in Railway engineering 1

1.1 RAILWAY STANDARDS 2

1.2 OBJECTIVE OF THE WORK 7

1.3 CASE STUDIES 11

1.3.1 HEATING VENTILATION AND AIR CONDITIONING 12

1.3.2 RAILWAY SIGNALLING SYSTEM 21

1.4 LIST OF MAJOR CONTRIBUTIONS 34

Fuzzy Theory for Reliability analysis 39

2.1 INTRODUCTION 40

2.2 FUZZY THEORY 41

2.2.1 BRIEF OVERVIEW 42

2.2.2 FUZZY SETS AND MEMBERSHIP FUNCTIONS 43

2.2.3 OPERATIONS BETWEEN FUZZY NUMBERS 47

2.2.4 DEFUZZIFICATION 48

2.3 FUZZY INFERENCE SYSTEMS 48

Risk based maintenance 55
3.1 INTRODUCTION 56
3.2 RELIABILITY CENTERED MAINTENANCE 57
3.3 RELATED WORKS ABOUT RCM 59
3.4 FUZZY-BASED RCM: THE PROPOSED APPROACH 60
3.5 CASE STUDY: RCM ASSESSMENT OF HVAC FOR HIGH-SPEED TRAINS 66
3.6 FROM FUZZY RCM TO FUZZY FMECA 73
3.7 BRIEF OVERVIEW OF FMECA 74
3.8 STATE OF THE ART OF FMECA 75
3.9 PROPOSED FUZZY FMECA APPROACH 78
3.10 CASE STUDY: FUZZY FMECA OF RAILWAY SIGNALING SYSTEM 86
3.11 FINAL REMARKS ON FUZZY FMECA 92
3.12 LAST PROBLEM OF FMECA: THRESHOLD ESTIMATION 93
3.13 A NEW APPROACH FOR THE THRESHOLD ESTIMATION 96
3.13.1 DESCRIPTION OF THE PROCEDURE 96
3.13.2 PRELIMINAR RISK ANALYSIS OF HVAC 99
3.13.3 CASE STUDY 1: HVAC PASSENGER UNIT 104
3.13.4 CASE STUDY 2: HVAC CABIN UNIT 107
3.13.5 STATE OF THE ART COMPARISON 108
3.14 FINAL REMARKS 110

Human Factor in Railway Engineering 111
4.1 HUMAN RELIABILITY: WHAT AND WHY? 112
4.1.1 HUMAN ERROR CLASSIFICATION 113
4.2 HUMAN RELIABILITY ANALYSIS TECHNIQUES 117
4.2.1 FIRST GENERATION TECHNIQUES 118
4.2.2 SECOND GENERATION TECHNIQUES 120
4.2.3 NEW STUDIES AND THIRD GENERATION TECHNIQUES 122
4.3 NEEDS FOR HUMAN RELIABILITY ANALYSIS IN RAILWAY ENGINEERING. 125
4.4 SYSTEMATIC REVIEW OF THE LAST TWO DECADES 126
4.4.1 SEARCH METHODOLOGY 127
4.4.2 BIBLIOMETRIC ANALYSIS 130
4.4.3 MOST SIGNIFICANT DOCUMENT 138
4.5 RAILWAY ACTION RELIABILITY ASSESSMENT 150

4.6 Final remarks 155

Proposed improvements in HRA for railway 157

5.1 Introduction 158

5.2 Review of fuzzy methods for HRA 159

5.3 First proposed method: fuzzy-based approach 160

5.4 Validation of the proposed method 176

5.4.1 Human activities performed on ATP 176

5.4.2 Human error probability estimation 177

5.4.3 Comparison with the classical RARA approach 181

5.5 Final remarks 183

Dynamic HRA: An innovative approach for railway industry 185

6.1. Second proposed method: Enhanced-SHERPA (E-SHERPA) 186

6.2. Structure of the proposed E-SHERPA 188

6.2.1 Nominal HEP 188

6.2.2 Contextual HEP 192

6.2.3 Application of the Yerkes-Dodson Law to Stress PSF 195

6.2.4 Introduction of breaks 198

6.3. Validation of the proposed E-SHERPA 203

6.3.1 Railway Track Maintenance Operation 206

6.3.2 Human error probability estimation 208

6.3.3 Validation with empirical data 213

6.4. Final Remarks 215

Conclusions 217

Reference 221

Annex A 243

List of original Publication 245

Abstract

This thesis focuses on the importance of human factor and maintenance activities in risk assessment for railway applications.

Risk based maintenance is a key factor of RAMS (Reliability, Availability, Maintainability and Safety) for railway. One of the widest used techniques to evaluate the optimal maintenance policy of complex systems is the RCM (Reliability Centred Maintenance). This procedure starts from a failure analysis before individuating the optimal maintenance operation focusing on a decision diagram which is very vague and subjective. Trying to solve this problem, the first part of this work introduces an innovative approach that proposes a new decision-making diagram. The new diagram is based on a fuzzy-FMECA (Failure Modes, Effects and Criticality Analysis) assessment combined with some Boolean variables in order to provide a unique maintenance task for every identified scenario depending on the O (Occurrence), S (Severity) and D (Detection) assessment. The proposed procedure provides a diagnostic-oriented decision diagram able to solve the problems of the standardized RCM procedure and, at the same time, to optimize the Operation&Maintenance cost and the system availability favoring CBM (Condition-Based Maintenance) tasks such as Condition Monitoring and Failure Finding procedures.

The proposed enhanced RCM is based on a FMECA, which is a central technique used to perform risk assessment in every industrial and technological field. Despite this, several papers in literature agree that classical FMECA suffer many drawbacks. The developed fuzzy FMECA technique aims to solve all these problems with a simple and effective tool that could be applied in railway applications. Moreover, an innovative risk threshold estimation method has been developed to divide critical and negligible modes after the FMECA assessment in order to prioritize countermeasures.

The second topic covered by this research is the analysis of human reliability in railway engineering. Human factors remarkably contribute to railway accidents and, as a matter of fact, it is one of the main causes of accident on the last years. This is the reason why it is mandatory to study and evaluate human reliability in maintenance operation of railway systems. Literature is plenty of techniques developed to study the human reliability, however the only validated method for railway field is RARA (Railway Action Reliability Assessment). RARA has been developed in 2012 and is characterized by a highly subjective and complex assessment. Trying to solve these needs, this work proposes an improvement of RARA method able to solve its main shortcomings thanks to fuzzy logic. Using the proposed fuzzy-RARA the analyst is facilitated in the assessment of the numerical parameters and the subjectivity is remarkably mitigated.

Finally, the last part of the work presents an innovative technique specifically developed for railway. This method integrates the Weibull distribution and aims to provide a time-dependent model for the Human Error Probability. Furthermore, the proposed method gave the possibility to select one or more variable breaks within the work shift, which is an aspect generally neglected by the state-of-the art.

Both the proposed methods for Human Reliability Analysis have been tested on the maintenance activities performed by qualified operators nearby the railroad. The results highlight the significant contributions of the human error within the contexts of the complete risk assessment of the railway system.

LIST OF FIGURES

Fig. 1. 1 - Factors influencing Railway RAMS 3

Fig. 1. 2 - Trend of the percentage of accident due to human factors..........................9

Fig. 1. 3 - Research objectives and summary of the work..11

Fig. 1. 4 – Main components of the whole HVAC system 14

Fig. 1. 5– Compressor...15

Fig. 1. 6– Heat exchanger..18

Fig. 1. 7 - Schematic of signal block section. When a block is unoccupied, the signal protecting it will show green. If a block is occupied, the signal protecting it will show red...22

Fig. 1. 8 - Schematic of 3-aspect signalled route showing the additional yellow aspect provided to allow earlier warnings and thus higher speed operation..........................23

Fig. 1. 9 - Schematic drawing of track circuit for unoccupied and occupied block. 25

Fig. 1. 10 - Schematic drawing of axle counters positioning along the track..............27

Fig. 1. 11 - Schematic drawing of an interlocking system..29

Fig. 1. 12 - ATP eqipment. Source: www.railwaysignallingconcepts.in 31

Fig. 1. 13 - Speed curve required to reach the target limit at the signal....................32

Fig. 1. 14 - Scheme of the Automatic Train protection under test highlighting the devices of the ground subunit (Two balises, an encoder and a semaphoric unit). 33

Fig. 2. 1 - Graphical comparison between Boolean logic (on the top side) and Fuzzy logic (on the bottom side)..43

Fig. 2. 2 - Height membership functions for a crisp set A (left plot) and a fuzzy set H (right plot). 45

Fig. 2. 3 - Example of triangular membership function. 46

Fig. 2. 4 - Example of trapezoidal membership function..47

Fig. 2. 5 - Example of membership functions for Severity.. 49

Fig. 2. 6 -Example of membership functions for Detection.. 50

Fig. 2. 7 - Example of membership functions for occurrence..................................... 50

Fig. 2. 8 -Example of membership functions for the RPN.. 51

Fig. 2. 9 -Block diagram of the inference system. 51

Fig. 2. 10 - Application of the implication method. 53

Fig. 2. 11 -Aggregation of the results in a fuzzy if-then inference system.................. 53

Fig. 3. 1 - Maintenance decision-diagram of classical RCM procedure according to International standard IEC 60300-3-11.. 58

Fig. 3. 2 - Membership functions for occurrence O: "Remote (R)", "Probable (P)", "High (H)". 61

Fig. 3. 3- Membership functions for severity S: "Very Low (VL)", "Tolerable (T)", "Critical (C)".. 61

Fig. 3. 4- Membership functions for detection D: "Almost Certain (AC)", "Medium (M)" and "Absolutely Uncertain (AU)". 62

Fig. 3. 5 - Proposed maintenance decision-diagram to assess optimal maintenance task using fuzzy logic.. 63

Fig. 3. 6 - Schematic diagram of fuzzy-based RCM assessment using "if-then" rules. 65

Fig. 3. 7- Summary of result achieved applying the proposed maintenance decision-diagram to the complete HVAC system under analysis. (a) Overall results of the proposed Fuzzy-based RCM procedure. (b) Comparison between diagnostic-based maintenance, scheduled maintenance, and corrective maintenance. 71

Fig. 3. 8 - Example of membership function of a generic trapezoidal fuzzy number A_{TRAP} = (a, b, c, d).. 78

Fig. 3. 9 - Example of membership function of a generic triangular fuzzy number A_{TRI} = (a, b, c)... 79

Fig. 3. 10 - Set of five triangular membership functions and their relative linguistic variables selected for each one of the FMECA influence factors. Occurrence is illustrated in a), while Severity is illustrated in b) and Detection is illustrated in c)................. 81

Fig. 3. 11 - Set of three trapezoidal membership functions and their relative linguistic variable used to assess the proper weight of Occurrence, Severity and Detection....... 82

Fig. 3. 12 - Flowchart of the proposed fuzzy-based tool highlighting every step of the procedure. The loop inside the light red box must be repeated for each one of the failure modes. 84

Fig. 3. 13 - Set of all the 125 possible membership functions for the Fuzzy Risk Priority Number in case of the following weights are set: $\omega O = \{'High'\}$, $\omega S = \{'Very\ high\ '\}$ and $\omega D = \{'High'\}$. The different colors stand for a different FRPN achieved using a different combination of the O, S and D. 85

Fig. 3. 14 - Fuzzy Risk Priority Number FRPN (continuous trends) and defuzzified $RPN*$ (dotted lines) obtained using two similar combinations of O, S and D. A small change in occurrence results in a small change in the risk priority number (both fuzzy FRPN and defuzzified $RPN*$). 86

Fig. 3. 15 - Classification of failure effects for the receiver board under test. The top level refers to the local effects, while the bottom level refers to the global effects, divided in detected and undetected. 87

Fig. 3. 16 - Screenshot of the MATLAB Graphical User Interface developed to rapidly implement the proposed fuzzy-based RPN estimation. 89

Fig. 3. 17 - Membership functions of the Fuzzy Risk Priority Number related to the seventeen identified failure mode in case of the same weights for O, S and D are set, as $\omega O = \omega S = \ \omega D = \{'High'\}$........ 90

Fig. 3. 18 - Results of the proposed fuzzy-based procedure. RPNs* are obtained setting the same weights for O, S and D. Three different scenarios are considered: $\omega O = \omega S = \omega D = \{'Medium'\}$ (blue bars), $\omega O = \omega S = \omega D = \{'High'\}$ (red bars) and $\omega O = \omega S = \omega D = \{'Very\ high'\}$ (yellow bars)........ 91

Fig. 3. 19 - Results of the proposed fuzzy-based procedure. The defuzzified RPNs* are obtained using two different scenarios: same weights of the parameters $\omega O = \omega S = \omega D = \{'High'\}$ (red bars) and different weights in order to prioritize the severity $\omega O = \omega D = \{'High'\}$ while $\omega S = \{'Very\ high'\}$ (grey bars). 92

Fig. 3. 20 - Flowchart of the new procedure for Risk Priority Number threshold estimation........ 96

Fig. 3. 21 - Examples of HVAC units located on a high-speed train........ 99

Fig. 3. 22- Block Diagram of HVAC under study........ 100

Fig. 3. 23- Representation of the whole “Passenger unit” FMECA result. All the RPNs are plotted ordered by size........ 104

Fig. 3. 24 - Step 1: repetition number of each RPN value. 105

Fig. 3. 25 - Application of the proposed procedure to the “Passenger unit” of the HVAC. The top plot illustrates the steps from 2 to 5 of the procedure, while the bottom plot is used to carry out the final step. 105

Fig. 3. 26 - Division of Risk Priority Numbers identified in the “Passenger unit” FMECA in negligible and critical values. 106

Fig. 3. 27 - Application of the proposed procedure to the “Cabin unit” of the HVAC. The top plot illustrates the steps from 2 to 5 of the procedure, while the bottom plot is used to carry out the final step. 107

Fig. 3. 28 - Division of Risk Priority Numbers identified in the “Cabin unit” FMECA in negligible and critical values..108

Fig. 4. 1 - Error classification based on Reason-Rasmussen theory. 115

Fig. 4. 2 - Schematization of search methodology using AND/OR logic gates. The grey boxes indicate the search keys..128

Fig. 4. 3- Literature review process for the analysis of HRA in railway. 129

Fig. 4. 4- Comparison of type of documents after the second screening phase. The total amount of documents is 755..131

Fig. 4. 5- Trend of published papers in HRA for railway engineering considering the last two decades..131

Fig. 4. 6- Number of total citations (blue dots) and number of citations excluding self-citations (red dots) of the 268 identified research articles..132

Fig. 4. 7 - Cloud word of the keyword co-occurrence in the analyzed research papers. 133

Fig. 4. 8- Qualitative evaluation of the geo-localization of published papers in the research topic under analysis..134

Fig. 4. 9- Detailed estimation of the country-by-country number of published papers about HRA for railway applications..134

Fig. 4. 10 - Detail of the bibliometric analysis regarding the affiliations of the authors. Only affiliations with at least 4 published papers have been considered...................135

Fig. 4. 11 - Comparison of the number of published papers divided per journal source. 138

Fig. 4. 12- HEP trend in the RARA technique..154

Fig. 5. 1- Flowchart of the proposed Fuzzy-based approach used to estimate the human error probability in railway engineering..161

Fig. 5. 2- Membership functions proposed to estimate the HEP of each Generic Task Type (GTT) included in the procedure. 164

Fig. 5. 3 - Example of a generic trapezoidal membership function. 166

Fig. 5. 4- MATLAB Graphical User Interface developed to rapidly implement the proposed HRA approach. The screenshot represents the dialog box for data entry. . 171

Fig. 5. 5- Screenshot of the proposed GUI after the selection of GTT and EPC. The input data are collected inside the right panel. The charts show the selected task and the last chosen EPC. 172

Fig. 5. 6- Output box of the developed MATALB Graphical User Interface. The software provides the fuzzy HEP and the defuzzification result, along with a note with the selected membership functions used to evaluate the HEP. 175

Fig. 5. 7- Results of the proposed approach. Fuzzy Human Error Probability and Defuzzified HEP in two different scenarios (Optimal case in blue and Stressed and Fatigued in red). Each plot illustrates the results of a different activity. 179

Fig. 5. 8- Bar chart of the defuzzified HEP* obtained using the proposed approach considering four different tasks and two simulation scenarios (1. Optimal case using blue and 2. Stressed and Fatigued using red). 180

Fig. 6. 1-Nominal HEP calculated as a Weibull function using equation (6.1) for each of the GTT. 191

Fig. 6. 2 - Yerkes-Dodson model describing the relationship between performance and stress. The intermediate part is the Eustress or beneficial stress. 196

Fig. 6. 3 Multiplier of the stress PSF considering the Y-D law. The PSF levels (blue bars) are compared to the Y-D stress-performance curve. 196

Fig. 6. 4 - 3-D trend of the contextual HEP of GTT R6 varying the working time and the PSF effects. Y-D law is included. 198

Fig. 6. 5 - Nominal HEP of the proposed E-SHERPA including a break in the middle of the working shift. 200

Fig. 6. 6 - Nominal HEP of the proposed E-SHERPA including two breaks within the working shift. The first break could represent a coffee break, while the second one stands for a lunch break 202

Fig. 6. 7 - Balises deployment on the railroad tie used by the SCMT to transmit information regarding the signal to the Onboard control. The distance between the balises refers to a rail track with maximum speed of 180 km/h. 204

Fig. 6. 8 - Complete “Ground subsystem” of the SCMT including an encoder and two balises. 205

Fig. 6. 9 - Proposed Graphical User Interface for the assessment of the E-SHERPA human reliability analysis. Task R6 is involved. PSF product is set equal to 10, the break starts after 4 h and the break duration is 1 h. The top subplot illustrates the nominal HEP, while the bottom subplot shows the contextual HEP achieved with the proposed E-SHERPA. 207

Fig. 6. 10 - Complete Flowchart of the balise maintenance including all the task that the operator should carry out when maintenance is required. 208

Fig. 6. 11 - Contextual HEP of the Maintenance task simulated using four different scenarios. Start time and duration of the break is set to a fixed value.....................210

Fig. 6. 12 - Contextual HEP of the Maintenance task simulated comparing SHERPA (top subplot) and E-SHERPA (bottom subplot) methods. A one-hour long break has been set in the E-SHERPA model..211

Fig. 6. 13 - Contextual HEP of the Maintenance task simulated varying the break duration (30 min – 60 min – 90 min – 120 min). Each plot shows 4 working hours before and after the break...212

Fig. 6. 14 - Contextual HEP of the Maintenance task simulated using only one long break (top subplot) or using two shorter breaks (bottom subplot). The total amount of break minutes is the same in both simulations (60 minutes) as well as the total amount of working hours (8 h)...212

Fig. 6. 15 - Contextual HEP of the Maintenance task simulated using all the possible Stress PSF proposed in Table 4 according to the Yerkes-Dodson law. 213

Fig. 6. 16 - Validation of the proposed E-SHERPA approach (top subplot) using field data regarding the human error observed during maintenance operation of railway signaling systems...214

List of Tables

Tab. 1. 1. 2019 main cause of railway accident. Source: [5]. 8

Tab. 1. 2. Technical characteristic of HVAC...14

Tab. 3. 1- Linguistic definition for Occurrence O, Severity S and Detection D used in the proposed method. 60

Tab. 3. 2 - Failure modes and effects analysis (FMEA) for an HVAC system...........67

Tab. 3. 3 - Input parameters of the proposed fuzzy-based RCM approach. The failure modes refer to the preliminary FMEA report in Table 2...69

Tab. 3. 4 - Extract of comparison between the proposed Fuzzy-based RCM and the classic RCM assessed following the guidelines of IEC 60300-3-11..............................72

Tab. 3. 5 -Assessment of the Membership functions for O, S and D. Seventeen Failure Modes have been identified during the analysis...88

Tab. 3. 6 -High-level taxonomy of the system under test 99

Tab. 3. 7- Criteria for Severity S assessment.. 100

Tab. 3. 8- Occurrence O evaluation criteria based on failure rate............................ 101

Tab. 3. 9- Detection D evaluation criteria.. 101

Tab. 3. 10 - Extract from the whole FMECA for the “Passenger unit” of the HVAC system under analysis 103

Tab. 3. 11 - Results comparison achieved using the proposed method and the other method available in literature 109

Tab. 4. 1 - State of the art of Human Reliability Analysis: summary of the main first generation techniques.. 119

Tab. 4. 2 - State of the art of Human Reliability Analysis: summary of the main second generation techniques.. 121

Tab. 4. 3 - State of the art of HRA: summary of the third generation techniques 123

Tab. 4. 4 - Most relevant authors in the field of Human Reliability for Railway Engineering since 2000. 136

Tab. 4. 5 - 10 top-cited research articles in the field of human reliability analysis for railway engineering. 137

Tab. 4. 6 - RARA Generic Task Type list....................151

Tab. 4. 7 - Error Producing Conditions list....................152

Tab. 5. 1- Generic Task Type and Human Error Probability according to RARA technique [307]. 163

Tab. 5. 2- Human Operations performed on the Ground unit of an Automatic Train Protection system. 176

Tab. 5. 3- Input data used to calculate the Human Error Probability of the four considered operations in two different scenarios. 179

Tab. 5. 4- Input Data used to calculate the Human Error Probability using the RARA method....................181

Tab. 5. 5- Comparison between Classical RARA method and Proposed Fuzzy-based Approach. 182

Tab. 6. 1–Generic Task Type and corresponding parameter values evaluated as proof included in Annex A 191

Tab. 6. 2–PSFs of the proposed method and corresponding multiplier value. Part A. Source [189]....................193

Tab. 6. 3– PSFs of the proposed method and corresponding multiplier value. Part B. Source [189]....................194

Tab. 6. 3– Performance Shaping Factors related to Stress factor integrating Yerkes-Dodson law 197

Tab. 6. 4– PSF assessed in four different simulation scenarios....................209

Abbreviations & Acronyms

ACIH	Analysis of Consequences of Human Unreliability
AHP	Analytic Hierarchy Process
AI	Artificial Intelligence
ANP	Analytic Network Process
APOA	Assessed proportion of affect
ART	Adaptive Resonance Theory
ATHEANA	A Technique for Human Error Analysis
ATP	Automatic Train Protection
BN	Bayesian Network
CART	Classification And Regression Tree
CES	Cognitive Environment Simulation
COCOM	Contextual Control Model
COSIMO	Cognitive Simulation Model
CPC	Common Performance Conditions
CREAM	Cognitive Reliability and Error Analysis Method
D	Detection
DEMATEL	DEcision-MAking Trial and Evaluation Laboratory
DMI	Driver Machine Interface
ECC	Electronic Control Card
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPC	Error Producing Condition
ERPN	Exponential Risk Priority Number
ERTMS	European Rail Traffic Management System
E-SHERPA	Enhanced Simulator for Human Error Probability Analysis
ETA	Event Tree Analysis
EVC	Enhanced Vital CPU
FANP	Fuzzy Analytic Network Process
FHIA	FMECA and HAZOP integrated Analysis
FIS	Fuzzy Inference System
FMEA	Failure Mode and Effects Analysis

FMECA	Failure Mode, Effects and Criticality Analysis
FPMK	Failures Per Million Kilometers
FRA	Federal Railroad Administration
FRPN	Fuzzy Risk Priority Number
FSK	Frequency Shift Keying
FTA	Fault Tree Analysis
GTT	Generic Task Type
GUI	Graphical User Interface
HAZOP	HAZard and OPerability analysis
HCR	Human Cognitive Reliability
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HERMES	Human Error Risk Management for Engineering Systems
HFACS	Human Factors Analysis and Classification System
HRA	Human Reliability Analysis
HuPeROI	Human Performance Railway Operational Index
HVAC	Heating Ventilation and Air Conditioning
IAQ	Indoor Air Quality
IGBT	Insulated Gate Bipolar Transistor
IRPN	Improved Risk Priority Number
LC	Level Crossing
LEU	Lineside Electronic Unit
LRU	Line Replaceable Unit
MA	Maximum Affect
MF	Membership Function
MIDAS	Man Machine Integration Design and Analysis system
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
NARA	Nuclear Action Reliability Assessment
NMI	Not Maskable Interrupt
O	Occurrence
OTDR	On Train Data Recorder
OTMR	On Train Monitoring Recorder
OTMS	On Train Monitoring System
OWGA	Ordered Weighted Geometric Averaging
PRA	Probabilistic Risk Assessment
PROCOS	Probabilistic Cognitive Simulator
PROMETHEE	Preference ranking organization method for enrichment

	evaluation
PSF	Performance Shaping Factor
PTC	Positive Train Control
QUALIFLEX	Qualitative Flexible Multiple Criteria Method
RAM	Reliability, availability and maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RANDAP	Reliability Analysis of Detailed Action Plans
RARA	Railway Action Reliability Assessment
RAV	Risk Assessment Value
RBD	Reliability Block Diagram
RCA	Root Cause Analysis
RCM	Reliability Centred Maintenance
RPN	Risk Priority Number
RPM	Revolutions Per Minute
RSSB	Rail Safety and Standards Board of UK
S	Severity
SAFPHR	Systems Analysis for Formal Pharmaceutical Human Reliability
SCMT	Italian acronym for train running control system
SHERPA	Simulator for Human Error Probability Analysis
SLIM	Success Likelihood Index Method
SPAD	Signal Passed At Danger
SPAR-H	Standardized Plant Analysis of Risk-Human Reliability Analysis
SSC	Italian acronym for supporting system for the driver
STAMP	Systems–Theoretical Accident Modelling and Processes
SYBORG	Simulation System for Behavior of an Operating group
THERP	Technique for Human Error Rate Prediction
TODIM	Portuguese acronym of interactive and multiple attribute decision making
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
UPS	Uninterruptible Power Supply
VIKOR	Serbian acronym of Multicriteria Optimization and Compromise Solution

Chapter 1

Reliability and Maintenance in Railway engineering

This chapter provides a general overview of the themes analyzed in this thesis outlining the importance of every topic. The aim of this section is to provide enough background information so that the reader can understand the context in which the research sits. More in detail, this chapter discusses the gap that this research aims to fill. The research questions are properly outlined, and the problems addressed by this study are extensively explained. The final part of the section illustrates the main contributions that this work will provide to the body of knowledge. The key element of novelties is thoroughly stressed to emphasize the importance of the thesis within the context of the RAMS disciplines in railway. The final part of the chapter briefly discusses the railway systems taken as case study in the following chapters.

1.1 Railway standards

Railway engineering is a very standardized field, in particular standard related to RAMS (Reliability, Availability, Maintainability, Safety) topic are:

- CENELEC 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process [1]
- CENELEC 50126-2 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety[2]
- CENELEC 50128 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems[3]
- CENELEC 50129 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling [4]

RAMS parameters represent a set of characteristics of a system's long-term operation achieved by the application of established engineering concepts, methods, tools and techniques throughout its life cycle. The RAMS of a system can be characterized as a qualitative and quantitative indicator of the degree that the system, or the subsystems and components comprising that system, can be relied upon to function as specified and to be both available and safe over a period of time. System RAMS is a combination of the interrelated characteristics, reliability, availability, maintainability and safety.

The goal of a railway system is to achieve a defined level of rail traffic at a given time, safely and within certain cost limits. The Railway RAMS process determines the confidence with which the system can achieve this goal. Railway RAMS has a clear influence on the quality with which the service is delivered to the customer.

The RAMS elements are interlinked in the sense that a weakness in any of them or mismanagement of conflicts between their requirements can prevent achievement of a dependable system. Attainment of in-service availability targets will be achieved by optimizing reliability & maintainability whilst considering the influence of maintaining safety. The related requirements can be met and controlled by a combination of design and implementation measures and through the ongoing, long-term maintenance and operational activities, all according to the system environment.

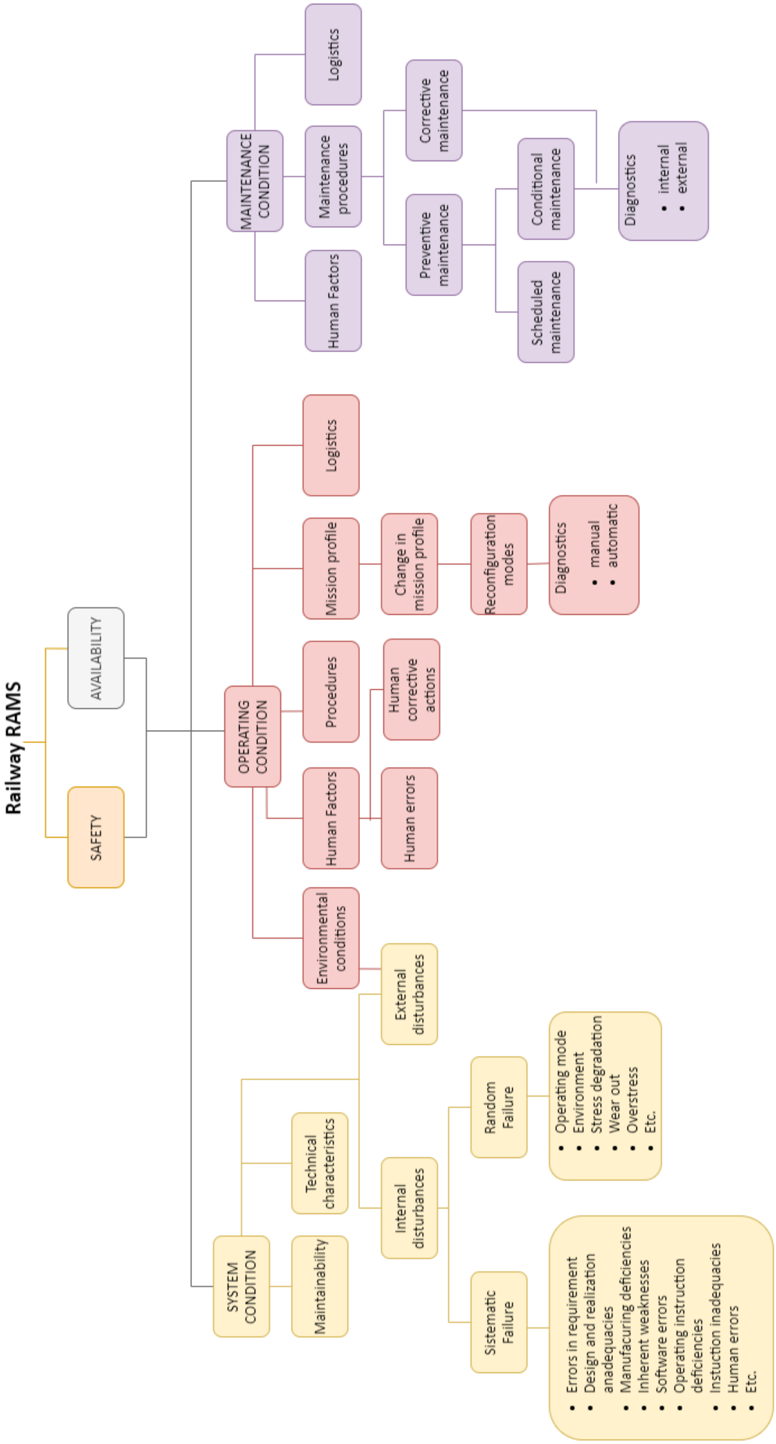


Fig. 1. 1 - Factors influencing Railway RAMS

Figure 1.1 identifies all the factors which influence the RAMS performance of railway systems, with particular consideration given to the influence of human factors. These factors, and their effects, are an input to the specification of RAMS requirements for systems.

The RAMS performances of a railway system are influenced by three conditions, that can interact with each other, as follow:

- By sources of failure introduced internally within the system at any phase of the system life cycle.
- By sources of failure imposed on the system during operation.
- By sources of failure imposed on the system during maintenance activities.

To create dependable units, factors which could influence the RAMS of the system need to be identified, their effect assessed, and the cause of these effects managed throughout the life cycle of the system, by the application of appropriate controls to optimize system performance.

Failures in a system, product or process are categorized as random failures or systematic failures:

- Random failures are due to causes which can be described by statistical distributions.
- Systematic failures are failures due to errors in the system life cycle activities which cause the product, system or process to fail deterministically under particular combinations of inputs or under particular conditions (e.g. combination of inputs or/and triggering events such as non-fulfilment of environmental or application conditions).

Systematic failures are mainly caused by human errors in the various stages of the system life cycle.

Therefore systematic failures are mainly treated by the application of appropriate processes, methods and organization. A major distinguishing feature between random failures and systematic failures is that random failures are in general due to events that can be statistically monitored so that their probability of occurrence can be estimated. Systematic failures are due to events for which statistical data is not usually available so that their probability of occurrence cannot generally be estimated.

The clear distinction between random and systematic failures might be blurred by the following observations:

- Systematic failures are reproducible, if conditions can be exactly replicated. If these conditions (the combination of input that activates them) are by themselves a random event, the occurrence of the systematic failures also exhibit a temporal random behavior by an outside point of view.
- Large fractions of failures, due to environmental conditions (e.g. temperature, moisture, humidity etc.) and external influences (EMC - Electromagnetic Compatibility, vibration), can be considered both systematic or random as well.

As can be clearly observed in Figure 1.1 Human factors are a core aspect within an integrated RAMS management process. An analysis of human factors, with respect to their effect on system RAMS, is inherent within the “systems approach” applied by railway standards.

Human factors can be defined as the impact of human characteristics, expectations and behavior upon a system. These factors include the anatomical, ergonomics, physiological and psychological aspects of humans. The concepts within human factors are used to enable people to carry out work efficiently and effectively, with due regard for human needs on issues such as health, safety and job satisfaction. Each human might react to situations in different ways, which impacts the RAMS performance.

The achievement of railway RAMS requires more rigorous control of human factors throughout the entire system life cycle, than is required in many other industrial applications.

Humans have the ability to influence the RAMS of a railway system positively or negatively. To maximize the positive influence and minimize the negative influence, the manner in which human factors can influence railway RAMS shall be identified and managed throughout the life cycle. This shall include the potential impact of human factors on railway RAMS not only within the Operation, Maintenance and Performance Monitoring phase, but also within the other phases of the system life cycle. The precise influence of human factors on RAMS is specific to the application under consideration and it can be evaluated using several techniques available in literature (both qualitative and quantitative approaches can be used).

The life cycle approach provides a structure for planning, managing, controlling and monitoring all aspects of a system, including RAMS, as the system under consideration progresses through the life cycle phases.

The focus of the RAMS process is to reduce the incidence of failures and/or the consequences throughout the life cycle, and thus minimize the residual risk resulting from these errors.

The Life cycle phases of a generic railway system can be summarized as follow:

1. Concept: remit of the project should be drawn up.
2. System definition and operational context: description of essential characteristics and functions of the system, and clarification of the interfaces to other systems including the input to be provided and the output that can be expected. On this basis the impact on RAMS parameters of neighboring systems can be derived. The intended operational conditions (maintenance, environment, etc.) that could impair the safe or good (RAM - Reliability, Availability and Maintainability) functions are stated to ensure that the operator is aware of them. The RAMS management is established, including a RAM plan and a Safety plan.
3. Risk analysis and evaluation: several steps (e.g. for safety: identify hazards associated with the system, identify events leading to hazards, determine risk associated with hazards, establish process for on-going risk management) should be followed to decide if a risk is tolerable. Risk analysis is an ongoing and iterative step and can continue in parallel with subsequent phases. It can be necessary to define further system safety requirements induced by the Risk Acceptance Criteria in order to reduce the risk to an acceptable level. System requirements can be derived / exist at different levels.
4. Specification of system requirements: detailing the initial system requirements (expected functions including their RAMS requirements) and the ones derived from risk assessment in phase 3 as well as defining criteria for acceptance and specifying the overall demonstration of compliance.
5. Architecture and apportionment of system requirements: allocation of requirements (including all RAMS requirements) to subsystems and components.
6. Design and implementation: subsystems and components should be created according to the allocated requirements (including RAMS

requirements).

7. Manufacture: the subsystems and components of the system should be manufactured and RAMS centred assurance arrangements established and applied.
8. Integration: all subsystems and components should be assembled and installed to form the complete system.
9. System validation: it should be validated that the system, product or process complies with the RAMS requirements in combination with external risk reduction measures, confirming that it is suitable for a specific intended use.
10. System acceptance: compliance of complete system with overall RAMS requirements is required for entry into service.
11. Operation, maintenance and performance monitoring: The objective of this phase is to operate, maintain and support the product, system or process such that compliance with system RAMS requirements is maintained. This includes to continuously evaluate the RAMS performance of the system and to derive corrective measures if required.
12. Decommissioning: the risk is controlled during the transition phase.

A risk assessment shall be undertaken for the system under consideration. For each identified hazard or its RAM equivalent, it shall be decided if the related risk can be considered as “broadly acceptable”. This decision shall be justified and recorded. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.

To summarize all these assumptions, it is possible to state that the railway standards underlines the importance of RAMS study in this particular field of application, with specific reference to the risk assessment and the human factor quantification.

1.2 Objective of the work

Section 1.1 resumes what are the topic contains in the railway standards and which are the steps and focus of RAMS in railway. Great attention must be paid on human factors. UIC (International Union of Railway) every year publishes a safety report indicating the main causes of railway accident in the previous year. Table 1.1 shows the values related to the last safety report published in 2021 with reference to accidents occurred in 2020 [5].

Tab. 1. 1. 2020 main cause of railway accident. Source: [5].

2019	**Cause at first level**	**Cause at second level**	
External Causes **89,9%**	THIRD PARTIES 88,4%	Trespassing	73,2%
		Vehicle (LC accident)	9,4%
		Pedestrian (LC accident)	3,7%
		Pedestrian on public railway area	1,7%
		Other or not specified	0,4%
	WHEATHER & ENVIRONMENT 1,6%	Environment	1,4%
		Weather	0,2%
Internal Causes **9,7%**	INFRASTRUCTURES 1,8%	Tracks and structures	0,8%
		Energy system	0,5%
		Other or not specified	0,4%
	ROLLING STOCK 1,7%	Running gear	0,8%
		Other or not specified	0,9%
	HUMAN FACTORS (Railway staff & subcontractors) 5,0%	Track and switch maintenance staff	0,6%
		Traffic operating and signalling staff	1,3%
		Train drivers	1,2%
		Other or not specified	2,0%
	RAILWAY USERS 1,1%	Passengers	1,0%
		Other or not specified	0,2%
CAUSES NOT IDENTIFIED			0,4%

Human factors result to be the second cause of accident in 2020, contributing with a 5% to the overall accident percentage.

Figure 1.2 shows the values of the accident caused by human factors varies over the years. It is possible to note that 2018, 2019 and 2020 are characterized by lower percentage of human factor accident, that is possibly due to an increasing attention on the human factor topic in railway.

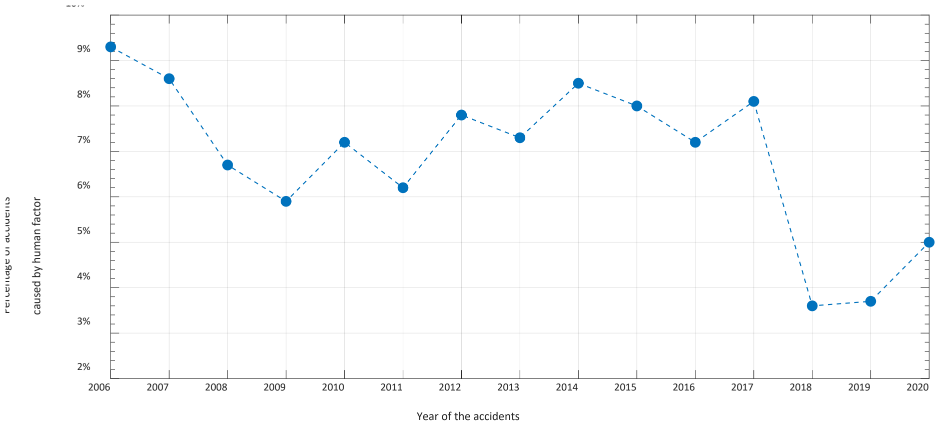


Fig. 1. 2 - Trend of the percentage of accident due to human factors.

In lights of the previous considerations, the aim of this research work is the optimization of maintenance in railway, focusing on two different (but strictly related) aspects:

a) Optimization of the maintenance decision-making process by risk related point of view.
b) Assessment of the human factors on maintenance task.

Firstly, the optimization of the maintenance plan (aspect a) has been investigated focusing on the RCM (Reliability Centred Maintenance) approach. This method is a standardized technique widely used in many different application fields. However, it leads the analyst to multiple possible choices relying significantly on the experts' subjectivity. Consequently, one of the objectives of this work is the introduction of an innovative fuzzy-based RCM to minimize the impact of subjectivity, simplifying the task selection and optimizing the maintenance policies. RCM is a risk-based maintenance technique which is built upon a FMECA (Failure Modes Effects and Criticality Analysis). FMECA is one of the RAMS methodologies suggested in railway standards to develop the risk assessment of a railway system. As a matter of fact, this method is extensively used during the design of railway system despite lots of papers recognize several issues of the classical FMECA. A discontinuous scale of possible values, subjectivity, high sensitivity to small changes, absence of weight factors, multiple repetitions of the same value and difficulty in threshold definition are some of the major drawbacks of the RPN (Risk Priority Number) assessed during FMECA. A detail description of such drawbacks will be presented in the following sections. Trying to solve those needs, this work introduces two innovative techniques in the field of FMECA. The first one is a fuzzy-based approach aiming at proving the optimal failure mode prioritization solving all the drawbacks at the same time (with the only exception of the threshold estimation). The second one is a more general approach which could be applied to classical FMECA and all the alternative methods present in literature to quantitively e effectively estimate the RPN threshold.

The second part of the work (aspect b) deals with the estimation of the HEP (Human Error Probability) during the maintenance operations performed by operator on railway tracks. As underlined by analyzing the UIC safety report presented above the impact of human error on railway accident can not be neglected. Furthermore, railway transportation technology implements several ATP (Automatic Train Protection) systems to avoid accident caused by the train driver errors, consequently the human activities significant for the safety of railway passengers mainly resides in the installation and maintenance phases of the equipment. Notwithstanding that there are only few methods specifically developed to estimate HEP for railway-related application. The widest used methodology is the RARA (Railway Action Reliability Assessment) developed and validated in 2012. RARA is extensively used since it is the only widely recognized technique in this field, however it suffers two major problems: remarkably high impact of subjectivity and significant complexity required for the assessment of many numerical values difficult to be precisely estimated. Trying to fill these gaps, this research aims at introducing an innovative fuzzy-based approach which simplifies the assessment of the HEP by means of linguistic variables. Fuzzy sets have been used to develop a simple and effective tool which solves the RARA drawbacks even if it is based on the same failure database.

Finally, this work investigates the potentiality of the modern third generation HRA (Human Reliability Analysis) techniques based on simulators to precisely assess the human performances. An extensive literature review showed a lack of modern simulator develop for railway tasks. As a consequence, the last objective of this work is the introduction of a new HRA method, based on Weibull distribution, able to estimate the human error probability as time-dependent model which assumes different values during the work shift. The effects of one or more breaks within the work shift have been simulated with a proposed software as well as the impact of different break durations. Furthermore, the proposed method aims at introducing the Yerkes-Dodson model to describe the concept of beneficial stress along with the impact of the classical stress.

The research goals and the objectives of the work previously described are summarized in figure 1.3.

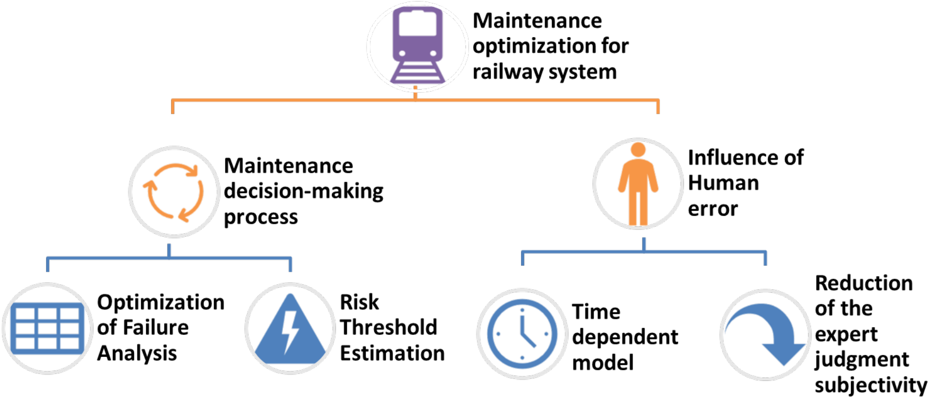

Maintenance optimization for railway system
Maintenance decision-making process
Influence of Human error
Optimization of Failure Analysis
Risk Threshold Estimation
Time dependent model
Reduction of the expert judgment subjectivity

Fig. 1. 3 - Research objectives and summary of the work.

1.3 Case studies

The above-mentioned innovative methods developed in this work have been applied to several case studies in order to test the methodologies and validate the results. More in detail, two complex systems such as Heating Ventilation and Air Conditioning (HVAC) and railway signaling systems have been studied and discussed.

HVAC is a complex system integrating mechanical, electric and electronic items; it is a mandatory equipment mounted on a train and in this work it has been analyzed in order to test and validate the risk threshold estimation and the maintenance decision making process.

Railway signalling systems are composed by several types of different equipment and safety systems, this work focuses on Automatic Train Protection (ATP) used to assess the contribution of the human error.

1.3.1 Heating Ventilation and Air Conditioning

A Heating Ventilation and Air Conditioning (HVAC) system is the technology of indoor and vehicular environmental comfort. The objectives of HVAC systems are to provide an acceptable level of occupancy comfort and process function, to maintain good indoor air quality (IAQ), and to keep system costs and energy requirements to a minimum [6]. Furthermore, one of the main objective of HVAC is to ensure emergency ventilation and sufficient air exchange [6]–[9]. In summary, HVAC has to ensure four functionalities: cooling capacity, heating capacity, ventilation capacity and emergency ventilation.

HVAC is an important part of residential structures, such as single family homes, apartment buildings, hotels and senior living facilities. It is also essential in medium to large industrial and office buildings, such as skyscrapers and hospitals, and in vehicles, such as trains, ships and submarines. In all these structures, safe and healthy conditions are regulated with respect to temperature and humidity, using fresh air from outdoors.

In underground trains, the influx of a large number of people and the presence of moving trains generate a reduction in oxygen and an increase in heat and pollutants. Mechanical ventilation is required to achieve the necessary air exchange and grant users of the underground train systems comfortable conditions. Ventilation systems have a second and even more important purpose: to guarantee safety in the event of a fire emergency. Moreover, to create a safe and clean environment, ventilation is required both in the tunnels and in the stations. Consequently, in high-speed trains the HVAC is a safety critical system, it must be working properly during the entire train journey to ensure emergency ventilation in case of hazardous events.

Furthermore, an HVAC system has also comfort related functionalities: it has to move heat to where it is wanted (the conditioned space), or remove heat from where it is not wanted (the conditioned space), and put it where it is unobjectionable (the outside air).

The heating and air-conditioning system, whose central unit is usually placed on the roof of the train, ensures the thermal comfort and the quality of the air on board. Temperature and air quality sensors also play a decisive role, because as well as managing the temperature, the system recycles the air and therefore regulates the amount of oxygen available in the train cars [10].

The first step of the functioning of the air condition unit is the suction of warm air by ventilators from the train exterior, then a liquid refrigerant absorb the heat, therefore the heat is rejected outside the train and finally cooled air is released into the train interior. A sensor measures the temperature and the quality of the air inside the train, then the air conditioning absorbs in the air, mixing 1/3 of external air with 2/3 of internal air. The unit reinjects recycled, filtered air into the train unit.

Each car is equipped with two units to provide Heating, Ventilation and Air Conditioning (HVAC) to the car. In order to ensure the proper system functionality, a control system is required to manage all the HVAC functionalities. In particular temperature and humidity control are regulated through inside and outside sensors connected directly to a microcontroller-based unit.

The HVAC system installed in each car consists of an air equipment conditioning, a control rack, extractor box, heater and floor heaters, convectors, the necessary probes to control the temperature of the different enclosures of the car, a pressure wave control and a control panel in each cabin [11]. As possible to see in figure 1.4 the main components of the unit 121 series are as follows:

- 2 Condenser Heat exchanger (batteries) (1)
- 2 Direct drive condenser fan and motor assemblies (2)
- 2 semi-hermetic compressors (3)
- 2 liquid tanks (4)
- 2 filters drier (moisture) (5)
- High and low pressure switches
- 4 moisture and liquid indicators (6)
- 2 evaporator heat exchanger (evaporator coil assemblies with two horizontally split sections) (7)
- 4 thermal expansion valves (8)
- 4 Discharge line check valve (9)
- By-pass valve
- 2 direct drive condenser fan and motor assemblies (11) (including temperature probes (12))
- Outdoor air temperature sensor (13)
- 2 heating coils in evaporator (14)
- 8 air filters (evaporator input) (15)
- 2 pressure wave controls
- 2 outdoor air dampers (16, 17)

- Control panel (18)

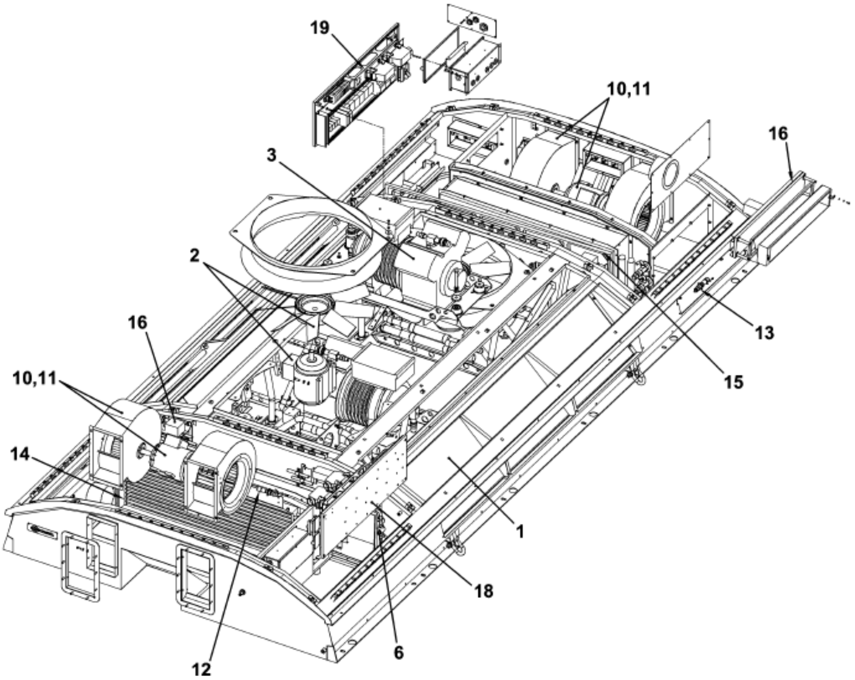


Fig. 1. 4 – Main components of the whole HVAC system

Tab. 1.2 contains all the technical information of the HVAC system under analysis.

Tab. 1. 2. Technical characteristic of HVAC.

Manufacturer	Merak
Cooling Power	32,5kW
Heating Power	37kW
Air Motion	4700m^3/h
Refrigerant	R-407C (11kg ± 15%)
Supply Voltage	72 VCC +25%/-30%

a) Refrigerant compressors

The compressor draws in the cold gases exiting the evaporator battery at low pressure and compresses them, so it comes out as gas at higher pressure and overheated [11].

The motor compressor is fitted with an electromagnetic valve to vary the capacity according to the demands of refrigeration load at any time.

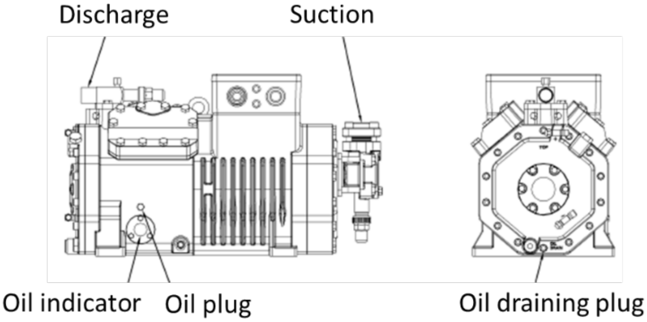


Fig. 1. 5– Compressor

This device allows the partially discharged starter (in two cylinders) relieving, in this way, the load imposed on the starter motor. The compressor incorporates a sensor to protect the motor against faults caused by the reheating of the coils due to lack of gas or excessive start cycles. This sensor disconnects the current input to the motor and resets automatically when the temperature decreases. The PSCT72-V protection module, installed in the junction box, is a device that verifies the thermal protection of the coils. These contain in the coils a PTC temperature sensor, which increases its resistance with temperature. The PSTC72-V is powered by the battery, it constantly reads the value of the PTC, and its output is a relay in series with the contactor of the compressor. Under normal conditions, the PTC has a low value and, upon arrival battery voltage to power the PSTC72-V, it closes its relay and allows the activation of the contactor, and hence the start of the compressor. However, if for various reasons the coil is overheated, the value of the PTC rises and the PSTC72-V opens its relay, so that the contactor is deactivated and the compressor stops (cut). Only when the coil is cools below a certain value, the PSTC 72-V again allows the start (reset). The cooling of the engine is achieved by the circulation of the refrigerant gas through the stator and rotor coils, which allows them to maintain their temperature below the limits allowed by the insulation.

Lubrication is performed by means of an oil pump coupled to the crankshaft, which can work rotating in both directions. The compressor has a sight glass located on the side of the crankcase to check the oil level. The compressor is mounted on four dampers to prevent vibrations and reduce noise.

The low-pressure safety switch, installed in the suction line, prevents the system works below atmospheric pressure; at the same time, interrupts the compressor in normal operation. The high-pressure safety switch, mounted on the discharge line, acts when the discharge pressure exceeds the allowable limit, stopping the compressor.

b) Liquid tanks

The liquid tanks are located in the central zone of the condenser module, installed horizontally next to each of the fan motors. The liquid reservoir provides the ability to contain all of the liquid refrigerant when the equipment is not functioning [11]. It is equipped with a rotalock type valve placed at the inlet and outlet thereof and a purge valve, located in the middle reservoir, which is used to remove non-condensable gases from the system and to remove the refrigerant from the equipment, as well as to evacuate the installation when it is necessary.

During normal operation of the equipment, the inlet and outlet valves of the liquid, as well as the outlet of the dehydrator filter should be open, while the bleed valve remains closed. The caps of these valves should be tightened always after performing any maintenance operation.

c) Drier Filter

The drier filter is constituted by a cylindrical container mounted on the line of liquid at the outlet of the liquid reservoir, inside which are housed a dehydrating cartridge of the interchangeable solid core type, made of a silica-gel and alumina activated; and a metal filter [11]. It also has a shut-off valve of Ø5 / 8 "(15.88 mm) located at the outlet, which allows to close the passage of refrigerant through it. The purpose of the dehydrating filter is to prevent the passage of any solid particles (dirt, oxide particles, welding debris, etc.) that can be found in the pipes, as well as retain moisture and acids that may exist in the refrigerant.

d) Moisture and liquid indicators

This element is located on the liquid line, at the outlet of the dehydrator filter and has two functions [11]:

- Display the moisture content of the system by means of an indicator element that changes of color in direct relation to the amount of humidity present in the system. When this is free of moisture, the indicator color is green, and becomes yellow as the moisture inside the system increases. If the indicator reaches a deep yellow color it is a sign that there is a large quantity of humidity inside the system and it is necessary to replace the dehydrator filter.

- Allow the visualization of the coolant flow through the molten glass visor, so that it can be easily seen if there is bubble passage, which indicates anomalies such as low refrigerant charge, insufficient liquid cooling refrigerant, low discharge pressure or restrictions in the liquid line.

e) Cooling system

The cooling system includes a high-pressure safety switch and a low-pressure safety switch. If the discharge pressure is excessive or if the suction pressure drops below their respective setpoints, the pressure switch, corresponding of a safety device, proceeds to cut the open circuit, causing the equipment to stop [11].

The compact equipment is composed by a safety pressure switch (high and low pressure) and the sensors (pressure probes) of the refrigeration circuit of the equipment, thus allowing the control and protection of the various operations. At the pressure distributor level of the panel, automatic or shell valves allow connect the high and low pressure gauges, while the pressure measurements of each circuit must be performed before vacuuming. These valves must be closed and sealed when not used to perform any operation. The high pressure safety switch stops the equipment when the high pressure exceeds a limit determined.

The low pressure safety switch prevents the system from operating below the atmospheric pressure. The high pressure sensor (probe) controls the discharge of the refrigerant output from the compressor. This collector generates an analogue signal between 4 and 20 mA, which is proportional to the discharge pressure value. This value is sent to the control module, which is the one that compares the analogue signal with the internal reference value. When the pressure of discharge exceeds the reference value, the control module adopts a cooling modulated before the limit pressure is reached.

Modulated cooling is the discharge procedure of the compressor cylinders in order to reduce the pressure of discharge when the system operates below the discharge pressure limit. The discharge of the cylinders reduces the cooling capacity, together with the pressure of discharge, thus preventing the operation of the system above the limit. Once discharge pressure falls within the operating range, the control connects new compressor cylinders, and the system returns to full capacity.

The low gauge controls the suction pressure of the refrigerant when entering the compressor. The transmitter generates an analogue signal between 4 and 20 mA, which is proportional to the value of the suction pressure. This value is sent to the control module, which compares the analogue signal with the internal reference value. When the suction pressure is lower than the control module adopts modulated cooling before the limit.

f) Evaporator heat exchanger

The evaporator batteries are formed by a copper tubes [11]. Inside the tubes circulates the coolant, which, when evaporated, causes a cooling of the tubes and fins, so that the air passing through them also cools to be subsequently pushed into the room. This battery is powered by two thermostatic expansion valves that distribute the refrigerant through the small distributor holes in the evaporator battery, producing as a consequence of this, a reduction of the pressure and with it the coolant temperature.

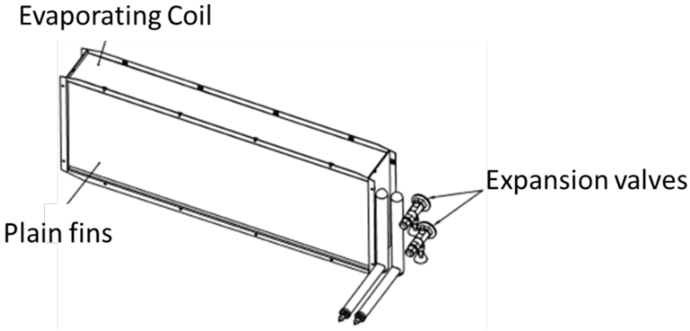


Fig. 1. 6– Heat exchanger

g) Thermal expansion valves

The function of the expansion valve is to allow liquid to enter in the battery in the adequate measure to achieve a correct evaporation of the refrigerant at the outlet of the same; while ensuring a sufficient differential pressure between the high and low sides pressure of the cooling system [11].

To perform this function, the valve consists of a valve body connected to a temperature-sensing bulb through a capillary tube. The valve body is mounted on the liquid line and the bulb is fixed to the outlet of the evaporator, in the suction line.

The bulb contains a small amount of refrigerant. The free space of the bulb, the tube capillary and the free space above the valve is filled with saturated steam at the pressure corresponding to the bulb temperature. The space below the membrane is in connection with the evaporator, so that the pressure here is the evaporation pressure.

The degree of opening of the valve is determined by the pressure produced by the temperature of the charge of the bulb acting on the upper face of the diaphragm and the pressure below the diaphragm, which is the sum of the evaporation pressure plus the pressure of the acting spring through the lower part of the diaphragm.

In this way, the thermostatic expansion valve works by the pressure difference between the steam pressure in the evaporator and the pressure of the charge in the thermal bulb. Market Stall that the thermal bulb is in contact with the suction line, the pressure in it depends on the temperature in said line, which allows controlling the same.

The thermostatic expansion valve is equipped with a pressure equalization line, connected to the outlet of the evaporator, next to the thermostatic bulb, to compensate the losses pressure due to the distributor and the evaporator surface. The function of the distributor of liquid is to achieve a uniform battery power.

h) Discharge line check valve

These items are electromagnetic servo controlled shut-off valves. They are located in each refrigerant circuit, in front of the liquid sight glass [11].

Normally they remain closed and must be energized to open them. Its mission is to avoid that coolant can enter in the compressor at times when it is not working.

The by-pass solenoid valve is installed between the high and low pressure line of the refrigeration. Its mission is to adapt the capacity of the compressor as a function of temperature by the injection of hot gas, taken from the outlet of the compressor to the evaporator battery inlet. In this way, the number of start / stop cycles of the compressor is reduced.

i) Direct drive condenser fan and motor assemblies

In order to drive the treated air into the room, the equipment is provided with two double suctions built by two centrifugal fans. Each fan is driven by a three-phase motor of 1.1 kW of power working at 1500 r.p.m. with a supply voltage of 400 V, 50 Hz. This motor is continuously operated.

Furthermore, this set also includes the driven air temperature probe [11].

j) Temperature sensors

The compact air conditioner has four temperature probes inside the equipment [11]:

- 2 outdoor air temperature probes located in the air inlets exterior renovation.
- 2 driven air temperature probes, located in the motor-fan evaporator.

All these probes use an NTC thermistor that has the characteristic of varying its electrical resistance as a function of temperature in such a way, that the greater is the temperature and the lower is its resistance and vice versa.

In this way the electronic control can inspect the different temperatures for select the most suitable operating mode and maintain the comfort conditions in the passenger rooms.

Outside the equipment has 5 probes:

- Return grilles (2 units installed in the air return grille in all cars).
- WC (2 units installed in the extraction rack of the WC).
- Platform (1 unit installed in the platform removal grid).

k) Heating coils in evaporator

The compact equipment includes two heating resistor housings installed each of them in parallel to the evaporator battery [11]. The system is protected against over-temperatures by a safety thermostat. Acts disconnecting the resistors through the electronic control, when the temperature around the resistances exceeds 90 °C and reconnects when the temperature returns to enter within the working range (69 °C).

l) Air filter

The compact air conditioning unit has eight air filters, four in each air intake to the evaporator battery [11]. Their mission is to prevent the passage of dust, dirt and any kind of solid particles that can penetrate the compact equipment and be retained between the fins of the evaporator battery, obstructing the air circulation, as this would cause a malfunction of the system, such as low pressure suction or ineffective conditioning of the room.

m) Outdoor air dampers

On the sides of the compact equipment, in the areas of external air intake, a damper is located to guarantee the air flow renovation in the different operating cycles. The change of position of the dampers is governed by the electronic temperature control [11].

Each damper is driven by a motor coupled directly to its shaft, which incorporates an anti-rotation device which prevents rotation about the axis. This motor is protected against overload and it stops automatically when it reaches the top of its route.

The external air gates close only at the initial start-up time if the temperature of the car is within the limits of preconditioning and if determined by the wave detection signal.

1.3.2 Railway Signalling System

According to the European standard IEC 50129 railway signalling is a system used to ensure the safe movement of trains [4][12]. There are two fundamental physical reasons why railway signalling system exists:

1. Trains are guided by the track and hence have to be routed in such a way as to avoid collisions with one another.
2. Trains (especially high-speed ones) cannot stop within the distance that the driver can see, so they need to have prior warning of the need to slow down and stop ahead.

The basis principle underpinning signalling systems is the Block System. Each line is divided into Block Sections, and except in particular circumstances only one train is permitted to be in each block section at any time. A signal is provided at the start and at the end of each block section to allow the train to enter and exit the block. If the block is occupied by a train, the signal will display a red "aspect" to tell the train to stop. If the section is clear, the signal can show a green or "proceed" aspect. The simplified diagram in figure 1.7 shows the basic principle of the block system.

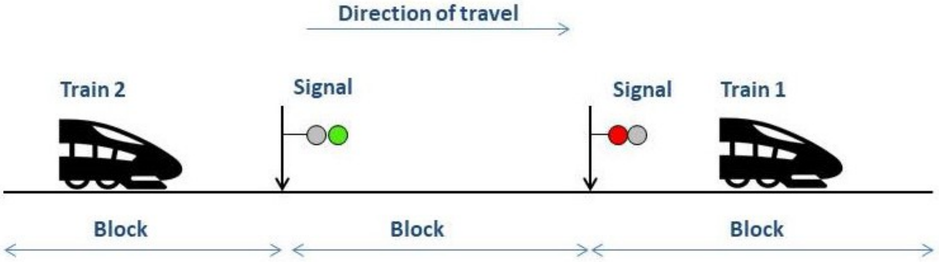


Fig. 1. 7 - Schematic of signal block section. When a block is unoccupied, the signal protecting it will show green. If a block is occupied, the signal protecting it will show red.

The block occupied by Train 1 is protected by the red signal behind it at the entrance to the block. The block behind ("in rear", as it is known) is clear of trains and a green signal will allow Train 2 to enter this block. This enforces the basic rule or railway signalling that says only one train is allowed onto one block at any time.

The basic, two-aspect, red/green signal is used for lower speed operation but for anything over about 50 km/h the driver of a train needs a warning of a red signal ahead to give him room to stop. In the UK, for example, this led to the idea of caution signals (originally called "distant" signals when they were mechanically operated semaphore arms) placed far enough back from the signal protecting the entrance of the block to give the driver a warning and a safe braking distance in which to stop. Each signal would now show a red, yellow or green aspect - a multi- aspect signal. The diagram in Figure 1.8 shows an example of line with 3-aspect signals.

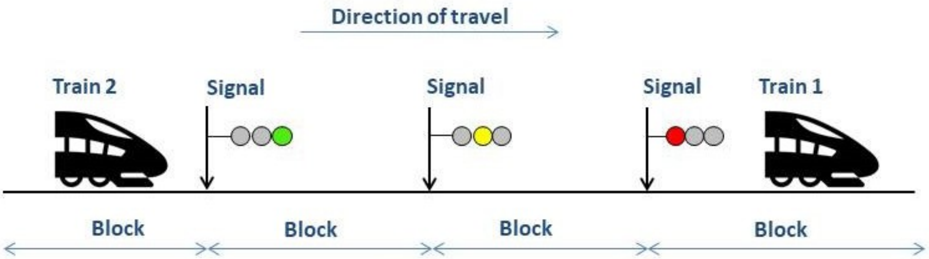


Fig. 1. 8 - Schematic of 3-aspect signalled route showing the additional yellow aspect provided to allow earlier warnings and thus higher speed operation.

The block occupied by Train 1 is protected by the red signal at the entrance to the block. The block behind is clear of trains but a yellow signal provides advanced warning of the red aspect ahead. This block provides the safe braking distance for Train 2. The next block in rear is also clear of trains and shows a green signal. The driver of Train 2 sees the green signal and knows he has at least two clear blocks ahead of him and can maintain the maximum allowed speed over this line until he sees the yellow.

The multi-aspect signalling commonly used in some countries like UK today has been converted into a 4-aspect system. It works similarly to the 3-aspect system except that two warnings are provided before a red signal, a double yellow and a single yellow. This has two purposes. First, it provides early warnings of a red signal for higher speed trains or it can allow better track occupancy by shortening the length of the blocks. The high speed trains have advanced warning of red signals while the slower speed trains can run closer together at 50 km/h or so under "double yellows" [13].

Based upon this simple principle, signalling systems have evolved to provide the following key functions:

Safety Functions:

- to prevent trains taking conflicting routes;
- to mantain a safe distance between trains;
- to protect trains from driver malfunction (incapacity / inattention / misjudgement);
- to ensure trains do not exceed their permitted speed.

Non safety functions:

- to maximise the use of the track;
- to route trains automatically and regulate their flow;
- to provide data on train running for passenger information purposes.

a) Train detection system

The train detection system is one of the main subsystems of a railway signalling system. The aim of train detection is to determine if a particular section of track is occupied by a train.

b) Track Circuits

With the original mechanical signalling systems the only form of train detection was manual observation by the signaller looking out of the signalbox window.

To protect against human error, track circuits were developed, which use insulated sections of the rails as an electrical circuit, which the wheels of a train shunts as it enters the section. Track circuits are used to determine whether a train is in a specific block and allow railway signalling systems to operate semi automatically, by displaying signals for trains to slow down or stop in the presence of occupied track ahead of them. A track circuit typically has power applied to each rail and a relay coil wired across them. When no train is present, the relay is energised by the current flowing from the power source through the rails. When a train is present, its axles short (shunt) the rails together; the current to the track relay coil drops, and it is de energised. Circuits through the relay contacts therefore report whether or not the track is occupied. A schematic example of the track circuit is shown in Figure 1.9.

Each circuit detects a defined section of track, such as a block. These sections are separated by insulated joints, usually in both rails. To prevent one circuit from falsely powering another in the event of insulation failure, the electrical polarity is usually reversed from section to section. Circuits are powered at low voltages (1.5V to 12V DC). The relays and the power supply are attached to opposite ends of the section to prevent broken rails from electrically isolating part of the track from the circuit. A series resistor limits the current when the track circuit is short-circuited. In the simplest form the transmitter is a battery and the detector is an electro- mechanical relay. Many much more sophisticated types exist using coded audio signals and frequency shift keying (FSK) modulation, which were developed to provide immunity from EMI (Electromagnetic Interference) generated by electric trains.

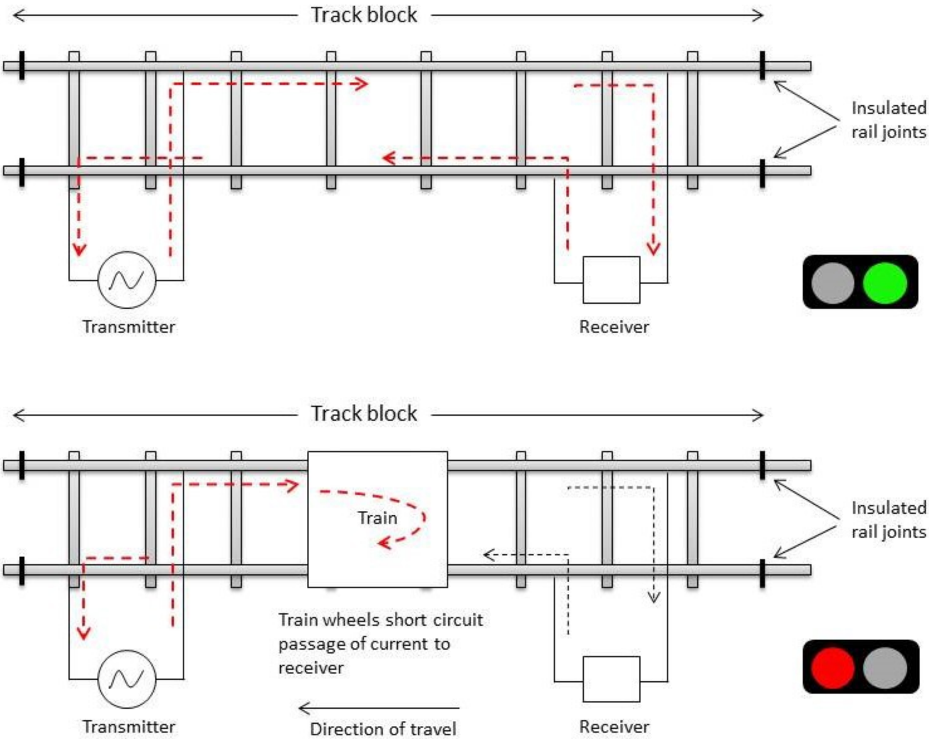


Fig. 1. 9 - Schematic drawing of track circuit for unoccupied and occupied block.

The track circuit illustrates the key principle of “Fail Safe” applied to all traditional signalling equipment, in that any break in the circuit between the transmitter and the receiver has the same functional effect as a train shunting the rails, and hence the system fails to a safe state. In Multiple Aspect Signalling installations, large numbers of individual track circuits cover the entire track layout to provide complete train detection. In some railway electrification schemes, one or both of the running rails are used to carry the return current. This prevents use of the basic DC track circuit because the substantial traction currents overwhelm the very small track circuit currents.

Where DC traction is used on the running line or on tracks in close proximity then DC track circuits cannot be used, as it is for 50 Hz AC electrification. To accommodate this, AC track circuits use alternating current signals instead of direct current (DC) but typically, the AC frequency is in the range of audio frequencies, from 91Hz up to 10kHz. The relays are arranged to detect the selected frequency and to ignore DC and AC traction frequency signals.

Again, failsafe principles dictate that the relay interprets the presence of the signal as unoccupied track, whereas a lack of a signal indicates the presence of a train. The AC signal can be coded and locomotives equipped with inductive pickups to create a cab signalling system.

Modern track is often continuously welded, with the joints being welded during installation. This offers many benefits to all but the signalling system, which no longer has natural breaks in the rail to form the block sections.

The only method to form discrete blocks in this scenario is to use different audio frequencies in each block section.

To prevent the audio signal from one section passing into an adjacent section, pairs of simple tuned circuits are connected across the rails at the section boundary. The tuned circuit often incorporates the circuit to either apply the transmitted signal to the track or recover the received signal from the other end of the section.

c) Axle counter

An axle counter is a device on a railroad that detects the passing of a train between two points on a track. A counting head (or "detection point") is installed at each end of the section, and as each train axle passes the counting head at the start of the section, a counter increments.

A detection point comprises two independent sensors, so the device can detect the direction and speed of a train by the order and time in which the sensors are passed.

As the train passes a similar counting head at the end of the section, the system compares count at the end of the section with that recorded at the beginning. If the two counts are the same, the section is presumed to be clear for a second train. This is carried out by safety-critical centrally located computers, called "evaluators", with the detection points located at the required sites in the field.

The detection points are either connected to the evaluator via dedicated copper cable or via a telecommunications transmission system. That allows the detection points to be located significant distances from the evaluator, and this is useful when using centralised interlocking equipment, but less so when signalling equipment is situated beside the line in equipment cabinets. The functional scheme in shown in Figure 1.10.

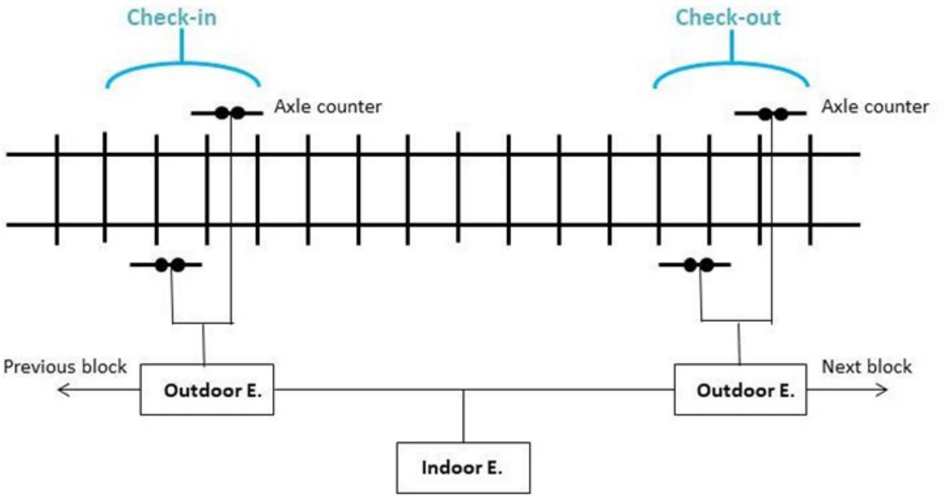


Fig. 1. 10 - Schematic drawing of axle counters positioning along the track.

Axle counters have many advantages:

- Differently from other signaling systems, an axle counter system can cover a very long section up to 15km.
- It does not get affected either by flooding of track or poor maintenance of tracks. Same thing cannot be said of the track circuit, which is highly susceptible to these conditions.
- It does not require insulating rail joints, thus, rails can be continuously welded. This reduces track wear and maintenance cost and increases traveling comfort.
- Efficiency and safe working of axle counters does not depend up various track parameters and climate condition such as length, ballast condition, drainage, stray voltage and currents, track feed voltage and lead cables, etc. like track circuits.

d) Interlocking

A rail network, even more than a road network must be controlled to allow trains to circulate in total safety. This control is taken care of by interlocking. Interlocking is an arrangement of points and signals interconnected in a way so that each movement follows another in a proper and safe sequence [68].

An interlocking calls and locks safe routes through railway stations and junctions. The interlocking locks a route only if it is safe for a given train, i.e. the route must be vacant from other trains and no conflicting routes must be locked contemporarily.

Locking a route for a train means reserving a sequence of track detection sections and locking the direction of movable track elements to allow the train moving from an origin signal to a target signal. Movable track elements include infrastructure elements that have a mutable direction such as switches, level crossings, movable bridges and movable derailment devices. The interlocking systems typically sets and locks movable track elements in a well-defined direction [14].

Throughout its journey a train will run on various track sections controlled by an interlocking system. Installed by the trackside, interlocking authorises the train to continue its journey or not, anticipating the state of traffic thanks to the connection to the track management equipment.

Thus interlocking systems must ensures the safe circulation of trains with regard to:

- the road network by controlling level crossings;
- the rail network as a whole.

Interlocking systems are able to detect the presence of a train on a track section thanks to information received from track circuits and balises. If another train approaches the section, the interlocking interfaces ask the train to stop by activating the signal lamps. They also control the points systems to ensure correct train routing.

Since the end of the 19th century interlocking has considerably evolved. The original, entirely mechanical systems have gradually been replaced by computerised systems which can handle far more complex circulation patterns like those operated in major stations.

As for information transmission, it is handled by a high-speed cable network. Train circulation parameters such as speed and braking distance are now handled by specialised systems such as ERTMS (European Rail Traffic Management System). Information is thus exchanged directly by radio thanks to antennas by the trackside.

A schemetic representation of a modern interlocking system is represented in Figure 1.11.

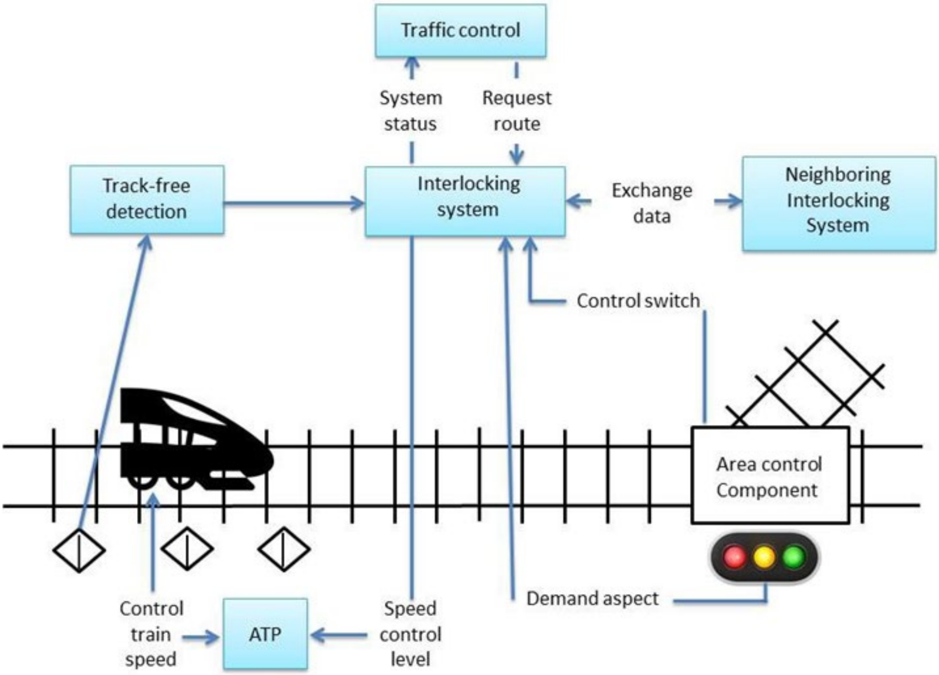


Fig. 1. 11 - Schematic drawing of an interlocking system.

e) Automatic Train Protection (ATP)

Automatic train protection (ATP) is a type of train protection system which continually checks that the speed of a train is compatible with the permitted speed allowed by signalling. If it is not, ATP activates an emergency brake to stop the train. All types of train protection systems aim to reduce or eliminate the possibility of driver error resulting in a train movement related accident by failing to obey a visually displayed line-side or in-cab signal instruction. The development of train protection on main line railways began with the introduction of warning systems and subsequently progressed to enforcement of the instructions issued by these systems. Originally, the warning systems alerted the driver that he or she was approaching an adverse or restrictive line-side signal aspect and required him or her to acknowledge the warning. Otherwise the systems would initiate a brake application after a short delay. Later developments included various levels of speed limitation and enforcement.

Also, some systems were expanded to cater for speed limits for permanent or temporary speed restrictions. Technologies adopted for such warning and train stop systems include combinations of permanent magnets and electromagnets, inductive polarity-changing responders, coded beacons and simply coded track circuits. More recently, fully Automatic Train Protection (ATP) systems have been developed to enforce speed limits and movement authorities at the full range of restrictive signals, with and without line-side signals and including permanent and temporary line speed limits. Driving is still manual but speed limits are always enforced.

There are principally two implementations of ATP systems: intermittent and continuous.

Intermittent systems use electronic beacons (inductive or radio frequency) or short electrical loops positioned within the meter. These types of short-range devices are often referred to as "balises" (from the French word for "marker"). There are two kinds of balises: active and passive ones. The former are track based transponders that are "woken up" by a low frequency signal. They receive their energy from a passing train and then send packets of information to the train (track speed limit, gradients and signal information). The latter are track based transponders that are powered from the signalling supply and that continuously send packets of information to passing trains. The continuous systems use a permanently active data transmission and monitoring system, either through electrical inductive coupling by means of track loops or coded track circuits or by means of radio transmission of limit of movement authorities. Balises receive information from the Lineside Electronic units (LEUs), that are connected to signalling equipment.

More in detail, ATPs are generally based on two subunits interacting with each other:

- An onboard subsystem.
- A ground subsystem.

The main equipment on train (on-board subsystem) generally includes the following items:

- An antenna that is mounted underneath each cab and receives information from balises.
- A computer that combines the information received from the trackside with train characteristics, such as train length and braking ability to calculate safe stopping distences and speeds.
- The ATP screen, known as the driver machine interface (DMI), which allows drivers to view information about the current track speed, the track ahead and system details.

The main devices of a generic ATP are shown in Figure 1.12.

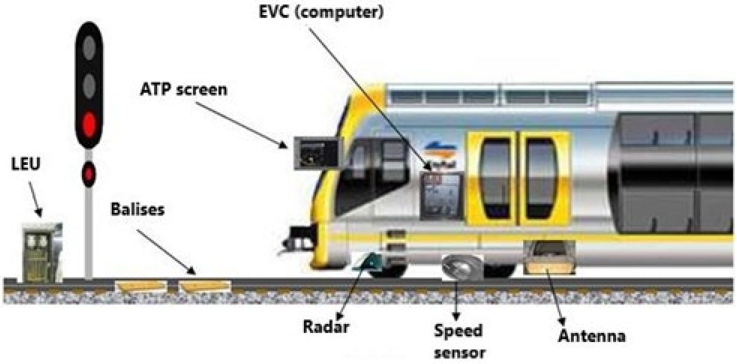


Fig. 1. 12 - ATP eqipment. Source: www.railwaysignallingconcepts.in

Fully operational ATP systems were first introduced on metros in the late 1960s and are now common on such systems all over the world. Most metro applications use continuous systems in conjunction with automatic train operation. The basic defining principle of ATP is that train speed is monitored against the current permitted speed limit. The speed may be limited by line profile or signal indication, that is, the need to protect routes of other trains and track related constraints. If the allowable speed is exceeded, a brake application is invoked until the speed is brought within the required limit or the train is stopped. Most ATP systems are based on conventional block signalling although these can be very short. Each block is described by a fixed dataset related to its location, length, gradient(s) and maximum speed limit(s). Each block will also have a variable data set derived from the signal aspects ahead and their effect on the resulting speed limit(s) for that block and the next block(s).

The speed limit on the approach to a restrictive signal forms a gradually reducing curve that follows the braking profile required to reach the target speed at the signal as shown in Figure 1.13. If the signal shows a stop aspect, the target speed will be zero. The on-board monitoring equipment will continuously compare the train speed with the curve required to achieve the target speed and will initiate a warning, usually both audio and visual. If action is not taken by the driver, the system will start a brake operation. In some implementations of the ATPs, a braking curve infringement calls for a full service brake initiation, in others cases it can activate directly the emergency brake.

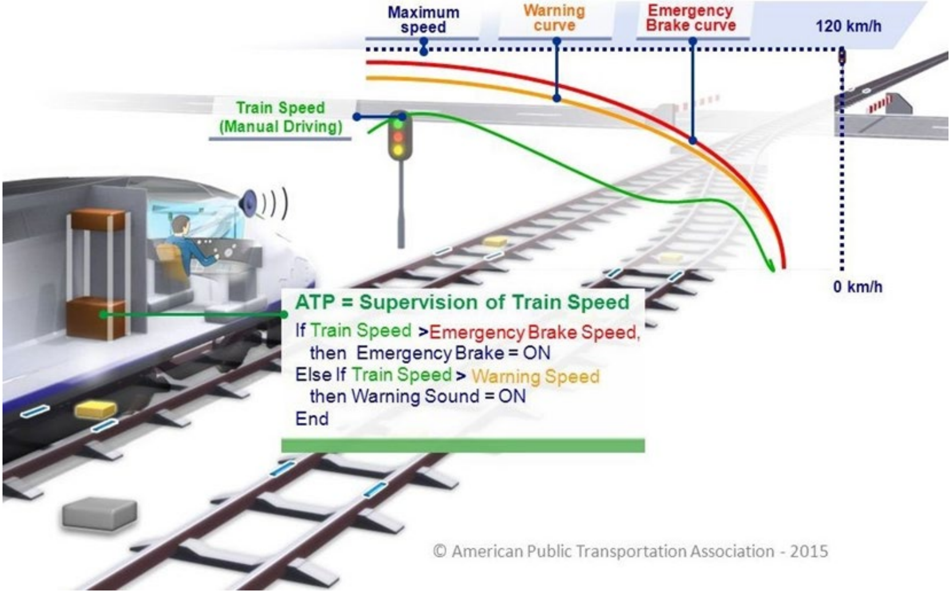

Maximum speed
Warning curve
Emergency Brake curve
120 km/h
Train Speed (Manual Driving)
0 km/h
ATP = Supervision of Train Speed
If Train Speed >Emergency Brake Speed,
then Emergency Brake = ON
Else If Train Speed > Warning Speed
then Warning Sound = ON
End
© American Public Transportation Association - 2015

Fig. 1. 13 - Speed curve required to reach the target limit at the signal.

There are also differences in the brake release function. Some systems allow the driver to release the brake once the train speed has returned within the prescribed curve. In others, the brake command is irrevocable and the train must be brought to a stand before the driver can release the brake. There are also railway undertaking specific rules about the consequences when the ATP system has intervened.

On the train, data comprising train weight, length, braking capability and maximum technically permitted speed are necessary to ensure compliance with speed limits set by the ATP system. Usually, the train consist data must be input by the driver before the trains starts its journey. In most cases, the performance of the equipment is monitored and recorded for further analysis in case of infringements or failures of the system. These systems are variously known as On Train Monitoring Systems (OTMS), On Train Data Recorders (OTDRs) or On Train Monitoring Recorders (OTMRs). They are the equivalent of the aircraft industry’s "black box".

Continuous ATP systems allow constant data updates to be transmitted to trains so that the train driver can respond to changes in signal aspects as soon as they occur. Intermittent systems can only transmit changes in signal aspects when the train passes over a beacon or loop. This can restrict line capacity if a driver is unable to respond to a signal clearance, even though he or she can see the change of aspect, until the train's on-board ATP computer has received a message from the balise located at the relevant signal. In order to overcome this problem, infill loops or balises are provided at some signals to provide drivers with an update of a signal aspect and to allow brake release if a less restrictive aspect is shown.

ATPs are particular useful to identify both hardware failure and/or human error. If the driver of the train fails to obey an instruction of railway signaling the ATP mitigates this failure adapting the train speed to the requirement of the signaling[4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15][4], [15].

The ground unit of the ATP under test is illustrated in Fig. 1.14. It comprises a set of two balises deployed in different point of the rail tracks. Usually, these kinds of transponder are located near a semaphore or a reduced speed zone and they are used to relay information regarding the signaling to the onboard subsystem of the passing train.

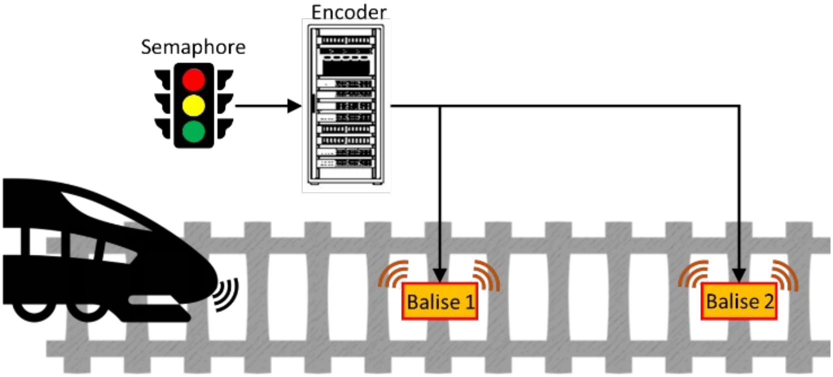


Fig. 1. 14 - Scheme of the Automatic Train protection under test highlighting the devices of the ground subunit (Two balises, an encoder and a semaphoric unit).

Most of ATP uses two nearby balises located in the center of the railroad track to ensure high reliability and safety requirements. To avoid crosstalk and ensure a correct communication between onboard unit and ground unit a set of strict requirements are forced during the balise installation.

Another fundamental equipment making up the LEU of the ATP under analysis included within the ground subsystem is the encoder which is used to convert the signaling information from semaphores and signals into messages suitable for the balises.

f) EVC board

The EVC (Enhanced Vital CPU) board is a microcontroller-based unit designed and assembled by Alstom Signalling Solutions S.r.l. and used for railway signalling systems.

EVC board is used in Italy and abroad for many applications:

- Ground signalling
  - axle counters for traditional railways;
  - axle counters for urban transportation;
  - low-complexity interlocking;
- On-board signalling;
  - on-board Automatic Train Protection (ATP) systems for traditional railways (Italy);
  - ATP system for urban transportation.

EVC board is a 32 bit 150MHz dual-microprocessor board with a vital 2 out of 2 architecture. Two microprocessors own identical core system components (RAM/ROM etc.), run identical program codes, read a single input from two different paths (read lines of external bus are dubled) or accept sunchronized inputs from a single input source. Internal address bus, control signals (including chip-select and read/write signals) and data bus outputs are constantly being compared by hardware at real-time. Any difference between the two processors' outputs will activate an NMI (Not Maskable Interrupt) to both processors, which will in turn halt the whole system. Once in the halt mode, microprocessors can be driven into an idle state, defined as the fail-safe state, until a hardware reset to start over the program.

1.4 List of major contributions

This thesis aims to optimize the risk assessment in railway field dealing with two major aspects: planning of maintenance activities by a reliability point of view and impact of human factors in maintenance operation within the whole risk assessment.

One of the widest used technique to assess the maintenance tasks of a generic complex system is the Reliability Centred Maintenance, which is a standardize technique based on a FMECA procedure. An extensive literature review highlighted that the classical RCM is an extremely subjective technique which leave to the analyst multiple choices. Thus, the selection of the maintenance task is not only guided by the preliminary risk analysis, but it relays remarkably on the expert's judgment.

The main contribution of this work regarding this topic is the introduction of a fuzzy-based decision-making diagram to guide the selection of the optimal maintenance task within the reliability-centered maintenance procedure. The proposed procedure helps to rapidly, easily, uniquely, and unambiguously identify the optimal maintenance policy, while the classical RCM procedure leads the analyst to multiple choices involving high subjectivity in the definition. Moreover, the methodology presented is a diagnostic-oriented decision diagram that favors the choice of condition-based maintenance whenever possible, (i.e. condition monitoring and failure finding procedures).

FMECA is the core of RCM and it is extremely useful to perform a risk assessment. Several papers in recent literature agree that classical FMECA is characterized by several drawbacks, such as high subjectivity of the RPN (Risk Priority Number) assessment and a difficulty of discerning critical and negligible failure modes. The identification of the most critical parts is usually performed by experts, leading to a high subjective decision. Alternatively, some companies apply corrective actions in a hierarchical order starting from the most critical components. Then, countermeasures are applied until the budget allows it. The major flaw of this cost-oriented approach is that some critical risk could not be mitigated. For some application this approach is valuable, quite the opposite safety related applications such railway systems require a more precautionary point of view. Consequently, it is extremely important to identify which components are critical and which are not by means of a risk threshold. The international standard IEC60812 which defines the FMECA technique does not explain how to evaluate a risk threshold value. Furthermore, only few papers in recent literature deals with this issue. This work introduces a new analytical approach to overcome this limit by estimating a Risk Priority Number threshold.

While to overcome the subjectivity issue, this work proposes a simple and effective tool that use Fuzzy theory to solve all the problems of the classical RPN and consequently provides an efficient methodology to prioritize failure modes according to their risk. In particular, this work proposes a fuzzy-based approach that uses fuzzy linguistic term to assess the O, S and D and then evaluates the RPN of each failure mode as the fuzzy multiplication of the indexes. Fuzzy weights are also taken into account to assess different importance to Occurrence, Severity and Detection. A graphical user interface was developed using MATLAB programming language to automatize the tool and make it accessible also on industrial field. The advantages of the proposed procedure are extensively illustrated emphasizing the benefits achieved with the proposed fuzzy-based tool to solve classical RPN drawbacks.

The second great topic covered by this work is human error and human factors, which are fundamental topics to be considered in a risk assessment of railway systems. RARA (Railway Action Reliability Assessment) is the only recognized HRA technique designed for railway, however is a very complex and subjective methodology which suffer many drawbacks. In order to solve these issues, a new method has been developed. The major contributions of the proposed method are the following:

- Introduction of an innovative HRA method specifically developed for operator tasks in railway engineering which uses fuzzy logic to estimate the HEP.
- Proposal of a RARA-based methodology able to solve two of the major problems of the classical RARA: the analyst subjectivity and the difficulty and complexity of a numerical assessment of the affect level.
- Validation of the results achieved on a real case study through a comparison with RARA method.

Recently HRA focused on third generation techniques, which represents the most modern techniques to assess the human reliability. There is not a third generation technique dedicated to railway, so E-SHERPA (Enhanced Simulator for Human Error Probability Analysis) has been developed to overcome this issue. The main contributions brings by this technique are the following:

- Introduction of the first third-generation HRA technique specifically developed and customized on railway engineering integrating the task provided by RARA within a SHERPA-based simulator (SHERPA is the acronym of Simulator for Human Error Probability Analysis).
- Accurate and detailed proof of the identification of the optimal Weibull parameter that best describe the human behavior.
- Time-dependent model of the human error probability varying during

the work shift which takes into account the fatigue cumulated during the shift by the operator and the beneficial effects of a break on the probability of committing an error. Both coffee break and lunch break are considered within the proposed method.

- Introduction of the Yerkes–Dodson curve describing the relationship between stress and performances in case of a difficult task. The Eustress concept (beneficial stress which increases the performance of the operator) is taken into account within the proposed procedure to model the performance shaping factor accordingly.

Chapter 2

Fuzzy Theory for Reliability analysis

This chapter provides an overview on fuzzy theory. The concept of fuzziness instead of discrete quantities adapts well to human reasoning that is inaccurate by nature. Fuzzy theory is exposed and explained clearly throughout the chapter using few examples. After that, the chapter focuses on the application of fuzzy inference system and the application of fuzzy theory to different aspect of reliability analysis.

2.1 Introduction

In the early '60s, Lofti A. Zadeh, a professor at the University of California, Berkeley, known for his contributions to set theory, began to warn that traditional systems analysis techniques were overly and unnecessarily accurate for many of the problems typical of the real world. The idea of degree of belonging, the concept underlying nuanced set theory, was introduced by him in 1964, and this led later, in 1965, to the publication of the first article 'Fuzzy Sets' and the birth of fuzzy logic [16]. The concept of a fuzzy whole, and of fuzzy logic, was enthusiastically received by some mathematicians, but most reactions were grouped between skepticism and open hostility. The tone of the controversy always remained very high especially in the early years of fuzzy logic, when its few supporters were not yet able to show any application.

However, in engineering laboratories fuzzy logic was proving promising in the field of control, until the first prototype of an application of the same appeared in 1974 by E. H. Mamdani, who developed a fuzzy controller for a steam engine [17]. Since then, studies on the uses of fuzzy logic have multiplied, especially in Japan where, perhaps for ideological reasons, but more likely for commercial reasons, Zadeh's ideas have met with much less resistance. The most famous fuzzy application is represented by the realization, in the mid-80s, of a control system for the Sendai metro[18].

Zadeh's text had a profound influence on the question of indeterminacy because it contrasted not only with probability theory, seen as the sole representation of uncertainty, but also with the foundations on which it itself rested: Boolean logic [19].

Fuzzy logic was introduced by Zadeh as a mathematical method for describing indeterminacy in everyday reality since the determinism of Boolean logic does not allow an exhaustive treatment of problems that by their nature are "nuanced" [20]. It, as the name suggests, is a type of logic that is based on seeing the quantities in an approximate way instead of discreet and for this reason it adapts well to human reasoning that is inaccurate by nature [21]. It then becomes clear that such logic is useful in reliability engineering for the following reasons:

- The imprecision in the modeling of problems makes the latter well describable by fuzzy logic.
- The information in possession regarding the problem under analysis can be affected by uncertainty and therefore it is natural to describe it using

fuzzy logic.

- In the event that the information regarding the problem under analysis is accurate, it may be too complex or expensive to obtain results with a high degree of accuracy. In these circumstances it may be convenient to address the issue through fuzzy logic.

As systems become increasingly complex, reliability analyses play an increasingly important role in the proper development of the system; however, they too are becoming more and more articulated. Much of the problem lies in the uncertainty in the design phase, in fact during the early stages of development the customer's needs are not too clear and the requirements and specifications are usually incomplete. This uncertainty is gradually resolved as the project develops through the various stages, from conception to completion. In the case of reliability, the uncertainty is also due to the fact that failures are relatively rare events (typically only a few per million hours of operation) and collecting enough data on which to base a statistical "probability of failure" turns out to be an expensive and difficult operation. Moreover, especially at the initial stage of design, the object that the probability of failure is often untraceable, and this probability must be "estimated" based on a "technical judgment" or on the knowledge one has of "similar" articles. Deriving these probabilities of failure through statistical methods and then calculating the reliability of a level of the system further increases the uncertainty. By allowing inaccuracy and rough analysis fuzzy logic helps restore the integrity of reliability analysis by introducing uncertainty and not forcing accuracy where this is not possible [22].

2.2 Fuzzy theory

In the classical forms of the Probabilistic Risk Assessment (PRA) approaches, failure rates, failure probabilities or other numerical data related to the failure behavior of system components are usually considered known. But in large and complex systems, not all such data is known due to limited observation and scarcity of statistical data.

This situation is especially relevant in the early design stages, when the requirements and specifications of system components are incomplete, and in the case of new and complex software components. The failure probability of a relatively new component with insufficient historical failure data could, in theory, be estimated based on expert judgment experience from similar components. Consequently, system safety and reliability could be evaluated based on generic statistical data, which may be taken from existing reliability databases. However, the use of generic data will add further uncertainty and imprecision to the results of the analysis.

By allowing imprecision and approximate analysis, fuzzy logic enables incorporating uncertainty in the analysis [23]. Fuzzy set theory was firstly used in FTA (Fault Tree Analysis) for system reliability analysis in [24]. Since then, a number of researchers have developed different fuzzy set theory-based FTA methodologies for system safety and reliability analysis, and many researchers have used these methodologies in a variety of application areas such as nuclear power plants, the process industries etc. Fuzzy set theory has also been applied in conjunction with dynamic extensions of the fault trees [25], [26]. The application of fuzzy set theory in safety and reliability engineering has been extended to FMEA [27], [28], Event tree analysis (ETA) [29], [30], Bayesian networks [31], [32], and Markov chain [33], [34].

2.2.1 Brief overview

Fuzzy theory was firstly introduced by Professor Lotfi A. Zadeh in 1965 [20] to handle the concept of partial-truth values between "completely true" and "completely false". A fuzzy set A is usually expressed in terms of its membership function μ_A which maps domain elements (x) in their respective degrees of belonging in the interval from 0 to 1, as follow [35], [36]:

$$\mathrm{A} = \{(x, \mu_A(x)) \mid x \in X\} \tag{2.1}$$

$$\mu_A(x): X \rightarrow [0,\ 1] \tag{2.2}$$

The strength of fuzzy is intrinsically correlated to equation (2.2), in fact the possibility of assessing a degree of membership that is not fixed to 0 or 1 but could varies within a range between “false” to “true” allows to achieve several advantages in reliability engineering.

Fuzzy is flexible and conceptually easy to understand, it introduces linguistic terminology and it allows to work with approximate values as well as incomplete or ambiguous data [21], [22].

An intuitive description of fuzzy theory and its differences with classical Boolean theory is given in figure 2.1, where the fuzziness concept is illustrated as shades of grey between white ("0" or false) and black ("1" or true).

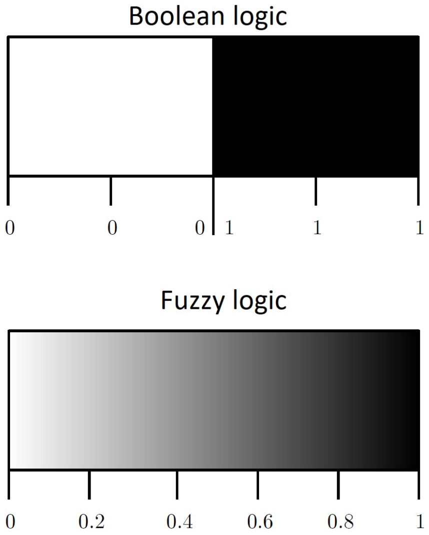


Fig. 2. 1 - Graphical comparison between Boolean logic (on the top side) and Fuzzy logic (on the bottom side)

2.2.2 Fuzzy sets and membership functions

Classical sets contain objects that satisfy precise properties of membership; fuzzy sets contain objects that satisfy imprecise properties of membership, that is, membership of an object in a fuzzy set can be approximate. For example, the set of heights from 1 to 2m is precise (crisp); the set of heights in the region around 6 feet is imprecise, or fuzzy. In general, given an exhaustive collection of individual elements x, which make up a universe of information X and various combinations of these individual elements on the universe A (sets), for crisp sets, an element x in the universe X is either a member of some crisp set A or not. This binary issue of membership can be represented mathematically with the indicator function in equation (2.3):

$$X_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases} \tag{2.3}$$

where the symbol $X_A(x)$ gives the indication of an unambiguous membership of element x in set A, and the symbols $\in$ and $\notin$ denote contained in and not contained in, respectively. The difference between crisp and fuzzy sets is explained in the following example.

In the universe of heights of people, let A be the crisp set of all people with $1\,\mathrm{m} \leq \mathrm{x} \leq 2\,\mathrm{m}$. A particular individual, x_1, has a height of 1.5 m. The membership of this individual in crisp set A is equal to 1, or full membership, given symbolically as $X_A(x_1) = 1$. Taking another individual as an example, x_2, has a height of 0.99 m. The membership of this individual in set A is equal to 0, or no membership, hence $X_A(x_2) = 0$, as shown in the left chart in Figure 2.2. In these cases, the membership in a set is binary, either an element is a member of a set, or it is not.

Zadeh extended the notion of binary membership to accommodate various "degrees of membership" on the real continuous interval [0, 1], where the endpoints of 0 and 1 conform to no membership and full membership, respectively, just as the indicator function does for crisp sets. However, the infinite number of values between the endpoints can represent various degrees of membership for an element x in some set on the universe. The sets on the universe X that can accommodate "degrees of membership" were defined by Zadeh as fuzzy sets. Continuing further on the example on heights, let H be the set of heights near 1.5 m. Since the said property is fuzzy, there is no unique membership function (MF) for the set H.

Properties of this function might be:

1. normality: $\mu_H(1.5) = 1$;
2. monotonicity: the closer H is to 1.5 m the closer μ_H is to 1;
3. symmetry: numbers equidistant from 1.5 m should have the same value of μ_H.

Such concept of fuzzy MF is shown in the right chart in Figure 2.2. A key difference between crisp and fuzzy sets is thus their membership function; a crisp set has a unique membership function, whereas a fuzzy set can have an infinite number of membership functions to represent it. For fuzzy sets, the uniqueness is sacrificed, but flexibility is gained because the membership function can be adjusted to maximize the utility for a particular application.

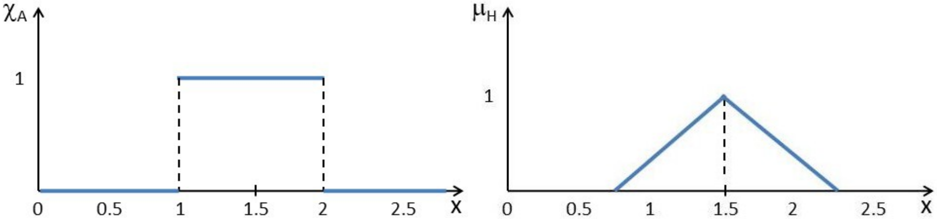


Fig. 2. 2 - Height membership functions for a crisp set A (left plot) and a fuzzy set H (right plot).

In the case where the membership function uniquely takes on the values 0 or 1, it reduces the fuzzy set to a crisp set, so it is deduced that classical crisp sets are special cases (i.e. subsets) of fuzzy sets.

It is easy to see how fuzzy set theory is extremely flexible and can be adapted to a wide variety of industrial applications. In the case of fuzzy sets, precision is sacrificed, but there is a gain in flexibility since the trend of the function to which it belongs can be chosen based on the context.

Among the different forms that the functions of belonging to fuzzy sets can take on, trapezoidal and triangular ones are widely used in reliability engineering to represent the blurred failure rates of system components or even the risk indices of an FMECA analysis.

a) Triangular fuzzy numbers

Let X be a collection of object universe and its elements are represented by x. As already said, a fuzzy set A in X can be characterized by a membership function $\mu_A : X \rightarrow [0, 1]$. The value of function $\mu_A(x)$ represents the degree of membership of x in A. A membership value 1 means the element is completely in set A and 0 means the element is completely not in set A. On the other hand, values between 0 and 1 represent the partial membership, where the higher the value the stronger the degree of membership is. A fuzzy number is a special type of fuzzy set and could be defined in different forms depending on the nature of the problem in hand [36]. Among different shape of membership functions, the triangular shapes is widely used in reliability engineering to represent fuzzy failure rates or probabilities of system components.

Let x, a1, a2, a3 ∈ R. A triangular fuzzy number A could be defined by the membership function μ_A as follows

$$\mu_A(x) = \begin{cases} \dfrac{x-a}{b-a} & for\ a < x < b \\ \dfrac{c-x}{c-b} & for\ b \leq x < c \\ 0 & otherwise \end{cases} \tag{2.4}$$

In the triangular fuzzy number, A = (a, b, c), the element b gives the maximal degree of membership, i.e., $\mu_A(b) = 1$. At the same time, a_1 and a_3 are the lower and upper bound of the evaluation data, respectively.

An example of triangular fuzzy number according to equation (2.4) is shown in Figure 2.3.

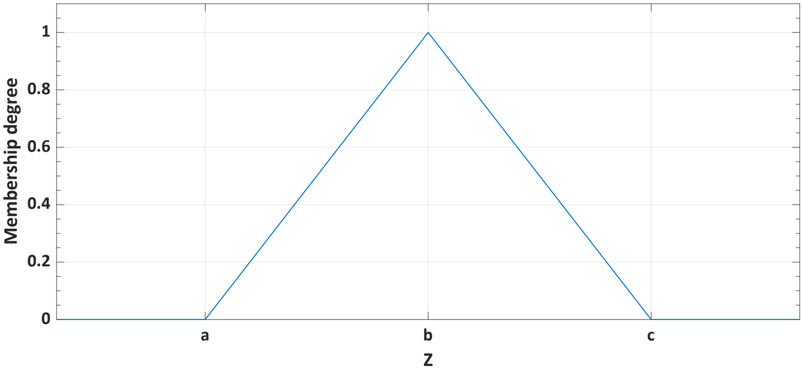


Fig. 2. 3 - Example of triangular membership function.

b) Trapezoidal fuzzy numbers

Let $z, a\, b, c, d\ \in \mathbb{R}$. A trapezoidal fuzzy number A_i can be defined by the membership function μ_{A_1}, as follows:

$$\mu_{A_1}(z) = \begin{cases} \dfrac{z-a}{b-a}\ if\ a\ < z < b \\ 1\quad if\ b \leq z < c \\ \dfrac{d-z}{d-c}\ if\ c \leq z < d \\ 0\quad otherwise \end{cases} \tag{2.5}$$

Usually, trapezoidal fuzzy number are represented using the following notation: $A_1 = (a, b, c, d)$.

An example of trapezoidal fuzzy number is shown in Figure 2.4.

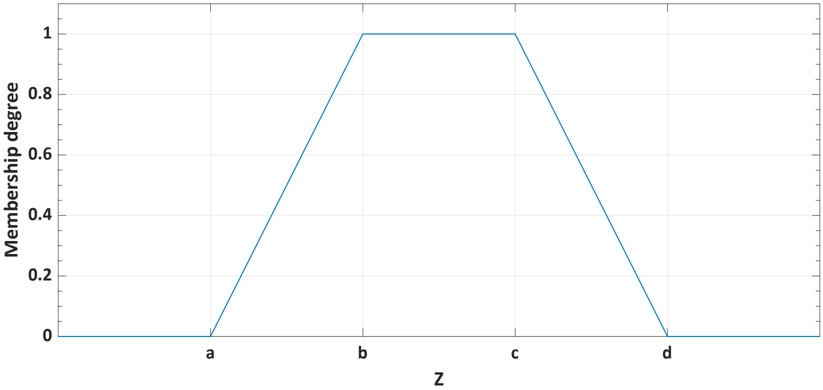


Fig. 2. 4 - Example of trapezoidal membership function.

2.2.3 Operations between fuzzy numbers

Consider two triangular fuzzy numbers A = (a_1, a_2, a_3) and B = (b_1, b_2, b_3). The possible arithmetic operations that can be performed on A and B are described by the following relationships [37], [38]:

$$Sum: A + B = (a_1 + b_1, a_2 + b_2, a_3 + b_3) \tag{2.6}$$

$$Difference: A - B = (a_1 - b_1, a_2 - \ b_2, a_3 - \ b_3) \tag{2.7}$$

$$Product: A \cdot B = (a_1 b_1, a_2 b_2, a_3 b_3) \tag{2.8}$$

$$Division: \frac{A}{B} = \left(\frac{a_1}{b_3}, \frac{a_2}{b_2}, \frac{a_3}{b_1}\right) \tag{2.9}$$

The results of the above equations are approximation performed for triangular fuzzy number in compliance with [37], [38]. Similar considerations can be drawn for trapezoidal fuzzy numbers. Let assumes C = (c_1, c_2, c_3, c_4) and D = (d_1, d_2, d_3, d_4). Thus, the base operations can be summarized as follow:

$$Sum: C + D = (c_1 + d_1, c_2 + d_2, c_3 + d_3, c_4 + d_4) \tag{2.10}$$

$$Difference: C - D = (c_1 - d_1, c_2 - d_2, c_3 - d_3, c_4 - d_4) \tag{2.11}$$

$$Product: C \cdot D = (c_1 \cdot d_1, c_2 \cdot d_2, c_3 \cdot d_3, c_4 \cdot d_4) \tag{2.12}$$

$$Division: \frac{C}{D} = \left(\frac{c_1}{d_4}, \frac{c_2}{d_3}, \frac{c_3}{d_2}, \frac{c_4}{d_1}\right) \tag{2.13}$$

2.2.4 Defuzzification

Generically it is necessary to convert the fuzzy number into a crisp number in order to be able to compare the results achieved with a fuzzy model against the results of a crisp model. This process is called defuzzification, which can be performed using different techniques [39]. The most widely used approach in reliability engineering is the centroid defuzzification or center of gravity method. Considering a triangular fuzzy number A=(a$_1$, a$_2$, a$_3$), its defuzzified value is obtained as shown in the equation (2.14).

$$z_0(A) = \frac{\int_{a_1}^{a_3} z\,\mu_A(z)\,dz}{\int_{a_1}^{a_3} \mu_A(z)\,dz} = \frac{a_1 + a_2 + a_3}{3} \qquad (2.14)$$

2.3 Fuzzy inference systems

Fuzzy inference is the process of mapping input variables to outgoing variables using a deduction mechanism based on fuzzy logic, which consists of If-Then rules, membership functions, and fuzzy logical operations. In the fuzzy inference process, If-Then rules form the deduction mechanism that indicates how to link input variables with output variables. A simple example of If-Then rule is the following:

If x is X, then y is Y

The first part of the rule is called *antecedent*, while the rest of the sentence is called *consequent*, where *x* and *y* are the input and output of the rule, respectively. The reason why If-Then statements are widely used lies in the fact that they are very similar to human reasoning [40], since they are based on adjectives and linguistic values. In the literature there are three different methodologies of fuzzy inference: that of Mamdani, that of Sugeno and finally that of Tsukamoto[17], [41]. All these techniques can be divided into two main stages. The first phase consists in the fuzzification of the input variables in appropriate functions of belonging (triangular, trapezoidal, Gaussian, etc.) and in the drafting of the rules. It is identical for all three inference techniques.

The second step is to aggregate the results of all If-Then rules to provide a single output value. In Mamdani inference the result of applying an If-Then rule is a fuzzy set. The results of all the rules are then aggregated in order to form a single fuzzy set, which is subsequently defuzzified. In the case of Sugeno inference, the result of the If-Then rule is a polynomial, from which a crisp number is obtained. Also in this case the results of each rule are aggregated in order to obtain a single output. Although Sugeno inference does not require the computationally burdensome process of defuzzification, the determination of polynomial parameters is complex and less intuitive than defining fuzzy sets characteristic of Mamdani inference. Finally, Tsukamoto's inference consists of a combination of the other two methods, but it is very complex and, consequently, has had limited expansion. It is therefore evident that the technique of inference most used in the literature is that of Mamdani, which has therefore been applied in this thesis work. This method is based on six steps that will be analyzed below, using an example of FMECA analysis.

Step 1: Choosing membership functions for input and output variables. Consider determining the amount of the RPN value of a given failure mode. The input variables are therefore: Severity, Detection and Occurrence. The first step of the method is to associate a number of membership functions defined in the range [1,10] to these variables. Each MF is identified by linguistic values that will then be used to determine the If-Then rules. Fig. 2.5-2.7 illustrates some examples of MFs for the Severity, Detection and Occurrence input.

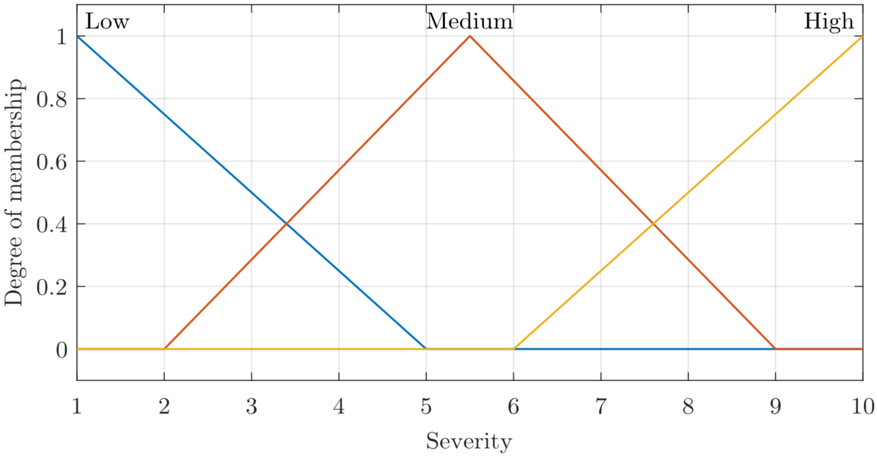


Fig. 2. 5 - Example of membership functions for Severity.

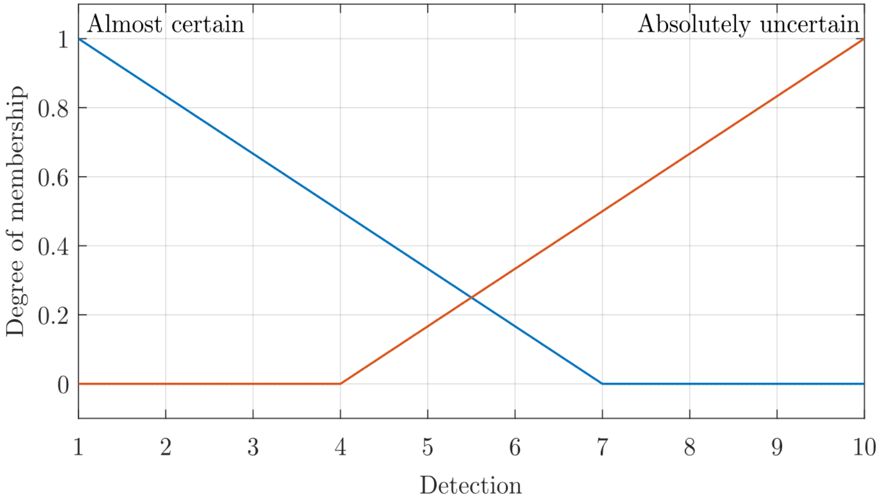


Fig. 2. 6 -Example of membership functions for Detection.

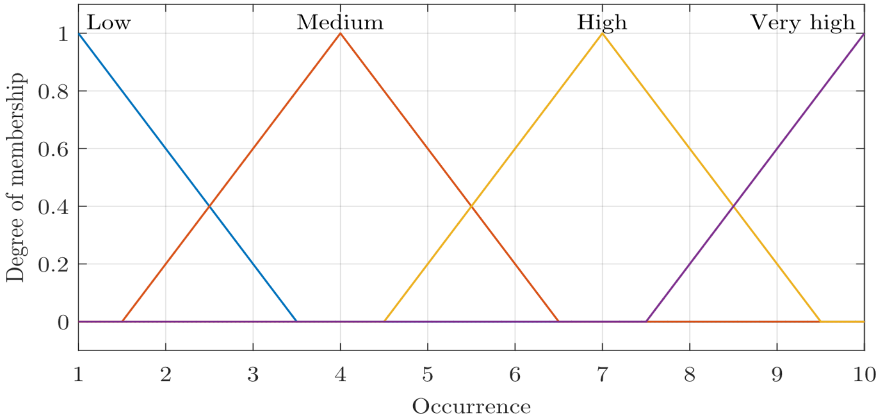


Fig. 2. 7 - Example of membership functions for occurrence.

The MFs of Fig. 2.5-2.7 have been obtained through the use of matlab's Fuzzy Logic Toolbox. The tool provides a graphical user interface (GUI) that allows the programming of an inference system (FIS Fuzzy Inference System) according to the user's needs.

The same procedure must also be applied to the output variable, which in this case is the RPN value (varying in the domain 1 - 1000), as shown in Fig.2.8.

The inference system is described using the block diagram in Fig.2.9. In particular, it is important to specify that, as already mentioned above, the output of the Mamdani inference process is a fuzzy number and, for this reason, it is assigned the name of FRPN (Fuzzy Risk Priority Number).

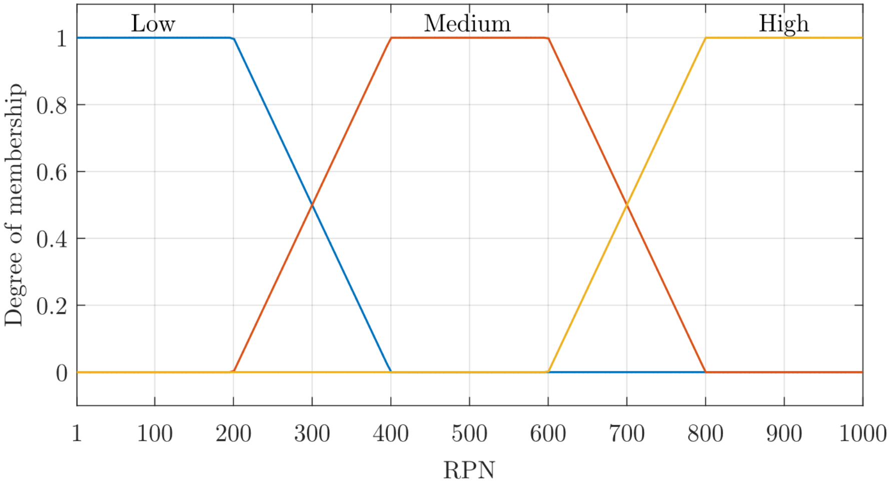


Fig. 2. 8 -Example of membership functions for the RPN.

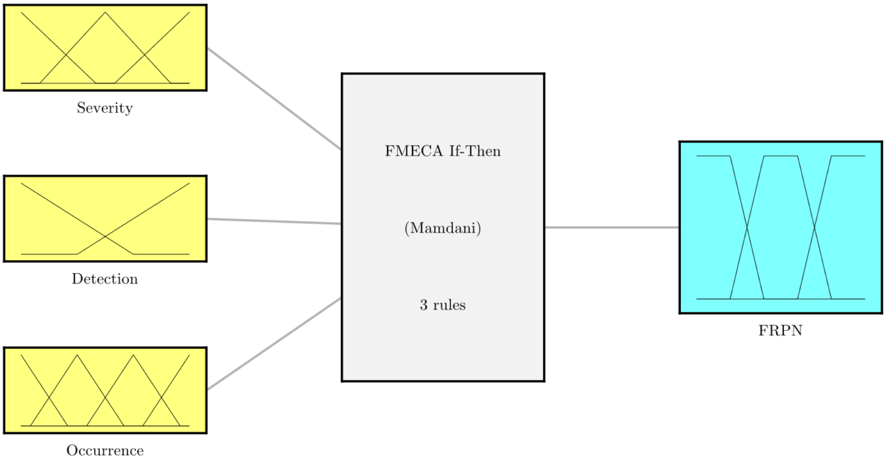


Fig. 2. 9 -Block diagram of the inference system.

Step 2: Definition of If-Then rules.

In this phase, the input variables are connected with the output variables through the drafting of simple rules. As for the example taken into consideration, rules can be defined such as:

If (**Severity** is **Low**) *and* (**Detection** is **Almost certain**) *and* (**Occurrence** is **Low**) *then* (**FRPN** is **Low**);

If (**Severity** is **Medium**) *and* (**Detection** is **Almost certain**) *and* (**Occurrence** is **Medium**) *then* (**FRPN** is **Medium**);

If (**Severity** is **High**) *and* (**Detection** is **Absolutely uncertain**) *and* (**Occurrence** is **High**) *then* (**FRPN** is **High**).

Step 3: Fuzzy operator application (AND, OR).

Since fuzzy logic is an extension of Boolean logic, in which the values of belonging are always 1 (completely true) or 0 (completely false), it must admit the same logical operations provided by Boolean logic as AND and OR. In fuzzy logic, unlike Boolean logic, operands A and B are degrees of belonging within the range [0,1]. According to [37], [38] the logic operator AND can be approximated to the minimum function when the fuzzy logic is consider. Quite the opposite, the logic operator OR is described by the maximum function. Thus:

$$A\ AND\ B = \ min\ (A, B) \tag{1.10}$$

$$A\ OR\ B\ = max\ (A, B) \tag{2.11}$$

Step 4: Application of the implication method (Then).

The input for the implication process is the result of the application of the fuzzy operator (in case of the AND operator this is the minimum degree of belonging of the crisp inputs to their membership functions) and is consequently a defined number, while the output, according to Mamdani's inference model, is a fuzzy number.

The implication is implemented for each rule and the most used method in the literature to perform it is that of truncation, which reduces the output fuzzy set to the value provided by *the antecedent,* as shown in Fig.2.10. In other words, if the rule is verified completely or in part (that is, if the indices fall within the three functions of belonging that make up the *previous*), then the relative function of output membership will be verified up to the level selected by the logical operation of AND (area in blue).

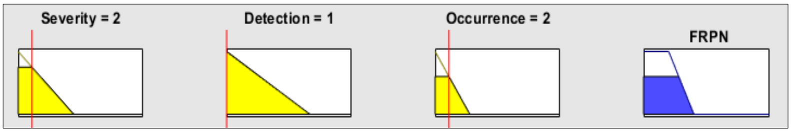


Fig. 2. 10 - Application of the implication method.

Step 5: Aggregation of results.

Since the overall result is based on the verification of all the rules, the outputs must necessarily be aggregated. As already mentioned, the output of each rule corresponds to a fuzzy number, so the aggregation will also give rise to a fuzzy number. The most used method to perform the aggregation is the maximum, which combines the outputs of each rule, as shown in Fig.2.11.

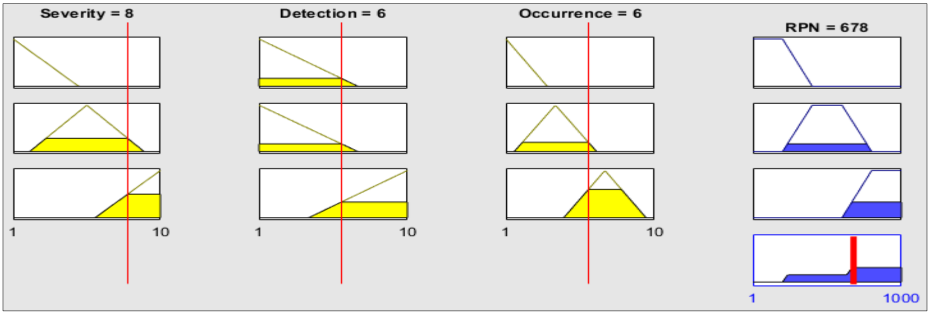


Fig. 2. 11 -Aggregation of the results in a fuzzy if-then inference system.

Step 6: Defuzzification.

Since the result of the aggregation is a fuzzy number, it is necessary to proceed with the defuzzification in order to obtain the crisp RPN. This value (shown in Fig.2.11 with a thick red line) is obtained by the center of gravity method.

The FMECA If-Then described in this paragraph allows to solve the problems of traditional FMECA, in fact the RPN is no longer calculated through the product between S, D and O but through an inference process that uses membership functions and If-Then rules. This method is therefore a hybrid technique as it allows to calculate the RPN through a fuzzy process starting from crisp values of S, D and O. The drafting of the If-Then rules allows you to provide a prioritization of the indices in order to overcome the inherent limitations of the traditional FMECA. Typically, in Safety-Related applications, the highest priority is assigned to Severity.

The great advantage of this technique lies in its applicability to any existing FMECA analysis.

Chapter 3

Risk based maintenance

This chapter deals with a powerful tool for maintenance planning, called Reliability Centred Maintenance. The chapter introduces a fuzzy-RCM to overcome the high subjective decision making of the classical procedure. Furthermore, the work also focuses on the optimization of a FMECA procedure, which is the core of RCM. Trying to solve the drawbacks of the classical FMECA, a fuzzy-FMECA and a new threshold estimation method are presented. The fuzzy approach allows to solve all the major problems of the RPN, while the threshold estimation method allows to distinguish critical and negligible failure modes with a simple, quantitative, objective and effective solution [1, 2, 3].

[1] The fuzzy-based RCM has been published as "L. Ciani, G. Guidi, G. Patrizi, and D. Galar, "Condition-Based Maintenance of HVAC on a High-Speed Train for Fault Detection," Electronics, vol. 10, no. 12, p. 1418, Jun. 2021."

[2] The fuzzy FMECA has been published as "L. Ciani, G. Guidi, and G. Patrizi, "Fuzzy-based approach to solve classical RPN drawbacks for railway signaling systems," IEEE Intelligent Transportation System Magazine, Article in Press, 2021."

[3] The RPN thresholds has been published as "M. Catelani, L. Ciani, D. Galar, G. Guidi, S. Matucci, and G. Patrizi, "FMECA assessment for railway safety-critical systems investigating a new risk threshold method," IEEE Access, vol. 9, pp. 86243–86253, 2021"

3.1 Introduction

Industrial production, driven by global competition, and radical advances are required in manufacturing technology if companies want to keep up. Industry 4.0 is transforming industrial manufacturing through digitalization and other new technologies (see for instance [42]–[46]). A main objective is reducing downtime by optimizing maintenance policies [47]–[51]. Reliability centered maintenance (RCM) is a method used to identify and select failure management policies, including maintenance activities, operational changes, design modifications or other actions to mitigate the consequences of failure [52]. RCM provides a decision process to identify applicable and effective preventive maintenance requirements or management actions to prevent the safety, operational and economic consequences of failures and identify the degradation mechanism responsible for those failures. The most important but challenging parts of the RCM process are failure mode effect and criticality analysis (FMECA) and task selection. FMECA is developed using the subjective knowledge of domain experts (for more reference about FMECA see for instance but not only [53]–[56]).

Meanwhile, the decision diagram proposed by the international standard IEC 60300-3-11 [52] for task selection is very generic, and the task choice mostly relies on the experience of the analyst that performs the RCM [57]. The classical risk priority number (RPN), output of the FMECA, also has many drawbacks, including gaps in the range, duplicates, subjectivity and dispersion [58]. Despite these disadvantages, RCM is a powerful solution, widely used in every industrial field in which service continuity represents a mandatory requirement, and maintenance must be optimized in terms of money and time [59].

The main contribution about this topic is the introduction of a fuzzy-based decision-making diagram to guide the selection of the optimal maintenance task within the Reliability-Centred Maintenance procedure. The proposed procedure allows to rapidly, easily, uniquely, and unambiguously identify the optimal maintenance policy, while the classical RCM procedure leads the analyst to multiple choices requiring a high subjectivity in the definition. Moreover, the methodology presented in this work is a diagnostic-oriented decision-diagram that whenever is possible prefer the choice of condition-based maintenance such as condition monitoring and failure finding procedure.

3.2 Reliability centered maintenance

Reliability centered maintenance is an effective way to select the appropriate maintenance policies for every type of system.

In compliance with the international standard IEC 60300-3-11, the classical RCM process is a structured procedure which could be divided into five steps [52]:

1. Initiation and planning: In this phase it is essential to establish a plan of the analysis and to identify the actual operating context of each item.
2. Functional failure analysis: This phase is implemented to understund the failure modes related to each item. For each one of them, failure causes and failure effects have to be identified before carrying out a complete criticality assessment of each component in compliance with FMECA procedure.
3. Task selection: This phase is used to select the appropriate maintenance task and the correct maintenance interval for each one of the identified failure modes. The standard IEC 60300-3-11 provide a dedicated decision-diagram to guide the maintenance task selection phase.
4. Implementation. During the life cycle of the system under analysis, the identified maintenance policies must be implemented accordingly.
5. Continuous improvement: This final step is a circular phase used to monitor the effectiveness of the maintenance plan and to ensure continuous improvement to the procedure optimizing step 2 and step 3 according to data acquired during implementation phase.

The most critical step of the classical RCM procedure is the selection of the maintenance task (Phase 3.). In compliance with international standard IEC60300-3-11 [52], Figure 3.1 shows how to guide the maintenance task selection in order to identify the optimal maintenance solution for the system under test. The maintenance decision-diagram aims to simplify the assessment of the optimal maintenance tasks.

The maintenance policy choice depends only on two conditions: if the failure is evident or not and if the failure will involve consequences on the safety level of the system under test. However, at least four possible task options are given in each orange box in Figure 3.1; this means that the international standard gives the designer a high level of subjectivity. Overall, the diagram is very generic and doesn't lead to a unique task choice; the designer is free to choose one or another option, based only on his or her expertise.

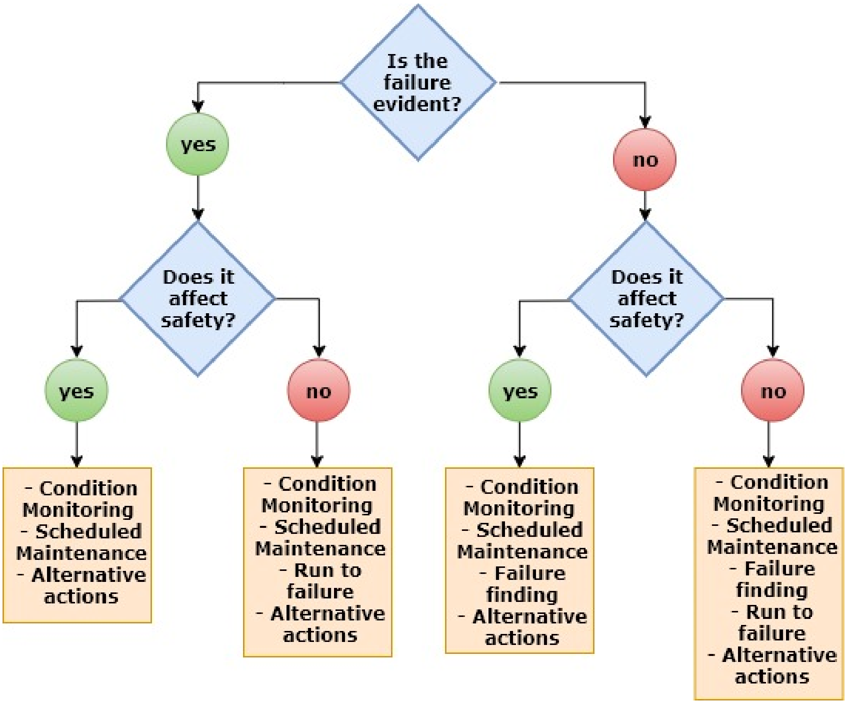

Is the failure evident?
yes
no
Does it affect safety?
yes
no
- Condition Monitoring - Scheduled Maintenance - Alternative actions
- Condition Monitoring - Scheduled Maintenance - Run to failure - Alternative actions
Does it affect safety?
yes
no
- Condition Monitoring - Scheduled Maintenance - Failure finding - Alternative actions
- Condition Monitoring - Scheduled Maintenance - Failure finding - Run to failure - Alternative actions

Fig. 3. 1 - Maintenance decision-diagram of classical RCM procedure according to International standard IEC 60300-3-11.

All possible maintenance tasks taken into account by the standard are explained as follows:

- Failure finding is applicable only to hidden failure. This task can either be an inspection or a function test to determine whether an item would still perform its required function if demanded [60].
- Scheduled maintenance is divided into scheduled restoration and scheduled replacement. This task consists of scheduled refurbishment or replacement of an item or its components.
- Condition monitoring is a continuous task which allows users to detect the health state of the system by monitoring some contextual parameter that could indicate the degradation and wear-out of the monitored item. Condition monitoring is able to indicate that the failure mode can be expected to occur if no corrective action is taken

[61], [62].

- No preventive maintenance is done if no maintenance action is required (i.e. Run to Failure).
- Alternative actions may be performed, as suggested by the designers and maintenance experts.

3.3 Related works about RCM

This section presents the results of an extensive literature review regarding innovative RCM procedure proposed in recent literature.

Some researchers propose an effective RCM assessment using reliability software [63]. In [64] the RCM is applied to the whole system under test instead of focusing on individual components. Others papers use analytical models and a dynamic approach [65], [66], while some authors create their own framework for maintenance decision making [67], [68]. Zakikhani et al. [69] proposes an availability-based RCM, while in [70] a whole dependability study (RAMS) is introduced to optimize maintenance policy. In [71] the variation trends of the failure rates of components under imperfect maintenance are used to optimize the maintenance of metro trains based on the concept of RCM. Afzali et al. [72] proposes a weighted importance reliability index model to prioritize the components in a complete RCM report. In [73] a stochastic RCM is proposed, while other papers introduce genetic algorithms to solve the mathematical problem of RCM optimization [74], [75].

Starting from a preliminary work presented in [76], this thesis proposes a new approach based on fuzzy set theory to overcome the limitations of traditional FMECA and RCM. It provides a customized decision diagram that uses fuzzy inference rules to mitigate the subjectivity problem of the classical procedure. The three parameters of the criticality analysis are fuzzified using appropriate membership functions; the resulting RPN given by the product of the three indices is a fuzzy number. The proposed decision diagram for the task selection is based on the fuzzy occurrence, severity and detection scores combined with other failure information using a set of if-then rules, one of the most frequently used and efficient fuzzy inference approaches [77]–[79].

3.4 Fuzzy-based RCM: the Proposed approach

FMECA, based on the fuzzy set theory approach, has been used in a variety of engineering fields to eliminate the drawbacks explained in the introduction section [58], [80]–[82]. In this paper, fuzzy logic is used not only to enhance the features of FMECA and RPN but also to introduce a new approach to maintenance decision-making. The first step to be performed is a classical failure modes and effects analysis (FMEA) to identify the failure modes, failure causes and failure effects of every components making up the system. The aim of FMEA is to highlight all the criticalities of the system, the causes that could lead to them and all the possible consequences. The second step is to define the linguistic variables of the three risk parameters, occurrence (O), severity (S) and detection (D), and rank them using fuzzy numbers instead of crisp numbers. The O, S and D indices can be divided into several linguistic terms, each identifiable by a different value. A three-value linguistic scale is used in the proposed approach, and each term is fully described in Table 3.1.

Tab. 3. 1- Linguistic definition for Occurrence O, Severity S and Detection D used in the proposed method.

Occurrence (O)	Severity (S)	Detection (D)
Remote (R) – the mode has a remote probability of occurring	**Very low (VL)** - the mode has low/no impact on the system	**Almost certain (AC)** – the mode will almost certainly be detected
Probable (P) – the mode has a medium probability of occurring	**Tolerable (T)** – the mode causes deterioration in the system	**Medium (M)** – the mode will probably be detected
High (H) – the mode will likely occur	**Critical (C)** – the mode leads to serious damage in the system	**Absolutely uncertain (AU)** – the mode will hardly be detected

The indices are transformed into fuzzy numbers via membership functions. All membership functions are trapezoidal. Figure 3.2 shows the membership functions related to Occurrence, Figure 3.3 highlights the Severity membership functions and Figure 3.4 illustrates the membership functions of the Detection.

The main advantage of this approach is that instead of choosing a crisp value within the range from 1 to 10 for each parameter, the designer can choose one of the three linguistic terms. This leads to a better accuracy and a less subjective assessment of the risk level because expert judgment now relies on the linguistic terms.

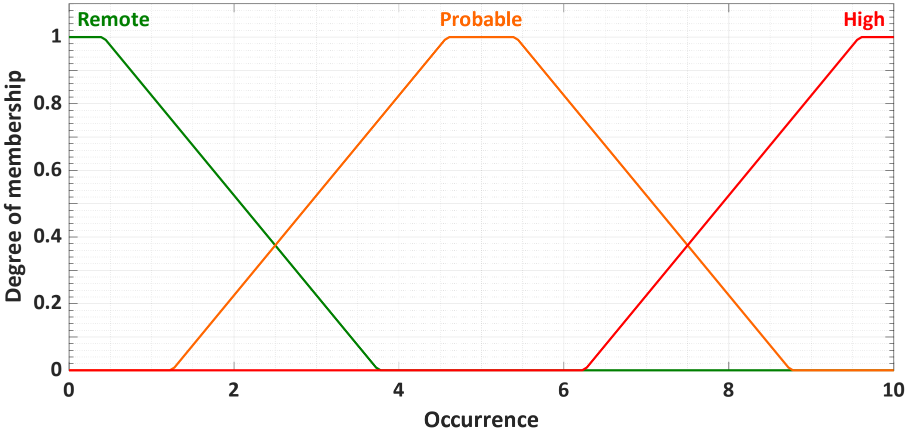


Fig. 3. 2 - Membership functions for occurrence O: “Remote (R)”, “Probable (P)”, “High (H)”.

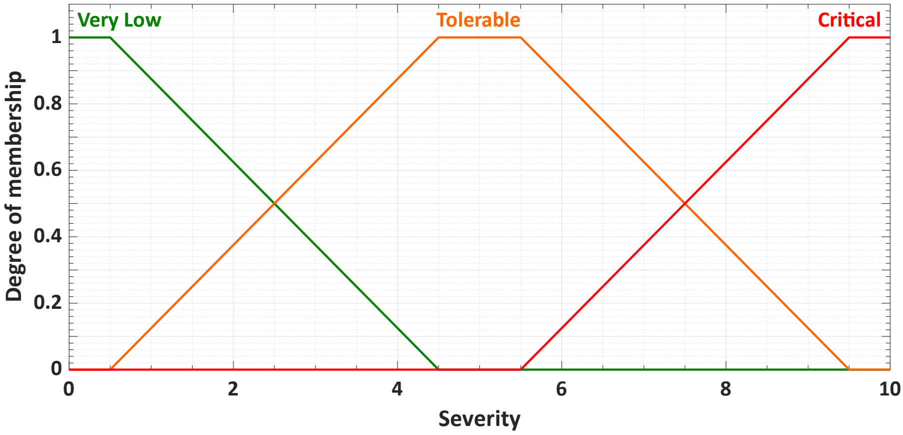


Fig. 3. 3- Membership functions for severity S: “Very Low (VL)”, “Tolerable (T)”, “Critical (C)”.

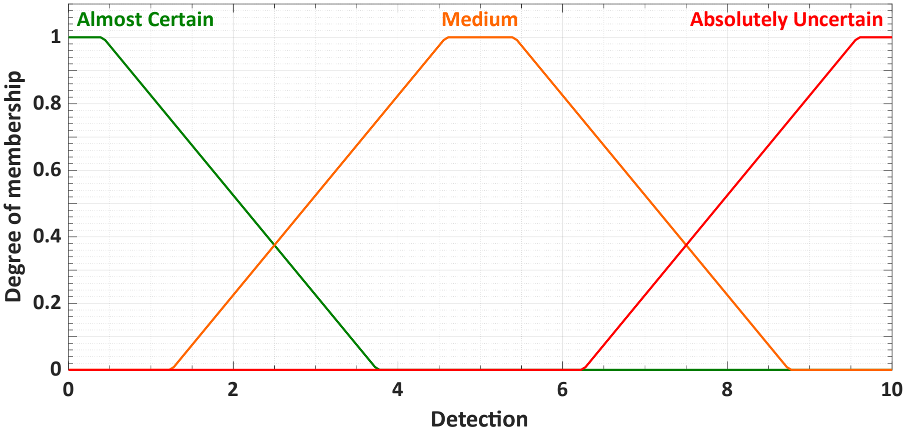


Fig. 3. 4- Membership functions for detection D: "Almost Certain (AC)", "Medium (M)" and "Absolutely Uncertain (AU)".

After the assessment of O, S, D, the fuzzy FMECA procedure requires the evaluation of the fuzzy risk priority number (RPN) using, for example, if-then rules (see, among others [77], [79], [83]), weighted geometric mean [84], OWA operator [85], TOPSIS theory [86] or multicriteria decision method [82]. In this paper, fuzzy if-then rules are used to calculate the Fuzzy risk Priority Number FRPN. Moreover, the proposed procedure focuses on the development of a new maintenance decision-diagram.

The new customized diagram is shown in Figure 3.5. In the diagram, the membership functions of O, S and D are identified by different colors, as in Figures 3.2, 3.3 and 3.4.

The proposed maintenance decision-diagram is a diagnostic-oriented approach which favor the choice of condition-based maintenance whenever a diagnostic system is applicable. Therefore, the membership function of the Detection variable plays a fundamental role in the procedure. For instance, if Detection is "Almost Certain - AC" then the proposed procedure suggests the implementation of condition monitoring to diagnose the health-state of the system and consequently optimize the maintenance policy based on the system's actual conditions.

For the sake of simplicity, the linguistic variables which define each membership function in Fig. 3.5 are abbreviated using only the first letter of each word, as in the captions of Figures 3.2 to 3.4 (or alternatively as described in Table 3.1). Different colors have been used to identify the different membership functions.

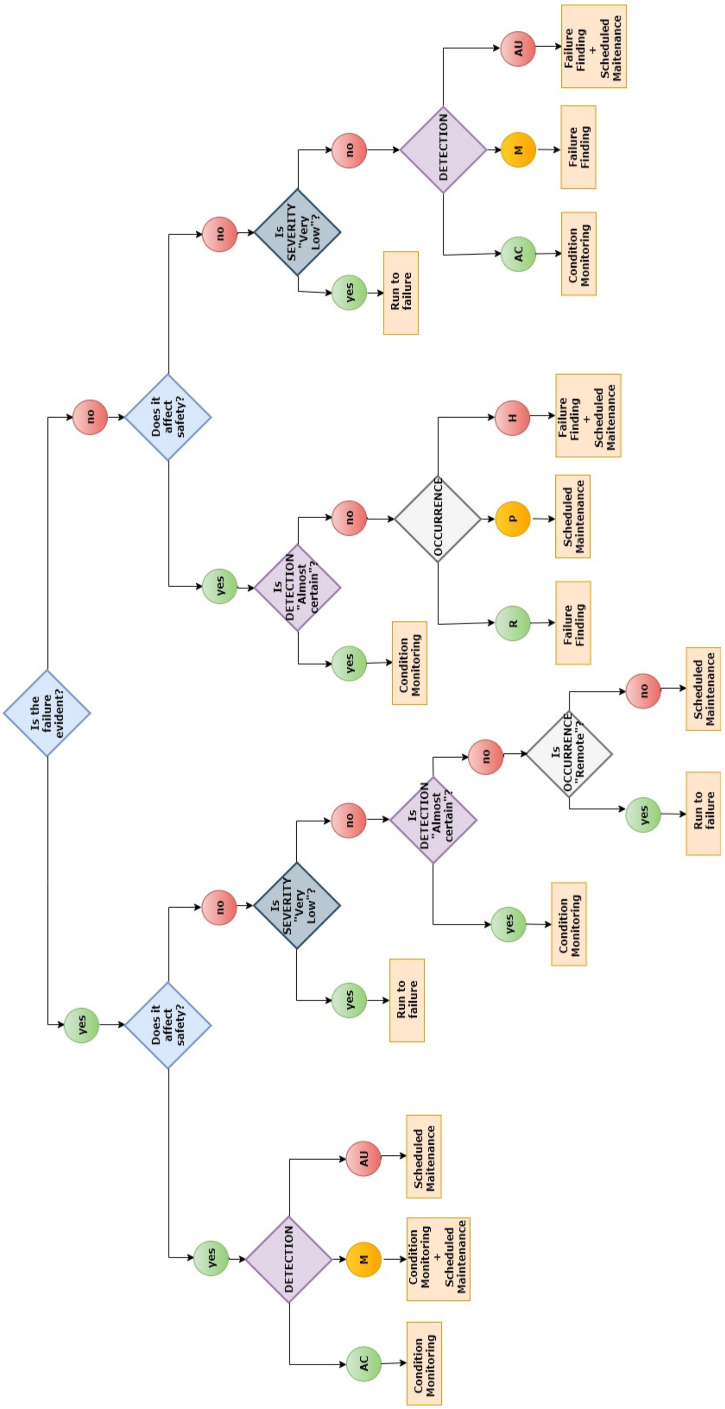


Fig. 3. 5 - Proposed maintenance decision-diagram to assess optimal maintenance task using fuzzy logic.

The information necessary to carry out the proposed procedure as in Fig. 3.5 are the following:

- Whether the failure is hidden or evident.
- Whether the failure has safety consequences on the system.
- What the membership functions of occurrence, severity and detection are.

Based on the answer of such inputs, the proposed decision diagram provides a univocal output, so that each set of inputs leads to a specific maintenance task choice. Designer subjectivity is minimized, and the task is selected in a more deductive and rational way. Furthermore, the proposed methodology is still compliant to the requirements and suggestions of the RCM international standard IEC 60300-3-11. In fact, the top side of the tree remains the same as the decision-diagram proposed in then international standard (see Fig. 3.1). The proposed procedure improves the bottom side of the tree introducing the fuzzy linguistic variables to provide a univocal and unique maintenance choice for each analyzed failure mode.

The decision-diagram proposed in Figure 3.5 could be automatized implementing a set of fuzzy-based if-then rules. Usually, the fuzzy "if-then" procedures presented in literature are solved using one of the following three types of fuzzy inferences. The Mamdani inference firstly proposed in [17] results in an aggregation of fuzzy sets that must be defuzzied to achieve the crisp output. The Sugeno inference [41] provides a polynomial function that must be solved to obtain the crisp output value. Finally the Tsukamoto inference [87] is a hybrid approach based on the previous ones which has not gain a great popularity in literature. In this work, the Mamdani inference is used since it provides optimal results with low computational complexity as well as easiness of use.

The proposed fuzzy system for maintenance task assessment has five inputs and two outputs. Three inputs (Occurrence, Severity and Detection) are fuzzy variables described by the three trapezoidal membership functions illustrated in Table 3. 1 and discussed above. The other two inputs are simple Boolean variables with only two states, "Yes" or "No". One is used to divide the failure into "hidden" or "evident"; the other classifies the failure's impact on safety. In other words, the proposed methodology is implemented using a hybrid system merging Boolean and fuzzy logic through a set of fuzzy if-then rules.

The two outputs of the fuzzy system are:

- The fuzzy risk priority number (FRPN) assessed combining Occurrence O, Severity S and Detection D. The FRPN output achieved with the proposed method is described using six trapezoidal membership functions.
- The optimal maintenance task, which is a linguistic variable assessed using all the five inputs described above. The optimal task choice is selected in compliance with the diagram for maintenance decision-making illustrated in Figure 3.5.

The proposed fuzzy logic system is illustrated in Figure 3.6, highlighting the inputs and the outputs. The inference logic uses nine rules to assess the fuzzy risk priority number and 36 rules to assess the optimal task. Obviously, this number varies if the risk rates O, S and D are described with more membership functions. For the sake of simplicity, this work analyzes the parameters using only three linguistic variables each.

However, it is important to note that when the number of possible linguistic values increases, the accuracy of the approach increases, along with its complexity.

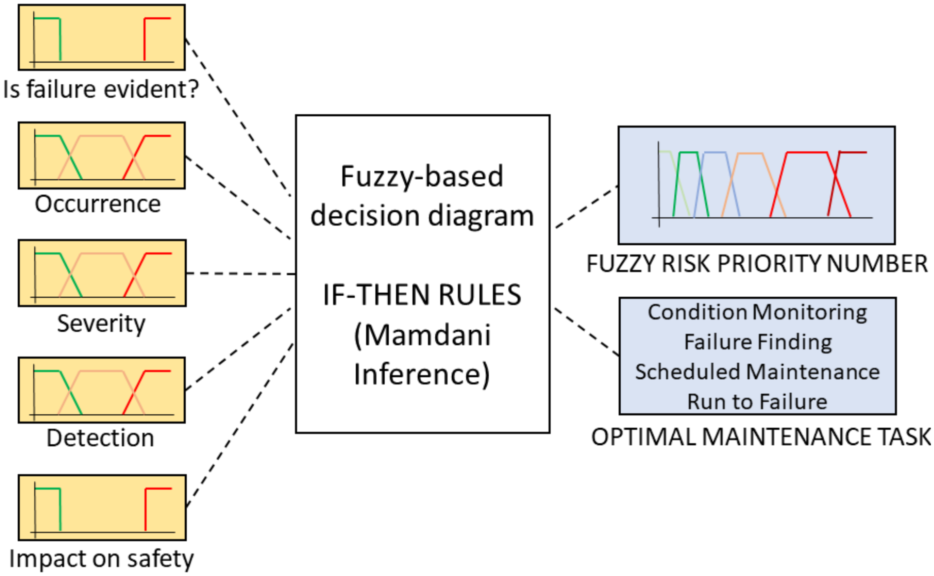


Fig. 3. 6 - Schematic diagram of fuzzy-based RCM assessment using "if-then" rules.

Two of the implemented rules are illustrated below, the first for the FRPN output and the second for the maintenance task selection:

> *If* (Severity is **Critical**) *and* (Detection is **Almost certain**) *and* (Occurrence is **Remote**) *then* (FRPN is **Critical**)
>
> *If* (Failure evident == **YES**) *and* (Impact on Safety == **NO**) *and* (Severity is **Tolerable**) *and* (Detection is **Almost Certain**) *and* (Occurrence is **Remote**) *then* (Optimal task == **Condition Monitoring**)

3.5 Case Study: RCM assessment of HVAC for High-speed trains

In this section, the proposed fuzzy-based RCM approach has been applied to an HVAC system installed on high-speed trains in order to test and validate the performances of the proposed approach. The complete RCM report is not available, however the results achieved for the most critical and complex components of the HVAC are illustrated in the following.

Five components are considered in this paper, namely the compressor, the Electronic Control Card (ECC), the watchdog, the IGBT module (Insulated Gate Bipolar Transistor) and the UPS (Uninterruptible Power Supply). The compressor draws in the cold gases exiting the evaporator battery at low pressure and compresses them, so they come out as overheated gas at high pressure. It includes a motor, a pump, some internal valves, a thermostat etc. The ECC is a microprocessor-based electronic board used to manage all the HVAC functionalities, while the watchdog is used to activate the emergency mode. The IGBT is used to drive the compressor motor in order to ensure cooling capacity, and finally the UPS ensures emergency power in order to guarantee emergency ventilation in case of breakdown of the overhead power line. Table 3.2 shows the failure modes and effects analysis carried out for the five components under analysis.

Tab. 3. 2 - Failure modes and effects analysis (FMEA) for an HVAC system

FAILURE MODES	**FAILURE CAUSES**	**LOCAL EFFECTS**	**GLOBAL EFFECTS**
COMPRESSOR: Increases the pressure of the refrigerant gas			
FM_C1	Motor seize up	Loss of pumping capacity	Loss of cooling capacity in the cabin
	Internal failure		
	Blocked compressor		
	Damage winding		
FM_C2	Overheating of compressor	Loss of protection	Possible damage of compressor
	Thermostat dirty		
FM_C3	Mechanical failure	Loss of refrigerant pumping	Loss of cooling capacity in the cabin
	Fretting compressor		
FM_C4	Internal failure	Loss of refrigerant gas pressure	Loss of cooling capacity in the cabin
	Valve dirty		
FM_C5	Motor is short circuit	Loss of pumping capacity. Short circuit of compressor	Loss of cooling capacity in the cabin
	Electric overload		
	Compressor motor protection failure		
ELECTRONIC CONTROL CARD (ECC): Regulate, monitor and diagnose the HVAC.			
FM_E1	Short circuit	Incorrect regulation of the temperature by the control card	Loss of cooling capacity in the cabin
	ECC dirty		
	Defect in printed circuit		
	Overload of the ECC		
WATCHDOG: Activates the emergency regulation mode.			
FM_W1	Hardware failure	Incorrect regulation of temperature	Loss of emergency regulation capacity
	Software failure		
IGBT MODULE: Electronic switch used to control the compressor			
FM_I1	Overcurrent	Loss of pumping capacity. Short circuit	Loss of cooling capacity in the cabin
	Overtemperature		
	Secondary breakdown		
FM_I2	Hot carrier injection	Insufficient current to drive the compressor.	Loss of cooling capacity in the cabin
	Electromigration		
	Temperature instability		
UPS: Provides power for emergency ventilation if the overhead power line fails			
FM_U1	Electric failure	Complete loss of functionality	Loss of emergency ventilation
	Ageing battery units		

The identified failure modes and the notation used to label them in Table 3.2 are described in the following list:

- Compressor
    - FM_C1: motor does not start on demand.
    - FM_C2: incorrect signal from thermostat.
    - FM_C3: pump gas leakage.
    - FM_C4: sticking internal valve.
    - FM_C5: internal overload motor protection.

- Electronic Control Card (ECC)
    - FM_E1: electronic control failure.

- Watchdog
    - FM_W1: watchdog doesn't act when the control fails.

- IGBT module
    - FM_I1: short/open circuit.
    - FM_I2: parameter drift.

- UPS
    - FM_U1: no output power.

Note that this is only an extract of the complete FMECA performed for the HVAC system under analysis. The complete report includes over one hundred failure modes and will be discussed in the following sections by the RPN threshold estimation point of view. In this case, only an extract of the most complex and critical items have been included in Table 3.2 and in the following analysis.

Table 3.3 shows all the inputs required by the proposed fuzzy-based RCM approach. Occurrence O, Severity S and Detection D are expressed in Table 3.3 using linguistic variables, while the other two inputs (i.e. definition of evident failure and impact on safety) are described using simple Boolean variables.

The parameters shown in Table 3.3 are used as input for the proposed framework for maintenance decisions as illustrated in Figure 3.5. Alternatively, the fuzzy inference system described in Figure 3.6 can be implemented to assess the optimal maintenance task for each failure mode identified during the preliminary FMEA procedure.

Tab. 3. 3 - Input parameters of the proposed fuzzy-based RCM approach. The failure modes refer to the preliminary FMEA report in Table 2.

Failure modes	O	S	D	Is failure evident?	Impact on safety?
FM_C1	High	Tolerable	Absolutely Uncertain	No	No
FM_C2	Remote	Very Low	Almost certain	Yes	No
FM_C3	Probable	Tolerable	Medium	Yes	No
FM_C4	Probable	Tolerable	Almost certain	No	No
FM_C5	Remote	Tolerable	Almost certain	Yes	No
FM_E1	Probable	Tolerable	Medium	Yes	Yes
FM_W1	Probable	Tolerable	Absolutely Uncertain	No	No
FM_I1	Remote	Critical	Almost certain	Yes	No
FM_I2	Remote	Tolerable	Medium	No	No
FM_U1	Probable	Critical	Almost certain	No	Yes

The results of the proposed fuzzy-based approach applied to the most critical components of the HVAC system installed in a high-speed train are summarized as follows:

- FM_C1: “failure finding plus scheduled maintenance”. Failure finding is implemented every month; in this way it is possible to obtain a larger interval for the scheduled maintenance (6 months).
- FM_C2: “no preventive maintenance (run to failure)”. The failure of the thermostat doesn’t represent critical damage for the system; therefore, corrective maintenance could be implemented.
- FM3_C3: “scheduled maintenance”. Operations on the pump are scheduled every 3 months.
- FM_C4: “condition monitoring”. The valve is monitored continuously using a position transducer and a pressure transmitter.
- FM_C5: “condition monitoring”. Several sensors are implemented to monitor the state of the compressor, including temperature, vibration,

pressure and load sensors.

- FM_E1: “condition monitoring plus scheduled maintenance”. The electronic board is monitored continuously by a dedicated device equipped with temperature, humidity and vibration transducers. These parameters are extremely useful to identify the health state of electronics. Moreover, the diagnostic device also uses interrogation algorithms and residual life computational algorithms. Furthermore, scheduled maintenance (in the form of visual inspection) is required once a year.
- FM_W1: “failure finding plus scheduled maintenance”. Failure finding is implemented every month; while scheduled maintenance (in the form of visual inspection and manual HW/SW testing) is required every year.
- FM_I1: “condition monitoring”. The IGBT is monitored continuously using a temperature transducer and two power meters used to provide both input/output voltage and current.
- FM_I2: “failure finding”. Failure finding is implemented every month to check the health state of the IGBT.
- FM_U1: “condition monitoring”. The UPS is monitored continuously in order to check the health state of the battery using voltage and current measurements to estimate the residual capacity of the battery.

The proposed approach offers a powerful solution because it allows designers to select the optimal maintenance policy without the need for subjective evaluation. Moreover, it privileges condition-based maintenance tasks, such as condition monitoring and failure finding. As a matter of fact, most paths of the decision-diagram lead to condition-based maintenance operations. In some cases (see the results obtained for FM_C1, FM_E1 and FM_W1), two tasks are implemented at the same time; one is condition-based maintenance (such as condition monitoring or failure finding), and the other is scheduled maintenance. In fact, in some circumstances, using condition monitoring or failure finding alone is not enough to guarantee high levels of availability. Scheduled maintenance allows designers to improve system performance, but the interval between two consecutive scheduled restorations could be greater because condition-based maintenance is implemented at the same time.

More generally, the proposed approach guides designers to the choice of condition monitoring as long as it is possible to monitor the parameters that influence the component's wear-out. This condition is taken into account using the fuzzy detection linguistic variable.

The complete results of the proposed Fuzzy-based RCM procedure applied to the whole HVAC system installed on a high-speed train are summarized in the pie charts in Figure 3.7.

Figure 3.7 (a) shows the percentage of each assigned task with respect to the complete HVAC maintenance plan. It is possible to sea that Condition monitoring and Failure finding procedures play a crucial role in the maintenance policies of the HVAC under analysis, with 44% and 25% of the tasks respectively. Quite the opposite, only the 3% of the failure modes are left to corrective maintenance (Run to Failure) because of safety implications of many failures related to the ventilation system of the train. Due to the mechanical and hydraulic components included in the system, scheduled maintenance still remains a considerable part of the HVAC maintenance plan. However, most of the time scheduled maintenance is carried out along with condition-based maintenance, such as condition monitoring (10%) and failure finding (7%).

Figure 3.7 (b) summarizes the results comparing condition-based maintenance against scheduled maintenance and corrective maintenance.

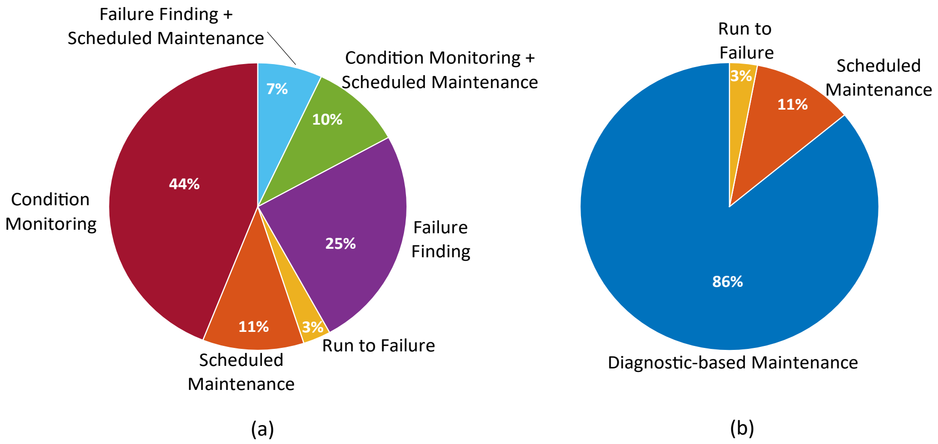


Fig. 3. 7- Summary of result achieved applying the proposed maintenance decision-diagram to the complete HVAC system under analysis. (a) Overall results of the proposed Fuzzy-based RCM procedure. (b) Comparison between diagnostic-based maintenance, scheduled maintenance, and corrective maintenance.

The results confirm how the proposed decision-diagram privileges the choice of a diagnostic approach with the 86% of the maintenance task in the proposed plan including condition monitoring or failure finding procedures.

Finally, the results achieved using the proposed fuzzy-based method are compared with a maintenance plan for the same HVAC achieved using the classic RCM according to the international standard IEC 60300-3-11. For the sake of brevity, only an extract of the comparison is included in Table 3.4. Analyzing Table 3.4 it is extremely evident the superiority of the proposed approach. Using the fuzzy linguistic variables and the if-then rules, the proposed methodology assigns a unique maintenance task to each failure mode, while the classic RCM let the designer the selection between at least four or five types of task without any further explanation on how to choose between them.

Tab. 3. 4 - Extract of comparison between the proposed Fuzzy-based RCM and the classic RCM assessed following the guidelines of IEC 60300-3-11

Failure Mode	**Selected Maintenance Task**	
	Proposed Fuzzy-based RCM	**Classic RCM IEC 60300-3-11**
FM_C3	Scheduled Maintenance	Condition Monitoring OR Scheduled Maintenance OR Run to Failure OR Alternative actions
FM_I2	Failure Finding	Condition Monitoring OR Scheduled Maintenance OR Failure Finding OR Run to Failure OR Alternative actions
FM_U1	Condition Monitoring	Condition Monitoring OR Scheduled Maintenance OR Failure Finding OR Alternative actions

3.6 From Fuzzy RCM to Fuzzy FMECA

RCM is a well-defined and structured procedure which significantly rely on FMECA. However, the latter method suffers many problems. The major issues of this technique are a remarkable contribution of the expert's subjectivity and a lack of a methodology to univocally distinguish critical failures and negligible failures. Trying to solve these problems this work proposes two innovative approaches:

- An innovative fuzzy FMECA has been developed to provide a non-subjective assessment of the Risk Priority Number. At the same time, the proposed method is also able to solve all the other drawbacks that the literature review about the classical FMECA pointed out (such as duplicates, gaps in the range, relative importance among the factors and high sensitivity to small changes - for more information see section 3.8).
- An innovative threshold estimation method to divide the critical and negligible modes in a more objective and structured way with respect to the other approaches available in literature.

A preliminary analysis about the drawbacks of the classical RPN has been published in [58]. Building upon this, the aim of this work is to proposes a simple and effective tool that use Fuzzy theory to solve all the problems of the classical RPN and consequently provides an efficient methodology to prioritize failure modes according to their risk.

In particular, this thesis proposes a fuzzy-based approach that uses fuzzy linguistic term to assess the O, S and D and then evaluates the RPN of each failure mode as the fuzzy multiplication of the indexes (See Section 3.9). Fuzzy weights are also taken into account to assess different importance to Occurrence, Severity and Detection. A graphical user interface has been developed using MATLAB programming language to automatize the tool and make it accessible also on industrial field. The advantages of the proposed procedure are extensively illustrated emphasizing the benefits achieved with the proposed fuzzy-based tool to solve classical RPN drawbacks. The output of this procedure is a dataset of RPN which must be processed using the proposed risk threshold estimation method (See Section 3.13) in order to divide the identified failures into two different clusters: a set of critical failure modes against a set of negligible failure modes (by a risk value point of view).

3.7 Brief overview of FMECA

Failure Modes, Effects and Criticality Analysis (FMECA) is widely considered an effective and efficient methodology for risk assessment, failure analysis and maintenance decision-making. It is a powerful and effective tool that could be easily applied to estimate the risk associated to every failure of a safety-critical system [54], [76], [88].

FMECA is commonly carried out to identify the potential hazardous events of a system or process, and consequently rank them to allow prioritization of countermeasures and reduce the risk level associated to the most critical events. Therefore, it provides an effective support tool that should be implemented during the design and development of safety-related systems in every industrial field. Usually, FMECA starts as a qualitative analysis (i.e. FMEA – Failure Modes and Effects Analysis) that identifies all the possible failure modes of the components that make up the system. Then, for each failure mode, failure causes and failure effects are identified. The second step is the Criticality Analysis, which is the quantitatively section of the FMECA worksheet which assesses different parameters to each failure mode and then calculates the risk level using a ranking called Risk Priority Number (RPN) calculated as follows [53]:

$$RPN = O \cdot S \cdot D \tag{3.1}$$

Occurrence (O) is an index that measures the probability that a failure mode will happen, where the greater the index the greater the frequency of occurrence. Severity (S) measures the impact of the failure effects on the system functionalities, low values of S stand for negligible failures, while greater values of S stand for catastrophic failures with safety implication. Detection (D) represents the probability that the failure mode will be diagnosed before its effects are manifested on the system. Detection is ranked in a reverse order compared to the previous parameters, the higher the D, the lower the possibility of detecting the failure [89]. The international standard IEC 60812 [53] suggest to use only integer number in a 1-to-10 scale to assess the values of O, S and D. Consequently, the RPN can assume values within the range [1; 1000]. Many papers in recent literature highlighted the disadvantages of the classical RPN equation, as well as lots of paper introduce the Fuzzy theory as support in the FMECA assessment.

3.8 State of the art of FMECA

The drawbacks of RPN are widely described in many papers (see for instance but not only [80], [81], [90]–[94]), in the following a brief explanation of the most critical ones are reported [58]:

- The complete set of possible RPN values is not continuous but it is characterized by many holes in the scale with only 120 unique values, while the number of possible combinations is 1000 in case of a 10-point scale.
- Since there are 1000 possible combinations and only 120 unique values, then also the duplicates of RPNs are a critical issue. In fact, many different combinations of O, S, and D could lead to the same RPN, consequently the prioritization of the modes may be difficult. The maximum repetition frequency in case of 10-point scale is 24, which means that 24 different combinations of O, S, D lead to the same RPN.
- Classical RPN formula suffers of high sensitivity to small changes of Occurrence, Severity and Detection.
- The relative importance among O, S and D is not considered and the three indexes have the same weight inside the formula.
- Subjective definition of O, S, D which are difficult to precisely determine using a scale of integer values.
- Miss of a non-subjective method to divide critical and negligible failure modes

Many works in recent literature also try to propose different methods to overcome the problems associated to the classical RPN. Braband [95] proposes to assess the new IRPN (Improved Risk Priority Number) as the sum of the Occurrence, Severity and Detection using logarithmic scale to evaluate the indexes. This method is the only alternative RPN included in the international standard IEC 60812 [53]. Chang et al. [96] propose an exponential RPN called ERPN given by the sum of three exponential functions, one for each of the indexes. This approach is enhanced in [97] using the product of occurrence and detection that stand as probability, and severity plays a role as value in power. In this way a higher weight to Severity is assessed compared to Occurrence and Detection. Several papers propose different RPN formulations introducing innovative coefficients and parameters. These solutions could solve at least two of the RPN drawbacks: the duplicate issue and the relative importance of the parameters. For instance, in [98] an alternative RPN is proposed by considering the associated quality cost and the capability of failure detection system as additional terms to optimize the prioritization of each failure mode. Carmignani [99] introduces a priority-cost FMECA calculating the priority of every potential design fault and the profitability in accomplishing the corrective design actions. In [100] the Root Cause Analysis (RCA) is used to assess sub-criterion weight and significant coefficient for Occurrence, Severity and Detection. Tang et al. [101] proposes an innovative approach considering the ambiguity measure of the experts that carried out the assessment of O, S and D to mitigate the subjectivity issue. Chang [102] suggests to use a method that integrates the ordered weighted geometric averaging (OWGA) operator and the decision-making trial and evaluation laboratory (DEMATEL) approach in order to a achieve an efficient and effective algorithm in risk analysis. In [103] a simple approach is proposed defining a new metric called RAV (Risk Assessment Value) as the product of Occurrence and Severity divided by Detection. In [104] Severity is obtained by summing different parameters related to safety, environment, costs, customer satisfaction and mission goal. In [105] a data-driven RPN calculation is introduced based on quantitative measures and sizable datasets to obtain a more formal and objective risk evaluation. Giardina [106] introduces a FMECA and HAZOP integrated analysis called FHIA to improve risk analysis of complex system. In [107] a method based on minimum cut set is proposed to take into account multiple failure modes and to extend the RPN definition by multiplying it with a weight parameter which characterize the importance of the failure causes within the system. Other papers such as [108]–[110] simply proposes to reduce the scale of O, S and D to reduce the possible combination of RPN values and slightly mitigate the above-mentioned drawbacks.

A widely used technique to overcome the RPN problems is the fuzzy logic [23]. Fuzzy theory was applied to FMECA procedure in many different industrial fields, such as nuclear power plant [111], traditional power plant [112], power electronic components [113], satellite [114], agriculture [115], Oil&Gas [116], tunneling operation [38] and many others. Fuzzy FMECA could be conducted in many different ways depending on the drawbacks that the procedure wants to overcome. In many paper the fuzzy “If-Then principle” is implemented because it is far too easy the assessment of O, S and D using linguistic terms (see for instance [27], [77]–[79], [83], [117]). All papers that use the fuzzy if-then to solve the FMECA drawbacks start representing Occurrence, Severity and Detection through linguistic variables that are associated to fuzzy membership functions [118]–[121]. Using a set of fuzzy inference rules, a fuzzy RPN assessment is obtained [122]–[127]. All the If-then FMECA procedures in literature are based on one of the following three types of fuzzy inferences to solve the if-then rules. The main disadvantages of all the if-then approaches is the number of rules that must be assessed.

If-Then FMECA is not the only way to introduce fuzzy theory inside the classical FMECA procedure. In [128] an approach based on convex normalized fuzzy number is introduced using the degree of match to estimate the matching between the expert judgments and the fuzzy number. Keskin et al. [129] proposes to use the fuzzy Adaptive Resonance Theory (fuzzy ART) to assess the Risk Priority Number. In [84] the fuzzy RPN is calculated using alpha-level sets and linear programming models through the weighted geometric means of the fuzzy number assessed for Occurrence, Severity and Detection. In [130] a fuzzy approach integrating weighted least square method is used to achieve robustness RPN results in term of uncertainty. In [131] a consensus-based group decision-making framework has been proposed based on possibilistic hesitant fuzzy linguistic information.

The integration of fuzzy theory with TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) method was firstly proposed by Chen [132], and then applied in many papers such as Braglia et al. [133], Carpitella et al. [82] or Mangeli et al. [134] to solve FMECA drawbacks.

In [135] the analytic hierarchy process (AHP) was used to integrate inside the classical FMECA some economic aspects. This approach has been enhanced in [86] combining fuzzy TOPSIS and AHP method.

Other papers integrate fuzzy logic with different approaches, such as TODIM (a Portuguese acronym of interactive and multiple attribute decision making) [136], VIKOR (a Serbian acronym of Multicriteria Optimization and Compromise Solution) [137], PROMETHEE (Preference ranking organization method for enrichment evaluation) [138] and QUALIFLEX (Qualitative flexible multiple criteria method) [139].

Despite the latter papers provide significant results in terms of RPN prioritization, the introduction of many different approaches within the classical FMECA remarkably increases the complexity of the procedure.

3.9 Proposed Fuzzy FMECA approach

As all the fuzzy reliability analysis discovered in literature the proposed approach is based on a linguistic assessment of Occurrence O, Severity S and Detection D.

In order to carry out this evaluation, both triangular and trapezoidal membership functions are allowed since they are the most common membership functions in reliability engineering [23].

Assuming that $z, a, b, c, d \in \mathbb{R}$, then a trapezoidal fuzzy number A_{TRAP} could be defined by means of the membership function $\mu_{A_{TRAP}}(z)$ which is given as follow [21], [36]:

$$\mu_{A_{TRAP}}(z) = \begin{cases} \dfrac{z-a}{b-a} & if\ a < z < b \\ 1 & if\ b \leq z < c \\ \dfrac{d-z}{d-c} & if\ c \leq z < d \\ 0 & otherwise \end{cases} \tag{3.2}$$

Figure 3.8 shows the generic trapezoidal fuzzy number A_{TRAP} described by the membership function in equation (3.3). A_{TRAP} can be identified also using the following short-term definition:

$$A_{TRAP} = (a, b, c, d) \tag{3.3}$$

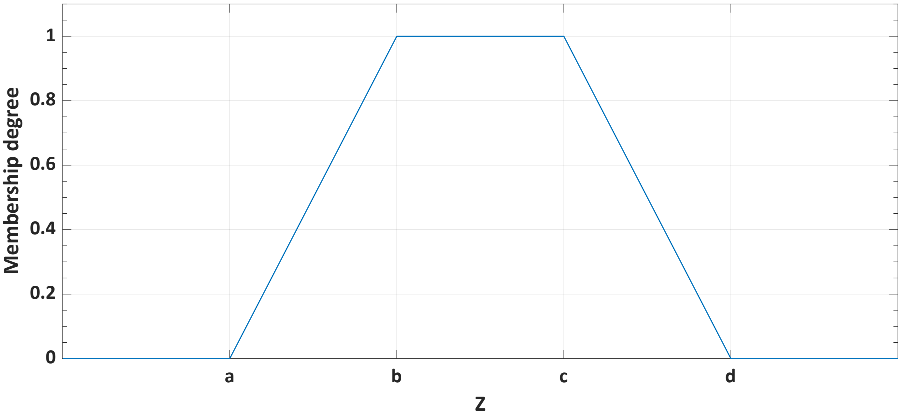


Fig. 3. 8 - Example of membership function of a generic trapezoidal fuzzy number $A_{TRAP} = (a,\ b,\ c,\ d)$

Considering the trapezoidal fuzzy number A_{TRAP}, the interval between b and c represent the set of values with the maximum degree of membership, while all the values lower than a or greater than d have degree of membership equal to zero.

Similar definition could be drawn also for triangular fuzzy number A_{TRI}. In this case the fuzzy number could be defined by means of the membership function $\mu_{A_{TRI}}(z)$ as follow [21], [36]:

$$\mu_{A_{TRI}}(z) = \begin{cases} \frac{z-a}{b-a} & if\ a < z < b \\ \frac{c-z}{c-b} & if\ b \leq z < c \\ 0 & otherwise \end{cases} \tag{3.4}$$

Figure 3.9 shows the generic triangular fuzzy number A_{TRI} described by the membership function in equation (3.5). A_{TRI} can be identified also using the following short-term definition:

$$A_{TRI} = (a, b, c) \tag{3.5}$$

In case of a triangular fuzzy number the value b represents the parameter with the maximum degree of membership, while a and c are the lower and upper bound respectively.

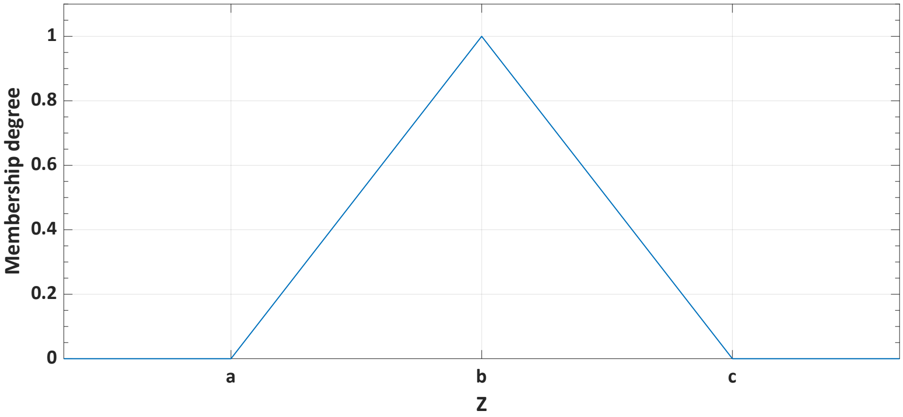


Fig. 3. 9 - Example of membership function of a generic triangular fuzzy number $A_{TRI} = (a,\ b,\ c)$

The evaluation of O, S and D by means of membership functions allow to considerably mitigate the RPN drawback related to the subjectivity. In fact, it is possible to define the parameters using linguistic variables and associates these variables to a set of membership functions. Using this procedure, the expert that has to carry out the assessment of the parameter should not arbitrarily decide a number within a predetermined range but has to choose between a set of linguistic terms that are closer to human reasoning.

In the proposed method both triangular and trapezoidal membership functions could be implemented. In order to follow the guidance of the international standard IEC 60812 [53] the assessment of O, S and D should be based on a 10-point scale. Despite this, the use of a limited scale (e.g from 1 to 5) provides remarkable benefits in term of attenuation of the RPN drawbacks (particularly the duplicates and the gaps in the range) as already demonstrated in a previous work [58]. For this reason, in this work Occurrence, Severity and Detection could assume values in the classical range from 1 to 10, but only five membership functions could be included in this range, so that the number of possible RPN combination is limited.

The Occurrence assessment is shown in figure 3.10.a where five triangular membership functions are considered. The relative linguistic variables are: {“Remote”, “Low”, “Moderate”, “High”, “Very High”}.

Figure 3.10.b shows the triangular membership functions selected during the Severity assessment with their relative linguistic variables: {“Insignificant”, “Marginal”, “Critical”, “Very critical”, “Catastrophic”}.

The membership functions of the Detection are shown in fig. 3.10.c according to the following linguistic variables: {“Almost certain”, “Probable”, “Possible”, “Remote”, “Almost uncertain”}.

A fuzzy weight for Occurrence ω_O, Severity ω_S and Detection ω_D must be defined in order to takes into account their relative importance and to assess a different weight to each one. In this way it is possible to diversify the impact of the three factors and consequently solve another one of the RPN drawbacks. This is done using a set of three trapezoidal membership functions (fig. 3.11) assuming values within the range [0 – 1] and described by the linguistic terms: {“Medium”, “High”, “Very High”}.

The experts that carry out the procedure must choose the proper weight or each parameter basing only on their linguistic term.

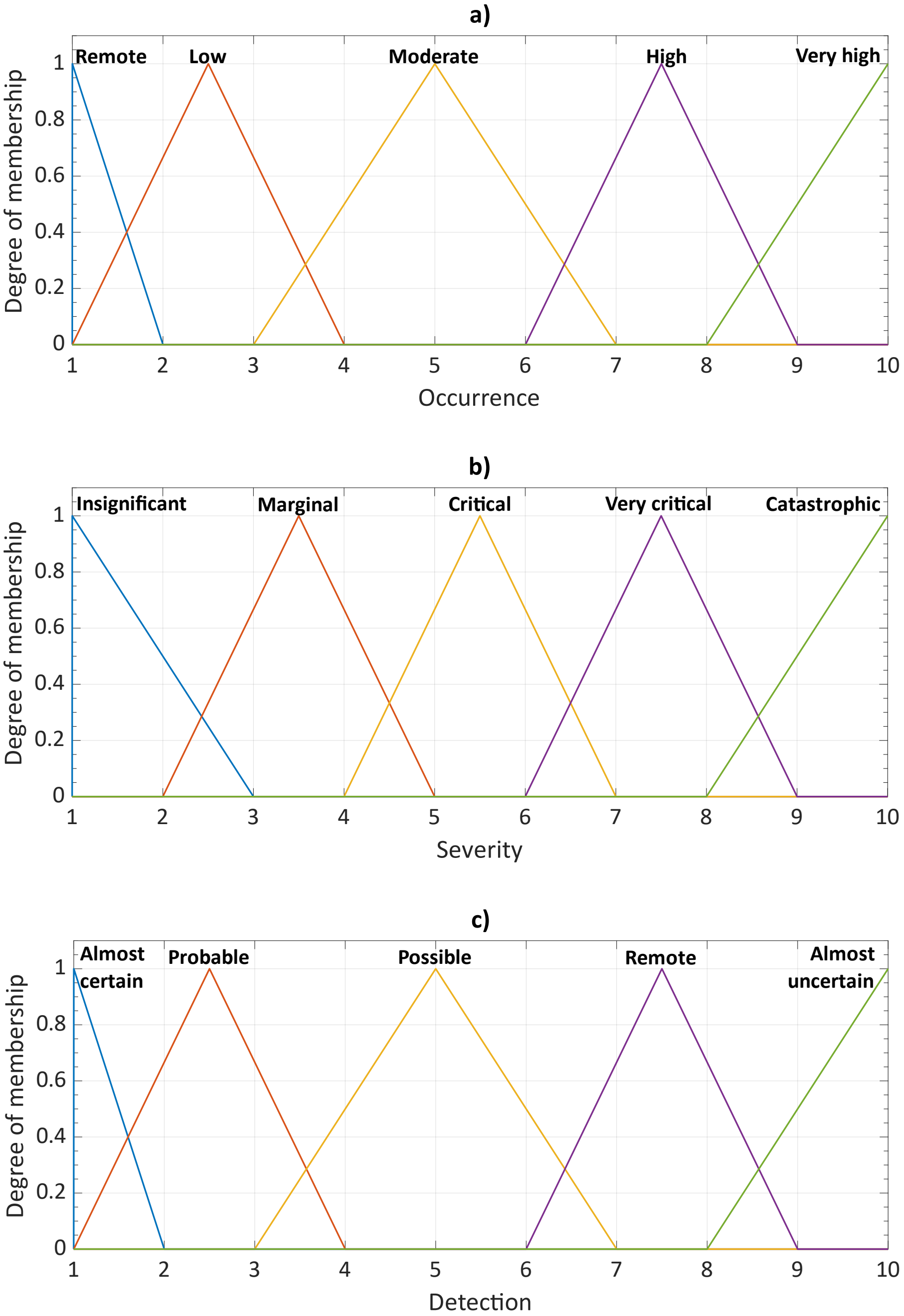


Fig. 3. 10 - Set of five triangular membership functions and their relative linguistic variables selected for each one of the FMECA influence factors. Occurrence is illustrated in a), while Severity is illustrated in b) and Detection is illustrated in c).

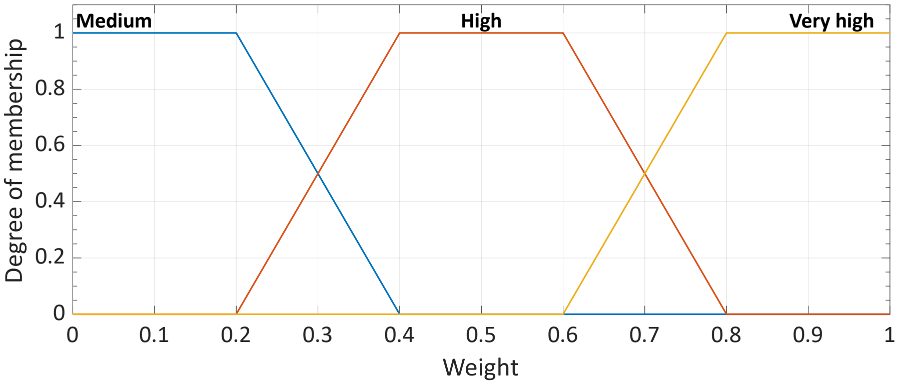


Fig. 3. 11 - Set of three trapezoidal membership functions and their relative linguistic variable used to assess the proper weight of Occurrence, Severity and Detection.

Then the obtained weights should be defuzzified using the centroid method. Starting from a fuzzy number and its corresponding membership function the defuzzification procedure is the process of generating a crisp logic value related to the starting fuzzy value. In this paper the centroid defuzzification is used. It returns z^* which is the center of gravity of the fuzzy number described by the membership function $\mu(z)$ as follow [36]:

$$z^* = \frac{\int z \cdot \mu(z)\, dz}{\int \mu(z)\, dz} \tag{3.6}$$

After the defuzzification procedure, three crisp weights are available: ω_O^* is the Occurrence weight, ω_S^* is the Severity weight and ω_D^* is the Detection weight.

The following step is the drafting of the FMECA worksheet, including the assessment of O_i, S_i and D_i as membership functions. The index $i = 1, \dots n$ refers to the failure modes identified during the procedure.

Then, the weighted occurrence ωO_i is given by the occurrence of the mode O_i to the power of the occurrence weight ω_O^*.

$$\omega O_i = O_i^{\omega_O^*} \qquad \forall\, i = 1, \dots n \tag{3.7}$$

Since $O_i = \left(O_{a_i}, O_{b_i}, O_{c_i}\right)$ is a triangular fuzzy number the exponentiation could be solve as follow [140], [141]:

$$O_i{}^{\omega_O^*} = (O_{a_i}, O_{b_i}, O_{c_i})^{\omega_O^*} = \left(O_{a_i}^{\omega_O^*}, O_{b_i}^{\omega_O^*}, O_{c_i}^{\omega_O^*}\right) \tag{3.8}$$

$$\omega O_i = \left(O_{a_i}^{\omega_O^*}, O_{b_i}^{\omega_O^*}, O_{c_i}^{\omega_O^*}\right) \qquad \forall\, i = 1, \dots n \tag{3.9}$$

Quite the same, the weighted severity ωS_i and the weighted detection ωD_i are given by:

$$\omega S_i = S_i{}^{\omega_S^*} = \left(S_{a_i}^{\omega_S^*}, S_{b_i}^{\omega_S^*}, S_{c_i}^{\omega_S^*}\right) \qquad \forall\, i = 1, \dots n \tag{3.10}$$

$$\omega D_i = D_i{}^{\omega_D^*} = \left(D_{a_i}^{\omega_D^*}, D_{b_i}^{\omega_D^*}, D_{c_i}^{\omega_D^*}\right) \qquad \forall\, i = 1, \dots n \tag{3.11}$$

Consequently, the Fuzzy Risk Priority Number $FRPN_i$ of each failure mode i could be obtained computing the fuzzy product of the weighted parameters as follow:

$$FRPN_i = \omega O_i \otimes \omega S_i \otimes \omega D_i \tag{3.12}$$

where the operator ⊗ stands for the product between fuzzy number achieved using the α-cut theory.

Finally, the RPN^* of each failure mode is obtained by means of centroid defuzzification of the corresponding FRPN as follow:

$$RPN^* = \frac{\int z \cdot \mu_{FRPN}(z)\, dz}{\int \mu_{FRPN}(z)\, dz} \tag{3.13}$$

where $\mu_{FRPN}(z)$ is the membership function of the fuzzy set FRPN obtained through eq. (3.12).

The complete fuzzy-based proposed procedure is illustrated in the flowchart in Fig. 3.12, highlighting each step of the method. The light red box in the figure represents the procedure loop that must be repeated several times until the risk assessment of each one of the identified failure modes is completed. It is important to note that the steps regarding the fuzzy weights are independent from the loop. Once the weights have been set and defuzzified, then they must remain the same for every failure mode since the definition of the weights is a upper-level assignments which must be independent from the risk assessment of the specified failure modes.

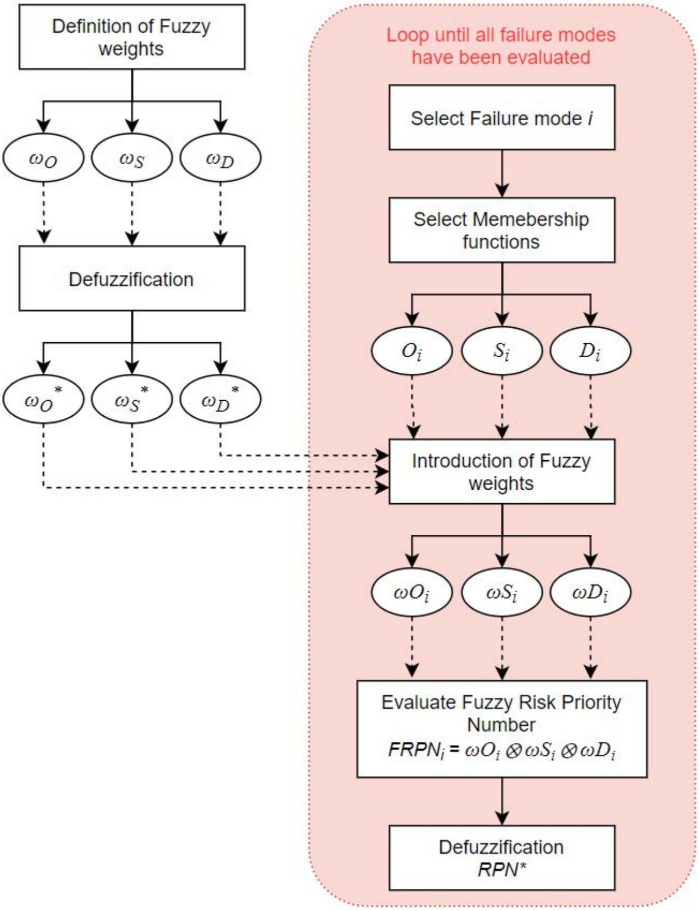

Definition of Fuzzy weights
ω_O
ω_S
ω_D
Defuzzification
$\omega_O{}^*$
$\omega_S{}^*$
$\omega_D{}^*$
Loop until all failure modes have been evaluated
Select Failure mode *i*
Select Memebership functions
O_i
S_i
D_i
Introduction of Fuzzy weights
ωO_i
ωS_i
ωD_i
Evaluate Fuzzy Risk Priority Number
$FRPN_i = \omega O_i \otimes \omega S_i \otimes \omega D_i$
Defuzzification
RPN^*

Fig. 3. 12 - Flowchart of the proposed fuzzy-based tool highlighting every step of the procedure. The loop inside the light red box must be repeated for each one of the failure modes.

Since five membership functions for each one of O, S and D were chosen, the possible combination of risk priority numbers are $5 \cdot 5 \cdot 5 = 125$. To better clarify the advantages of the proposed technique, Fig. 3.13 shows all the 125 possible combination of $FRPN$ fixing the following weights: $\omega_O = \{'High'\}$, $\omega_S = \{'Very\ high\ '\}$ and $\omega_D = \{'High'\}$.

Fig.3.13 highlights how the proposed approach solves other two of the above-mentioned RPN drawbacks: the duplicate issue and the "gaps in the range" problem. In fact, every combination of Occurrence, Severity and Detection provides a unique FRPN membership function, and thus a unique value of the defuzzified RPN^*.

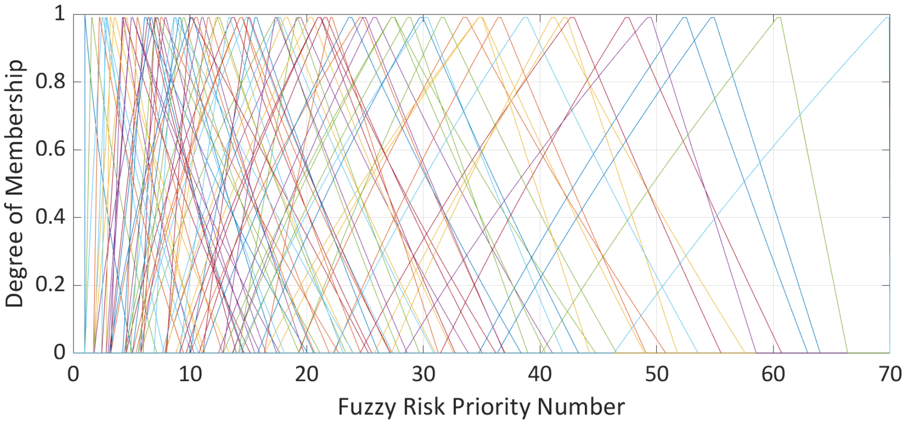


Fig. 3. 13 - Set of all the 125 possible membership functions for the Fuzzy Risk Priority Number in case of the following weights are set: $\omega_O = \{'High'\}$, $\omega_S = \{'Very\ high\ '\}$ *and* $\omega_D = \{'High'\}$. *The different colors stand for a different FRPN achieved using a different combination of the O, S and D.*

As a consequence, the proposed procedure provides no duplicates in the Risk Priority Number assessment, and every different combination of O, S, and D lead to a different RPN. Regarding the "gaps in the range" problem, fig.3.13 highlights that FRPN assume value in the range [1; 70] (in case the weight ω_O, ω_S and ω_D are set differently, then FRPN will result in a different range).

Within this range, every possible crisp value of RPN has a membership degree greater than zero. Furthermore, almost every crisp value within the range has a not null membership degree of belonging to two or more membership functions. As a consequence, also the "gaps in the range" issue is solved using the proposed approach.

The last RPN drawbacks not already solve is the high sensitivity to small changes of Occurrence, Severity and Detection. Fig. 3.14 shows a practical situation using the proposed approach. The blue membership function is obtained setting $O = \{'High'\}$, $S = \{'Very\ Critical'\}$ and $D = \{'Remote'\}$. A small change is performed to achieve the red membership function (i.e. O is moved to $\{'Very\ High'\}$ while S and D are maintained constant). The dotted lines in the figure represent the defuzzified RPN^* obtained in the above-mentioned situations.

The obtained risk priority numbers (both fuzzy FRPN and defuzzified RPN^*) are really close, and only a small difference is evident.

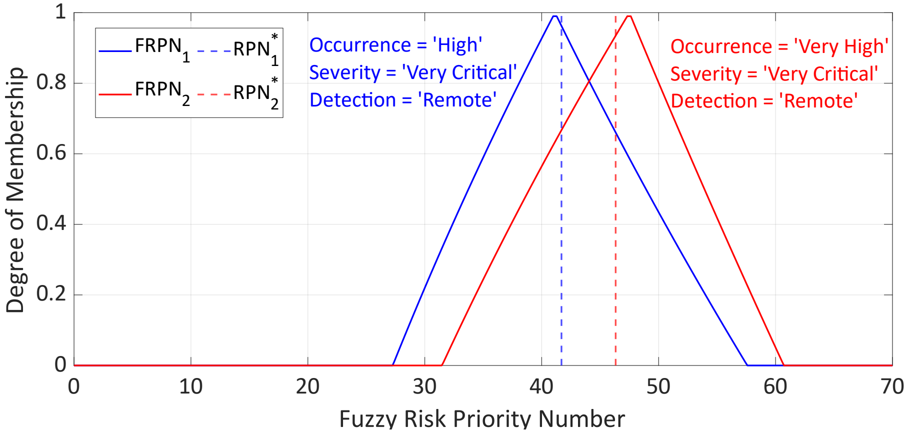


Fig. 3. 14 - Fuzzy Risk Priority Number FRPN (continuous trends) and defuzzified RPN^* *(dotted lines) obtained using two similar combinations of O, S and D. A small change in occurrence results in a small change in the risk priority number (both fuzzy FRPN and defuzzified* RPN^**).*

An analog scenario in case of the classical FMECA is the following:

- $O = 9,\ S = 9,\ D = 9$ which results in $RPN = 729$;
- $O = 10,\ S = 9,\ D = 9$ which results in $RPN = 810$;

Therefore, while the classical RPN suffer a high sensitivity to a small change in occurrence, the proposed approach is proven to be an effective method in the solution of this issue.

3.10 Case study: Fuzzy FMECA of Railway signaling system

The analysis of the receiver system of the ATP under test (See Section 1.3.2) pointed out seventeen failure modes, identified using the notation from “Failure mode #1” to “Failure mode #17”. Fig. 3.15 shows the classification of the failure effects for the system. All the seventeen failure modes could have only two possible local effects: no carrier signal transmitted or an increase of the transmitted power. Both effects are referred to the receiver board level. Instead, the global effects refer to the train running level and could be different in case the failure mode is detected or not. The severity assessment has been conducted based on the information of the failure effects included in Fig. 3.15.

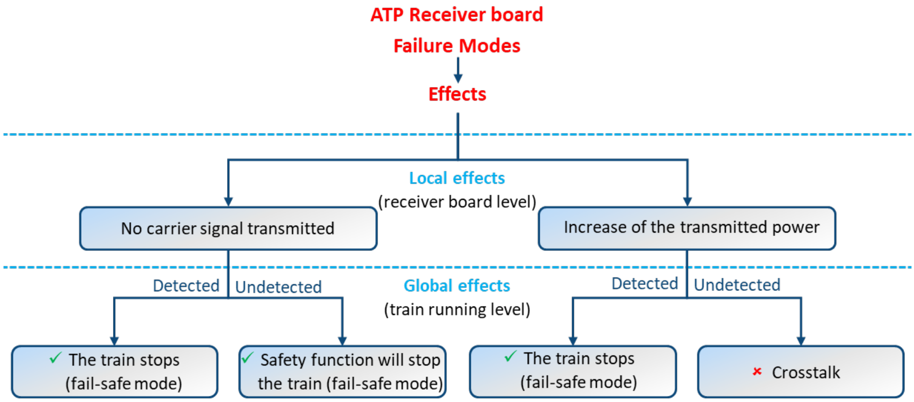

ATP Receiver board
Failure Modes
Effects
Local effects
(receiver board level)
No carrier signal transmitted
Increase of the transmitted power
Detected
Undetected
Global effects
(train running level)
Detected
Undetected
✓ The train stops (fail-safe mode)
✓ Safety function will stop the train (fail-safe mode)
✓ The train stops (fail-safe mode)
× Crosstalk

Fig. 3. 15 - Classification of failure effects for the receiver board under test. The top level refers to the local effects, while the bottom level refers to the global effects, divided in detected and undetected.

In particular, every failure mode which involve a crosstalk effect is considered extremely critical and its relative membership function will be $S = \{'Critical'\}$ or $S = \{'Very\ Critical'\}$ or $S = \{'Catastrophic\}$ depending on the amount of transmitted power increase. While every failure mode which involve a fail-safe stop of the train is not critical and they will have a membership function equal to $S = \{'Insignificant'\}$ or $S = \{'Marginal\}$ depending on the safety-oriented system that will stop the train.

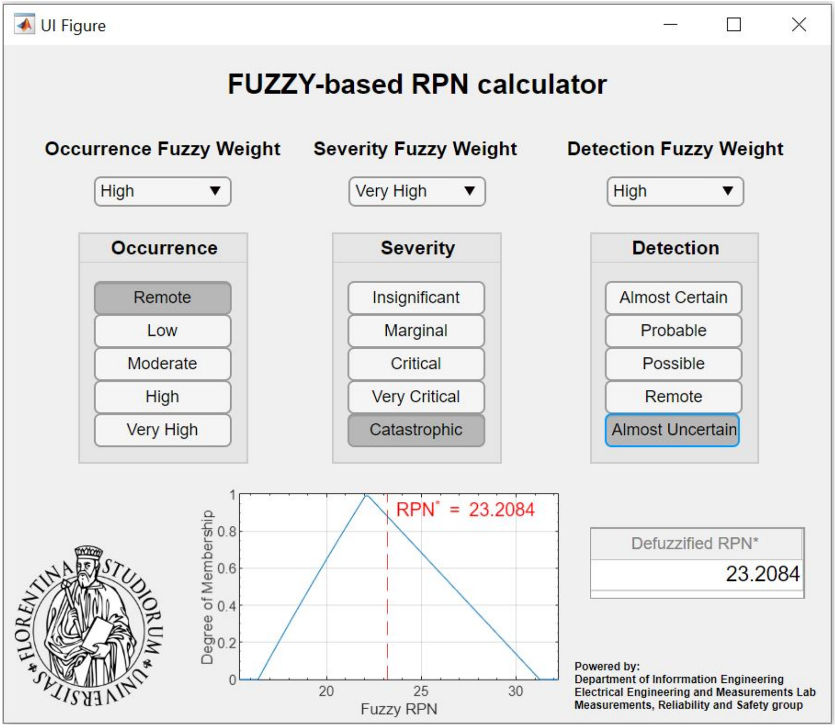
It is also important to note that the receiver board under test integrates a power detector electronic circuit used as diagnostic system to monitor the power transmitted by the receiver board. This diagnostic system allows to diagnose almost certainly some of the identified failures, consequently their relative value of Detection membership function will be $D = \{'Almost\ Certain'\}$. All the other failure modes that are not covered by the diagnostic system are instead characterized by detection $D = \{'Almost\ Uncertain'\}$ since it will be not possible to diagnose the failure.

Finally, the assessment of the occurrence has been conducted using the failure rate of the failure mode under test to estimate the probability that the event will occur. Table 3.5 summarizes the assessment of O, S and D membership functions for the seventeen failure modes identified during the analysis.

Tab. 3. 5 -Assessment of the Membership functions for O, S and D. Seventeen Failure Modes have been identified during the analysis

Failure mode	O	S	D
#1	High (6, 7.5, 9)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#2	Moderate (3, 5, 7)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#3	Moderate (3, 5, 7)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#4	Moderate (3, 5, 7)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#5	Moderate (3, 5, 7)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#6	Moderate (3, 5, 7)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#7	Remote (1, 1, 2)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#8	Remote (1, 1, 2)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#9	Moderate (3, 5, 7)	Insignificant (1, 1, 3)	Almost certain (1, 1, 2)
#10	Remote (1, 1, 2)	Catastrophic (8, 10, 10)	Almost uncertain (8, 10, 10)
#11	Very high (8, 10, 10)	Insignificant (1, 1, 3)	Almost uncertain (8, 10, 10)
#12	Moderate (3, 5, 7)	Very critical (6, 7.5, 9)	Almost uncertain (8, 10, 10)
#13	Remote (1, 1, 2)	Very critical (6, 7.5, 9)	Almost uncertain (8, 10, 10)
#14	Remote (1, 1, 2)	Catastrophic (8, 10, 10)	Almost uncertain (8, 10, 10)
#15	Remote (1, 1, 2)	Marginal (2, 3.5, 5)	Almost uncertain (8, 10, 10)
#16	High (6, 7.5, 9)	Very critical (6, 7.5, 9)	Almost uncertain (8, 10, 10)
#17	High (6, 7.5, 9)	Marginal (2, 3.5, 5)	Almost uncertain (8, 10, 10)

A Graphical User Interface (GUI) based on MATLAB platform has been developed to carry out the proposed fuzzy-based approach. A screenshot of the proposed GUI (namely "Fuzzy-based RPN calculator") is illustrated in Fig. 3.16 in case of the actual assessment of the failure mode #10.



UI Figure

FUZZY-based RPN calculator

Occurrence Fuzzy Weight: High

Severity Fuzzy Weight: Very High

Detection Fuzzy Weight: High

Defuzzified RPN*: 23.2084

Powered by:
Department of Informmation Engineering
Electrical Engineering and Measurements Lab
Measurements, Reliability and Safety group

Fig. 3. 16 - Screenshot of the MATLAB Graphical User Interface developed to rapidly implement the proposed fuzzy-based RPN estimation.

The developed GUI required six inputs for each one of the identified failure modes, namely:

- the Occurrence Fuzzy weight ω_O;
- the Severity Fuzzy weight ω_S;
- the Detection Fuzzy weight ω_D;
- the Occurrence membership function O;
- the Severity membership function S;
- the Detection membership function D.

The GUI provides two different output in the bottom side of the figure. The first one is an intuitive and effective label that stands for the defuzzified RPN^*. The second one is a plot of the FRPN membership function and its relative defuzzified value achieved using the centroid defuzzification.

In order to test and validate the performance of the proposed approach, several simulations with different weight scenarios have been run.

Figure 3.17 shows the membership functions of all the seventeen FRPN achieved using the O, S and D assessment in Table 3.5 and fixing the same weights for the three parameters, as $\omega_O = \omega_S = \omega_D = \{'High'\}$.

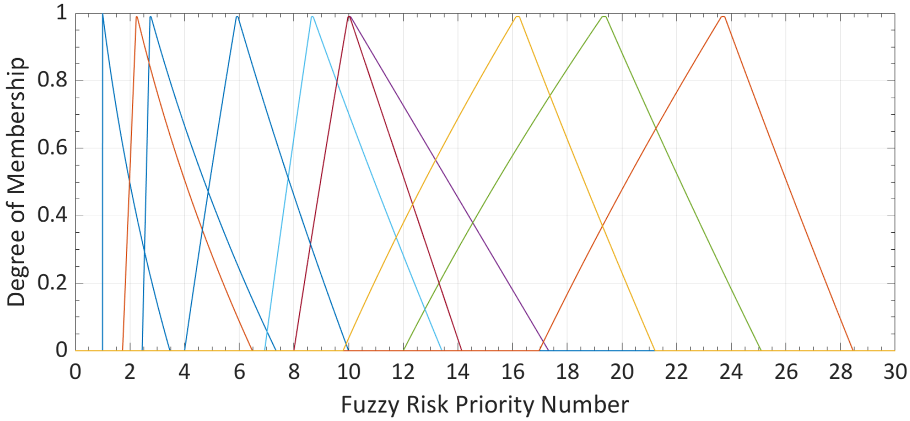


Fig. 3. 17 - Membership functions of the Fuzzy Risk Priority Number related to the seventeen identified failure mode in case of the same weights for O, S and D are set, as $\omega_O = \omega_S = \omega_D = \{'High'\}$.

The lowest FRPN are related to failure modes #7 and #8 which are both characterized by $O_{\#7} = O_{\#8} = \{'Remote'\}$, $S_{\#7} = S_{\#8} = \{'Insignificant'\}$ and $D_{\#7} = D_{\#8} = \{'Almost\ certain'\}$.

The most critical failure mode is #16 which is characterized by $O_{\#16} = \{'High'\}$, $S_{\#16} = \{'Verycritical'\}$ and $D_{\#16} = \{'Almost\ uncertain'\}$. Even if only few failure modes were investigated in this example, there are no gaps inside the range between the lowest and highest FRPN. Moreover, the only duplicates obtained are referred to failure modes characterized by exactly the same assessment of O, S and D, highlighting the ability of the procedure to solve the classical RPN drawbacks.

In Fig. 3.18 three different scenarios are compared using different colors of the bars. The same fuzzy weight is assessed to each one of the parameters in every simulation included in this figure.

In particular, in the first one $\omega_O = \omega_S = \omega_D = \{'Medium'\}$ (blue bars), in the second one $\omega_O = \omega_S = \omega_D = \{'High'\}$ (red bars) while in the third one $\omega_O = \omega_S = \omega_D = \{'Very\ high'\}$ (yellow bars). As it is possible to see in Fig. 3.18, varying simultaneously the weight of the factors the analysis provides consistent results. The ranking of the defuzzified $RPNs^*$ maintain the same ordering regardless the value of the weights.

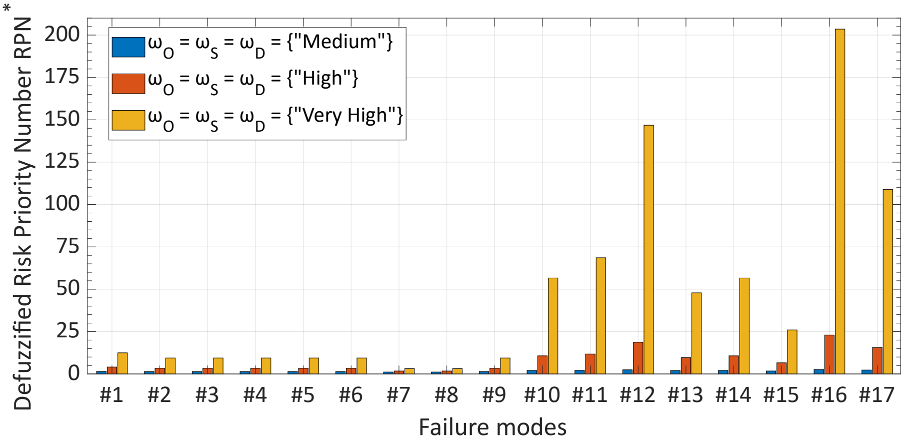


Fig. 3. 18 - Results of the proposed fuzzy-based procedure. RPNs are obtained setting the same weights for O, S and D. Three different scenarios are considered:* $\omega_O = \omega_S = \omega_D = \{'Medium'\}$ *(blue bars),* $\omega_O = \omega_S = \omega_D = \{'High'\}$ *(red bars) and* $\omega_O = \omega_S = \omega_D = \{'Very\,high'\}$ *(yellow bars).*

The only remarkable difference between the three set of data in Fig. 3.18 is the height of the bars, which stands for the defuzzified value of the RPN. In other words, when the weights of the parameters are set equal to each other, the higher the weight the higher the RPN, even if the prioritization of the mode provides the same failure ranking.

Therefore, if a designer wants to set the same weight for O, S and D, then it is advisable to use the highest possible weight (i.e. $\omega_O = \omega_S = \omega_D = \{'Very\,high'\}$) in order to distribute the $RPNs^*$ in a wider range and consequently allow an easier identification of the most critical modes.

One of the most important features of the proposed tool is the ability to set different weights to O, S and D, increasing the importance of one factor with respect the others. Consequently, the testing of the tool under this scenario plays a critical role in the validation of the procedure.

Fig. 3.19 shows a comparison between the defuzzified $RPNs^*$ firstly obtained using the same weights of the parameters $\omega_O = \omega_S = \omega_D = \{'High'\}$ (red bars) and then obtained using different weights in order to prioritize the severity, as follow: $\omega_O = \omega_D = \{'High'\}$ while $\omega_S = \{'Very\,high'\}$ (grey bars). The assessments achieved using these scenarios are quite similar to each other. The most striking result emerge comparing the failure modes #10 and #11.

Increasing the importance of the Severity, the prioritization of these two failure modes changes. Considering the same weights, failure mode #11 has a defuzzified RPN^* slightly higher than failure mode #10. When the weight of

Severity is increased up to $\omega_S = \{'Very\ high'\}$ the defuzzified RPN^* of failure mode #10 become significantly higher than the one of failure mode #11.

This is essentially due to the Severity value of failure mode #10 which is $S_{\#10} = \{'Catastrophic'\}$ while the severity value of failure mode #11 has been set to $S_{\#11} = \{'Insignificant'\}$.

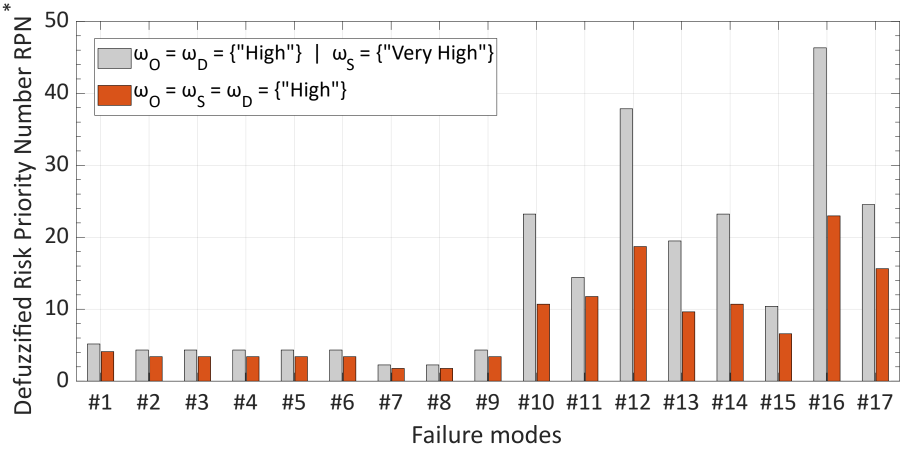


Fig. 3. 19 - Results of the proposed fuzzy-based procedure. The defuzzified RPNs are obtained using two different scenarios: same weights of the parameters $\omega_O = \omega_S = \omega_D = \{'High'\}$ (red bars) and different weights in order to prioritize the severity $\omega_O = \omega_D = \{'High'\}$ while $\omega_S = \{'Very\ high'\}$ (grey bars).*

3.11 Final remarks on Fuzzy FMECA

This paper presents an innovative fuzzy-based tool used to assess the risk of the failure mode identified during a FMECA procedure. Many papers agreed that the classical RPN suffers several drawbacks. The proposed approach aims to provide a practical and easy solution to each one of the classical RPN problems maintaining unaltered the core of the classical procedure illustrated in the international standard IEC 60812. The proposed approach succeeds in fulfill all these needs, as follow:

- The set of possible fuzzy FRPNs is still not continuous, but every crisp value within the interval between the minimum and the maximum FRPN has a degree of membership greater than 0 in at least two FRPN membership functions (as in Fig. 3.13).

- Using different membership functions and different weights for O, S and D every combination of the parameters provides a unique FRPN and consequently also a unique defuzzified RPN*, solving the duplicate issue (as in Fig. 3.13).
- The problem of high sensitivity to small changes of Occurrence, Severity and Detection is remarkably reduced in the proposed approach (as in Fig. 3.14).
- The relative importance among O, S and D is considered introducing different weights for each parameter.
- The problem of a difficult definition of O, S, D is drastically improved introducing the linguistic assessment of the parameter (as in Fig. 3.10)

Moreover, the central novelty of the proposed tool is the ability to achieve the above-mentioned target with a simple approach that could be easily applied with low cost and low computational complexity. A MATLAB-based graphical user interface has been developed to rapidly implement the risk assessment of the system under test using the proposed approach. The proposed fuzzy-based method has been applied to a receiver circuit of the onboard subsystem of an ATP highlighting optimal results.

3.12 Last problem of FMECA: threshold estimation

In the last years, many studies have been carried out to analyze the failure occurrence of railway equipment as well as to evaluate the impact of a failure on transportation (see for example [142]). Cheng et al. [143] evaluate the reliability of metro door systems using a FMECA procedures. Kim et al. [144] investigate the effects of a failure of the brake system for a railroad unit with a FMECA. Dinmohammadi et al. [142] analyze the risk associated to a passenger door system. Carretero et al. [145] uses FMECA as starting point for the development of a maintenance plan in railway infrastructure. Deng et al. [146] proposes a new framework based on FMECA method to study the vulnerability of a subway system. Marquez et al. [147] carry out a Reliability

Centred Maintenance based on FMECA for a railway turnout.

This section focuses on a Failure Mode, Effects and Criticality Analysis (FMECA) for a HVAC system in a high-speed train. A study of the HVAC's critical areas is mandatory to optimize its reliability and availability. The critical components identified by FMECA needs to be fully analyzed in order to find countermeasures and lower the risk level.

RPN parameter is used to evaluate the risk level associated to each failure mode. With this knowledge, designers can take effective actions to eliminate high risk failure modes [120], [148]. The method is simple and convenient, but its strong subjectivity and unified evaluation standards may result in inaccurate risk determination. Thus, it may have a misleading effect on establishing improvement actions. In addition, after determining the RPN risk sequence, it is necessary to implement corrective actions for the failure mode whose RPN value is higher than the acceptable risk standard.

The identification of the most critical parts is usually performed by experts, leading to a high subjective decision. Alternatively, some companies apply corrective actions in a hierarchical order starting from the most critical components. Then, countermeasures are applied until the budget allows it. The major flaw of this cost-oriented approach is that some critical risk could not be mitigated. For some application this approach is valuable, quite the opposite safety related applications such railway systems require a more precautionary point of view. Consequently, it is extremely important to identify which components are critical and which are not by means of a risk threshold.

The international standard IEC 60812 (2018) [149] which defines and standardizes the FMECA does not sufficiently explain how to univocal distinguish the non-critical modes with the critical modes which need corrective actions. Many works in recent literature highlight some drawbacks of the RPN and try to propose different methods to overcome that problems. Several papers propose different RPN formulations introducing weight factors or innovative coefficients and parameters (e.g. [96], [101]). Others solve the problems introducing fuzzy-logic or other analytical theories in FMECA, see for instance [82], [150]. However, most of the papers does not deal with the RPN threshold estimation problem. Therefore, one of the major aims of this work is to fill this gap proposing a methodology for threshold estimation regardless the application field or the mathematical model used to calculate the RPN.

Usually the threshold for the modes is subjectively set by the judgement of multiple experts in the matter (see for instance but not only [104], [151]–[153]), and only few papers propose their own approaches for the threshold value.

Bluvband et al. [154], [155] highlight for the first time that RPNs follows a trend and recommend a graphical tool for RPN analysis. Firstly, the RPN are plotted ordered from the smallest to the largest. Bluvband illustrates that the RPNs of a complete FMECA form a right-skewed distribution, the critical modes belong to the upper-right part while the negligible modes to the first tail on the left. The threshold value is calculated in a qualitative way by the division between the negligible failure modes and the critical failure modes. The method proposed by Bluvband [154], [155] is an intuitive and simple graphical tool. The idea at the basis of this approach seems to be very interesting. The main concern of the method is related to the subjectivity for the division of the two datasets characterized by different slopes.

Zhao et al.[156] propose a method to obtain a more objective and accurate RPN analysis. The RPNs are plotted ordered by size, then using linear regression the RPNs are fitted with a polynomial approximation of the first order, finally the confidence levels are plotted on the same figure. The threshold RPN is determined by the turning point from the confidence levels (i.e. the first RPN point coming out the confidence bounds). This approach is based on a simple linear approximation method, but in many practical cases the RPNs do not follow a linear trend. Therefore, the approximation of the values with a single straight line provides a significant error.

Another procedure to evaluate the threshold value is the 80:20 Pareto principle [157]–[159]. According to this technique, 20% of failure modes produce 80% of the total RPNs. In contrast to the Bluvband method, the Pareto approach uses a bar chart where the failure modes are sorted from the highest risk priority number to the lowest. This bar graph is combined with a cumulative distribution function that shows the percent contribution of all preceding failures. The 80:20 rule is used to distinguish the negligible and critical modes. Pareto chart is not suitable for some kind of risk-assessment application because it is not always verified that the 80% of the criticalities arise from 20% of the causes, or in other words that the 80% of the RPNs represents the 20% of the failure modes.

A comparative analysis has been published in [54] where a statistical approach based on a boxplot was compared with the other method proposed in literature. The method proposed in [54] could be used as a first screening of the failure modes, while a more accurate and quantitative approach is required in case of safety-critical system (such railway systems).

3.13 A new approach for the threshold estimation

The failure modes characterized by high RPNs have to be distinguish from the modes with lower RPN values. As explained, very few papers in literature deal with this concept. Therefore, a new analytical approach is introduced in this section to overcome the subjectivity and to find a RPN threshold value.

3.13.1 Description of the procedure

Figure 3.20 shows the flowchart of the proposed procedure.

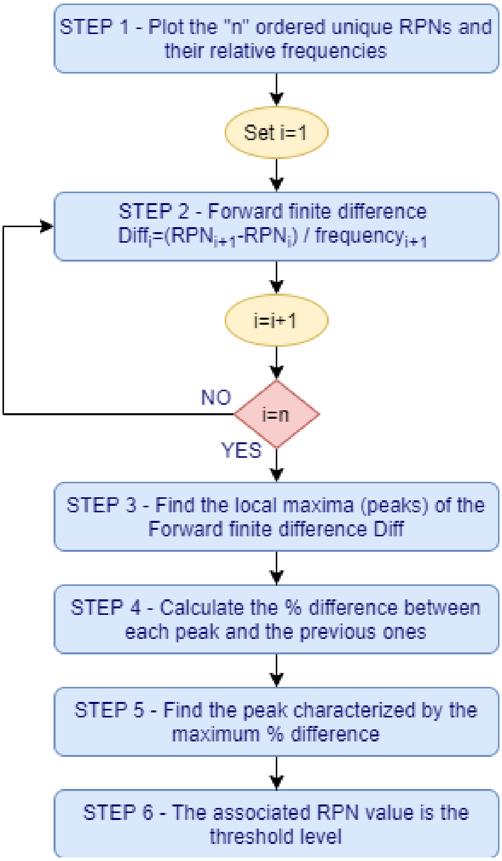

STEP 1 - Plot the "n" ordered unique RPNs and their relative frequencies
Set i=1
STEP 2 - Forward finite difference
$Diff_i=(RPN_{i+1}-RPN_i) / frequency_{i+1}$
i=i+1
i=n
NO
YES
STEP 3 - Find the local maxima (peaks) of the Forward finite difference Diff
STEP 4 - Calculate the % difference between each peak and the previous ones
STEP 5 - Find the peak characterized by the maximum % difference
STEP 6 - The associated RPN value is the threshold level

Fig. 3. 20 - Flowchart of the new procedure for Risk Priority Number threshold estimation

The first step requires to consider the frequency of each RPN, i.e. the repetition number of each RPN.

For each unique RPN the forward finite difference is calculated. Then the difference is weighted with the size of the sample (frequency of each unique RPN).

In particular, the weighted finite difference $Diff_i$ is defined as the ratio between the forward finite difference of the unique RPN and the frequency of the unique RPN, as follow:

$$Diff_i = \frac{RPN_{i+1} - RPN_i}{frequency_{i+1}} \tag{3.14}$$

where RPN_{i+1} and RPN_i represent the *(i+1)-th* and the *i-th* unique failure modes respectively, while $frequency_{i+1}$ stands for the repetition frequency of the *(i+1)-th* unique RPN.

As the first derivative of a continuous function represents the instantaneous rate of change, the finite difference represents the same concept for discrete data set. So, the higher is the difference, the higher is the variation between two consecutive values. The forward finite difference introduces the repetition of the RPN value as denominator in order to take into account how the repeated values lower the increment. The following step is the identification of the local maxima (peaks) of the finite difference $Diff$. Each peak represents a remarkable increase of two nearby RPNs, the higher the peak the greater the RPN increase. The aim of the proposed procedure is to precisely identify a value that divides the ordered RPNs trend in two different groups: the negligible modes characterized by a gradual change of the RPN values, and the critical modes characterized by a sudden increase of those value. Consequently, the identification of the peaks in the finite difference trend is a fundamental step that allows to quantitatively understand the RPN increments.

Then, the following steps are used to identify the *"first significant peak"*, which is the peak that divides the RPNs into two well-defined and different subsets. In order to find this peak, the proposed procedure is based on the evaluation of the percentage difference $\Delta Peak_i$ between each peak and the previous ones (step 4). More in detail, equations (3.15)(3.16) explain the evaluation of percentage increment between the peak i and the mean value of the three previous peaks PP_i.

$$PP_i = \frac{Peak_{i-1} + Peak_{i-2} + Peak_{i-3}}{3} \tag{3.15}$$

$$\Delta Peak_i = 100 \cdot \frac{Peak_i - PP_i}{PP_i} \, \% \tag{3.16}$$

Then, step 5 consists in the identification of the maximum value of the percentage differences evaluated in the previous step. The peak characterized by the maximum value of percentage difference is the *"first significant peak"* and the associated RPN divides the dataset into two subsets.

The evaluation of $\Delta Peak_i$ as the simple increment between the peak *i* and the peak *i-1* could lead to untrustworthy results since the percentage increase is great enough also for the lower peaks. Moreover, comparing each peak with the same constant value (e.g. the minimum peak, or the first peak, or the first finite difference value, etc.) leads always to identify the peak with the greater value, regardless the dataset.

As explained before, the aim of this procedure is not to identify the highest peak, instead it is to identify the first peak much higher than all the previous peaks. Consequently, $\Delta Peak_i$ has been evaluated as the percentage difference between a peak and a small set of previous peaks. More in detail, the mean value of the three previous peaks was used since it provides effective results in several datasets.

The final step consists in the identification of the unique RPN which divides the dataset into two subsets. The index of the *"first significant peak"* is the index of the unique RPN associated to the threshold level.

The proposed approach uses the idea of the identification of two different data set but allows to delete the subjectivity issue that influences most of the previous works using an analytical procedure based on weighted forward finite differences.

The following subsections illustrates the application of the procedure to different FMECAs. Firstly, the proposed procedure has been applied to the "Passenger unit" FMECA described in the previous section. Then, it has also been applied to the "Cabin unit" FMECA in order to validate the method with a different dataset.

3.13.2 Preliminar Risk Analysis Of HVAC

Figure 3.21 shows the location of the train's HVAC system [160], [161]. There are two units located on the roof of the train: one for the cabin area (called "Cabin unit" in the following) and another one for the passenger area or salon (called "Passenger unit" in the following) [162]–[164].

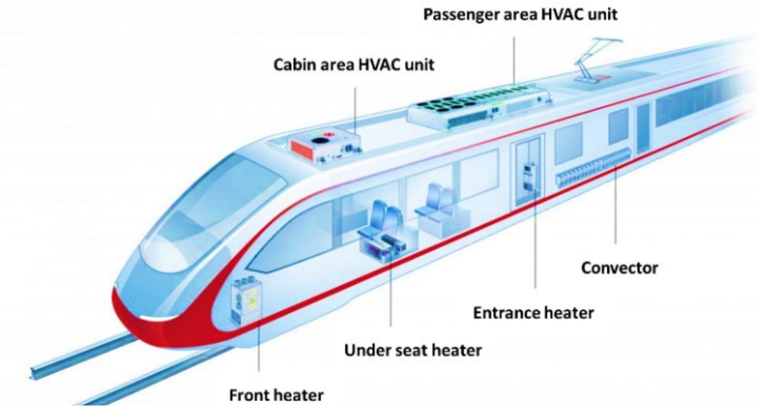


Fig. 3. 21 - Examples of HVAC units located on a high-speed train

The system under analysis is an HVAC assembly in S-121, a high-speed train. Table 3.6 describes the high level taxonomy of the HVAC under study, according to ISO 14224 [165].

Tab. 3. 6 -High-level taxonomy of the system under test

Taxonomy level	Taxonomy hierarchy	Description
1	Industry	Railway
2	Business Category	High Speed
3	Installation	S121
4	Unit	Front car
5	System	HVAC system

Figure 3.22 shows a block diagram of the "Passenger unit" HVAC under analysis. In particular it is composed by four different sub-systems: cooling, heating, ventilation and control system. The cooling and heating systems aim is to provide a thermal comfort inside the train (the cooling provides air-conditioned while the heating increases the temperature), ventilation provides fresh air and finally the control has to regulate and manage all the other devices. Each system is also divided into several subunit as shown in the figure.

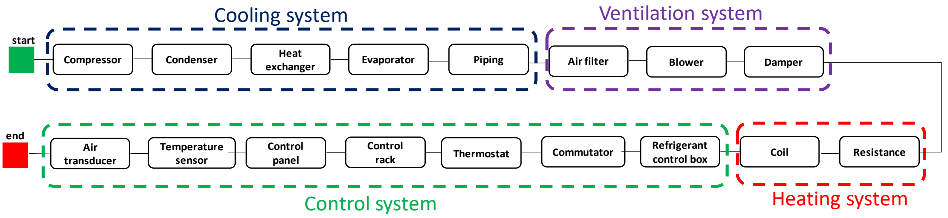


Fig. 3. 22- Block Diagram of HVAC under study

The “Cabin unit” is a bit different from the “Passenger unit”. It is simpler, it is composed by a lower number of components and it uses the control system integrated in the “Passenger unit”.

Classification criteria are used to consistently attribute the level of severity, occurrence and detection to each failure mode. These criteria are established in part from the literature and others are specifically chosen for the type of device analyzed. Table 3.7 illustrates the criteria for the choice of the severity index, Table 3.8 gives the criteria for the assignment of occurrence values and Table 3.9 shows the assessment of the detection value. The above-mentioned tables were developed to analyze both “Passenger unit” and “Cabin unit”.

Tab. 3. 7- Criteria for Severity S assessment

Severity	**Criteria**	**Rating**
None	No discernible effect	1
Very minor	Comfort reduction	2
Minor	Possible failure of one component	3
Very low	Partial loss of one function	4
Low	Considerable loss of one function	5
Moderate	Loss of one function	6
High	Loss of two functions	7
Very high	Loss of all function	8
Hazardous with warning	Possibility of fire	9
Hazardous without warning	Loss of safety without warning	10

Tab. 3. 8- Occurrence O evaluation criteria based on failure rate

Failure mode occurrence	**Rating**	**Failure rate λ_M [FPMK]**
Remote: Failure is unlikely	1	$\leq 1 \cdot 10^{-5}$
Low: Relatively few failures	2	$1 \cdot 10^{-4}$
	3	$5 \cdot 10^{-4}$
Moderate: Occasional failures	4	$1 \cdot 10^{-3}$
	5	$2 \cdot 10^{-3}$
	6	$5 \cdot 10^{-3}$
High: Repeated failures	7	$1 \cdot 10^{-2}$
	8	$2 \cdot 10^{-2}$
Very High: Failure is almost inevitable	9	$5 \cdot 10^{-2}$
	10	$\geq 1 \cdot 10^{-1}$

Tab. 3. 9- Detection D evaluation criteria

Criteria	**Rating**
Completely detectable	1
Partially detectable	2
Impossible to detect	3

A severity rank is allocated to each failure mode based on the severity of the effect on the overall system performance and safety in light of the system requirements, objectives and constraints [149].

Table 3.8 propose the assessment of the occurrence based on the mode failure rate value. If λ is the failure rate of the component, then the mode failure rate λ_M is given by:

$$\lambda_M = \alpha \cdot \lambda \tag{3.17}$$

Where the failure rate fraction expressed by α represents the weight of the mode compared to the other failure modes. In particular, a 1-to-10 scale is assessed, where the higher is the mode failure rate, the higher is the occurrence rate. The failure rate is generally expressed in failure/hour, but for this application, the information on time is less meaningful than distance. In fact, trains only work certain hours, so the information on the distance travelled is more important and more significant than time. Therefore, the failure rate of the mode in Table III are expressed in FMPK - failures per million kilometers.

Table 3.9 gives the detection criteria used in the case study. Since detection data were barely available for the HVAC system under study, the proposed scale varies from 1 to 3.

Table 3.10 shows an extract of the whole FMECA for the “Passenger unit” of the HVAC system studied. The columns report the following information:

- Failure mode description: manner in which an equipment or machine failure can occur.
- Failure rate fraction (α): a percentage which describes the weight of each failure mode in the component. The sum of every failure rate fraction has to be 100%.
- Failure rate for failure mode (FPMK): frequency with which the failure mode appears, expressed in failures per million kilometers.
- Failure causes: causes of the failure mode.
- Local effect: normally limited to the effects on the item exhibiting the specific failure mode.
- Global effect: effects of the failure as it would be seen at the next higher/lower level (within the system/ equipment structure).
- Occurrence (O): rating of the likelihood of occurrence of each cause of failure
- Severity (S): rating of the severity of each effect of failure
- Detection (D): rating of the likelihood of prior detection for each cause of failure (i.e. the likelihood of detecting the problem before it reaches the end user or customer.
- Risk priority number (RPN): product of the three ratings.

Failure data were provided by the HVAC manufacturer “MERAK.” Note that data do not consider any stress applied. The whole “Passenger unit” FMECA is composed of 109 different modes and table 3.10 shows only an extract of them. The result of the whole FMECA are reported in Figure 3.23 which illustrates all the 109 Risk Priority Number ordered by size from the smallest to the largest, to improve the readability of the values. The minimum RPN value is 3, associated to the relay, and the maximum is 216, associated to the blower. The figure also highlights several duplicates in the risk priority number scale, in particular the maximum repetition frequency is related to RPN 72, which can be formed by 14 different combinations.

Tab. 3. 10 - Extract from the whole FMECA for the "Passenger unit" of the HVAC system under analysis

Failure mode	α	Failure rate [FPMK]	Cause of failure	Local effect	Global effect	O	S	D	RPN
COMPRESSOR									
Motor seizes up	60%	1,68E-02	-Internal failure -Blocked compressor -Damage winding	Loss of pumping capacity	Loss of cooling function	8	6	3	144
Thermostat doesn't detect temperature over limit	2%	5,62E-04	-Overheating of compressor -Thermostat dirty	Loss of overheating protection	Possible damage of compressor	3	5	3	45
Pumping leakage	25%	7,02E-03	-Mechanical failure -Fretting compressor	Loss of refrigerant pumping	Loss of cooling function	6	6	3	108
Valve fails to close	8%	2,25E-03	-Internal failure -Valve dirty	The refrigerant doesn't increase the pressure	Loss of cooling function	5	6	3	90
Internal overload motor protection	5%	1,40E-03	- Motor is short circuit -Electric overload -Motor protection failure	Short circuit of compressor	Loss of cooling function	4	6	3	72
HIGH PRESSURE SWITCH									
Pressure switch in close position	30%	3,08E-03	-Internal failure of the pressure switch -Dirtiness in the refrigerant circuit	No detection in case of high pressure of refrigerant	Possible overpressure	5	5	3	75
Pressure switch in open position	50%	5,13E-03	-Internal failure -Dirtiness in the refrigerant circuit	Incorrect indication of overpressure	Compressor is stopped	6	6	3	108
Refrigerant leakage	20%	2,05E-03	-Refrigerant leakage in the distributor	Leak of refrigerant in the component	Compressor is stopped	5	6	3	90
EVAPORATOR COIL									
Refrigerant leakage	100%	1,04E-02	-Presence of corroded or critical zones	Leak in the component	Loss of cooling function	7	6	3	126
EXPANSION VALVE									
Refrigerant leakage	80%	4,62E-03	-Presence of corroded or critical zones	Leak in the component	Loss of cooling function	6	6	3	108
Valve is not opened	5%	2,89E-04	-Internal failure	Expansion valve is blocked close	Loss of refrigerant circulation	2	6	3	36
Valve is not closed	15%	8,67E-04	-Internal failure	Expansion valve is blocked open	No expansion of refrigerant	4	5	3	60

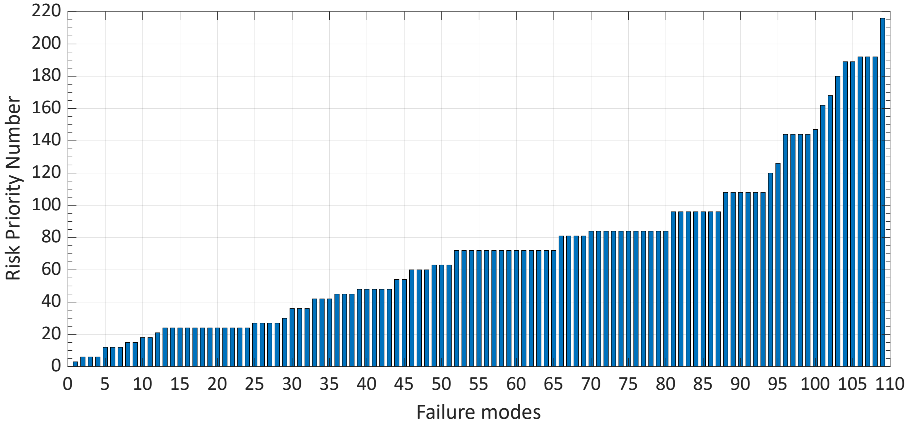


Fig. 3. 23- Representation of the whole "Passenger unit" FMECA result. All the RPNs are plotted ordered by size

Also, the "Cabin unit" of the HVAC system was analyzed using the FMECA procedure. The complete results were not reported in this work for the sake of brevity. In this second analysis, the minimum RPN value is 4, associated to the pipes, and the maximum is 168, associated to the emergency inverter. Also, in the "Cabin unit" FMECA there are several duplicates in the risk priority number, in particular the maximum repetition frequency is for the RPN 12, which can be formed by 12 different combinations.

3.13.3 Case study 1: HVAC passenger unit

In this section the procedure is applied to a first case study, so the data coming from the "Passenger unit" FMECA are used to test the effectiveness of the proposed method.

Figure 3.24 shows the first step of the procedure. The height of the bar represents how the RPN (in the abscissa) is repeated in the FMECA, the higher is the bar more frequent is the mode. This plot helps to identify all the unique RPNs and their relative number of repetitions. The value of RPNs unique numbers (the number of bars in fig. 3.24) is $n = 31$ so the finite difference $Diff$ will be composed by 30 elements.

The top plot of fig. 3.25 illustrates the steps from 2 to 5 of the procedure carried out on the "Passenger unit".

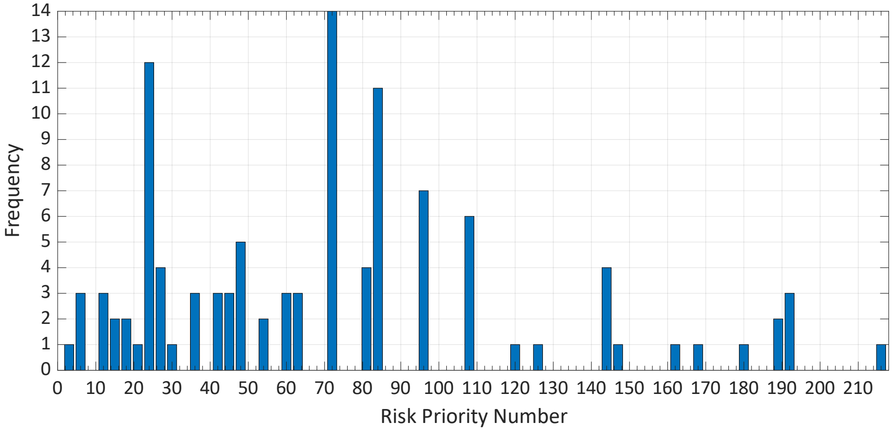


Fig. 3. 24 - Step 1: repetition number of each RPN value.

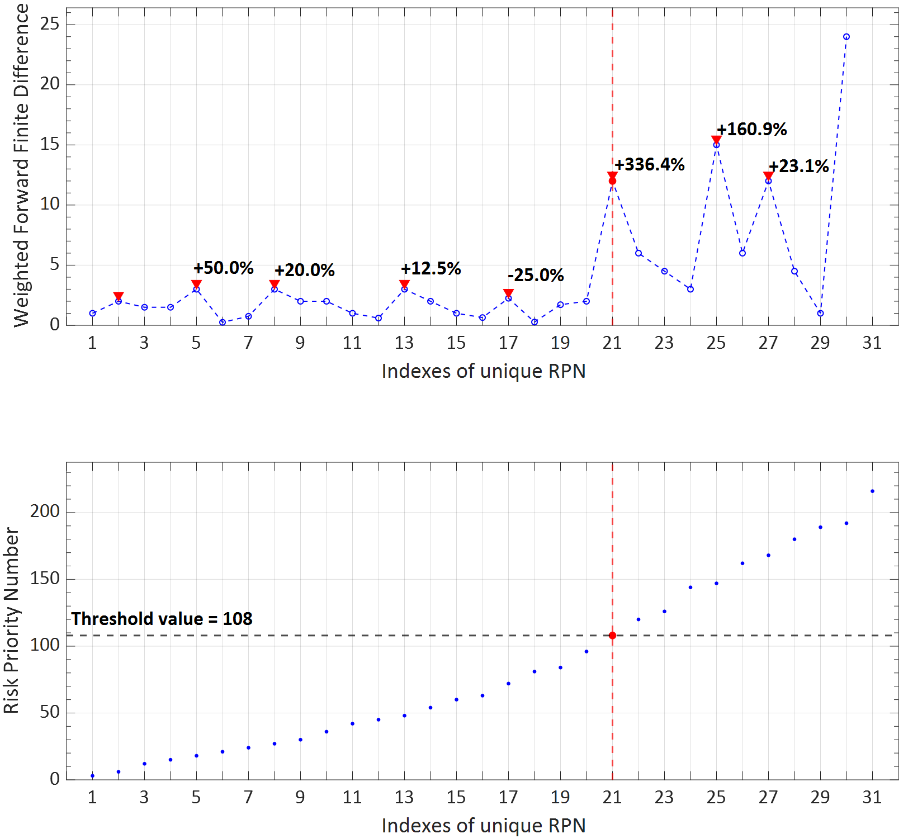


Fig. 3. 25 - Application of the proposed procedure to the "Passenger unit" of the HVAC. The top plot illustrates the steps from 2 to 5 of the procedure, while the bottom plot is used to carry out the final step.

The forward finite differences have been calculated, then the values have been illustrated as blue dots in the top subplot of figure 3.25. The figure highlights that the first twenty markers are lower than 3, while the 21st value is very different respect to the others. This high value represents a significant difference between the 21st and 22nd unique RPNs, which involves a rapid increase of the subsequent ordered RPN. In the top graph of Fig. 3.25 the peaks are marked using red triangles, 8 peaks were identified in the "Passenger unit" FMECA.

Near each peak there is a label indicating the percentage difference $\Delta Peak_i$ between this peak and the three previous peaks. The index of the *"first significant peak"* is the one that corresponds to the maximum value of $\Delta Peak_i$. It is highlighted using a red dotted line, which indicates the index of the unique RPN associated to the threshold level. The final step is illustrated on the bottom plot of fig. 3.25, which corresponds to the identification of the RPN threshold value. This graph highlights that the corresponding RPN to the 21th index is the value 108, which will be the threshold value.

All the RPNs higher than the threshold have to be considered critical, while all the RPNs lower than or equal to 108 are considered negligible. Figure 3.26 shows all the values of RPN evaluated for the "Passenger unit" FMECA (the same data of Figure 3.23) and the threshold line (black dotted line). All the RPNs below the threshold are illustrated using green dots and are considered negligible, while the red dots stand for the RPNs above the threshold which are considered critical.

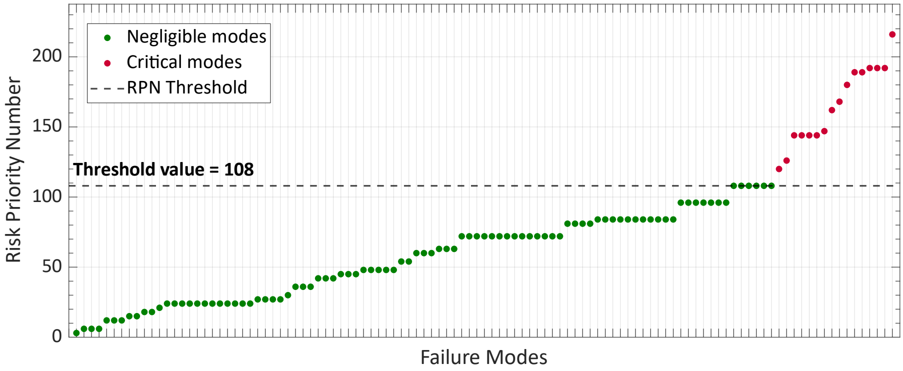


Fig. 3. 26 - Division of Risk Priority Numbers identified in the "Passenger unit" FMECA in negligible and critical values.

In the “Passenger unit” FMECA, 16 out of 109 failure modes were found unacceptable. This means that nearly 15% of the failure modes require some sort of corrective action.

3.13.4 Case study 2: HVAC cabin unit

This subsection tests the proposed procedure with another set of data coming from the cabin unit of the same HVAC. A FMECA has been developed and the resulting RPNs are used as input of the method (See Fig. 3.27).

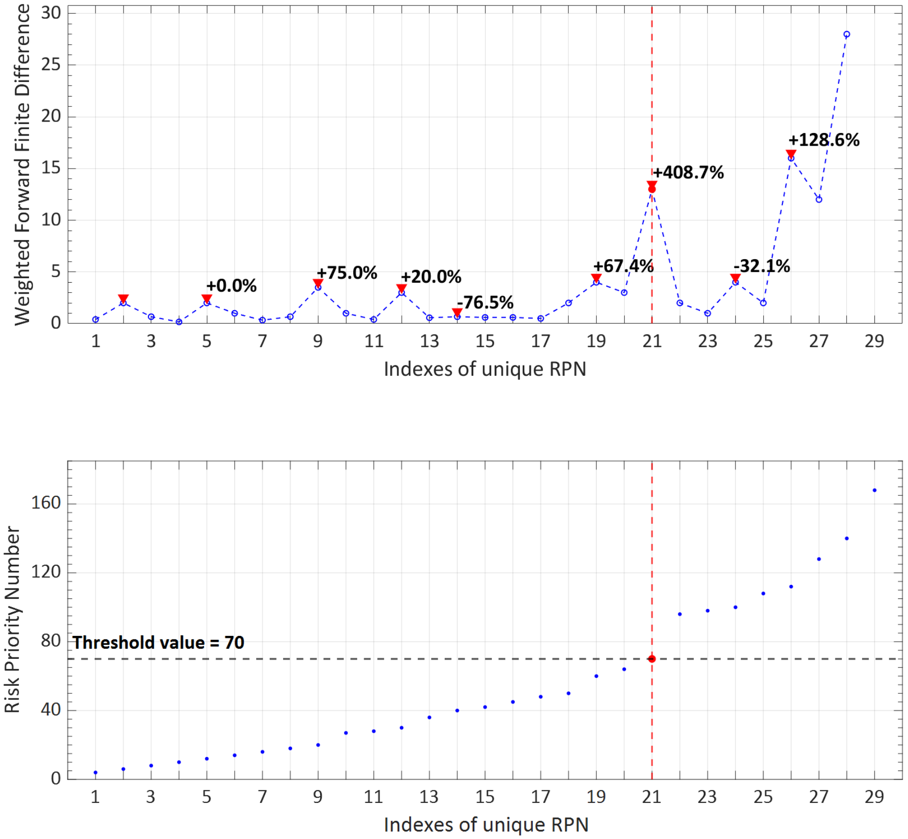


Fig. 3. 27 - Application of the proposed procedure to the “Cabin unit” of the HVAC. The top plot illustrates the steps from 2 to 5 of the procedure, while the bottom plot is used to carry out the final step.

The top plot of figure 3.27 shows the trends of the forward finite differences (step 2). The peaks are highlighted by red triangles (step 3), and from a qualitative point of view it is possible to note a sudden increase of the difference between the 20th and 21st unique RPN. To quantitative identify the first significant peak, step 4 and 5 are used with this dataset. Clearly the highest variation is the 21st unique RPN with a 408.7% increase.

Then step 6 allows to identify the threshold value associated to the 21st unique RPN, the bottom of figure 3.27 shows all the unique Risk Priority Numbers and their indexes. The threshold associated to the 21st index is the RPN=70.

Figure 3.28 shows all the Risk Priority Numbers as dots and the threshold limit. In this case study the method identifies 12 critical failure modes over 90 total modes. So, in this case the 13% of the modes needs to be mitigated.

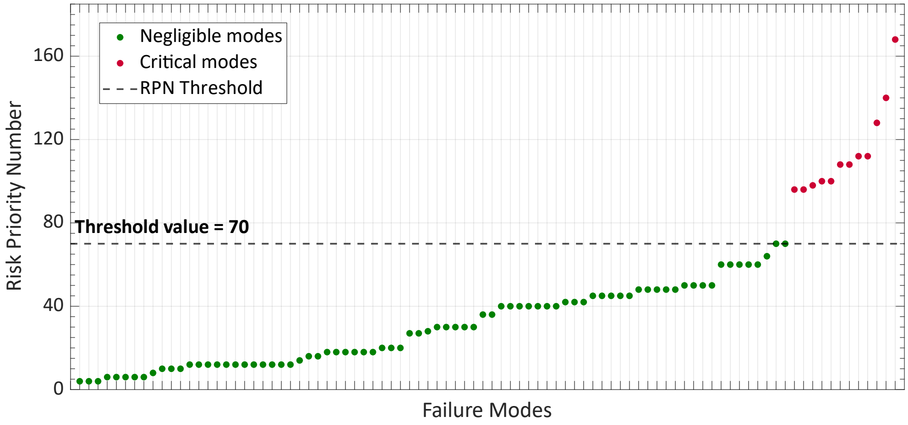


Fig. 3. 28 - Division of Risk Priority Numbers identified in the "Cabin unit" FMECA in negligible and critical values.

3.13.5 State of the art comparison

Finally, the proposed procedure was compared with the other approaches available in literature. The results achieved for both case studies are summarized in table 3.11 which includes the RPN threshold value and the number of critical failure modes.

The comparison firstly highlights the inadequacy of Zhao and Pareto approaches for this kind of application.

Tab. 3. 11 - Results comparison achieved using the proposed method and the other method available in literature

METHOD	**Case study 1**		**Case study 2**	
	RPN_{th}	**Critical modes**	**RPN_{th}**	**Critical modes**
Proposed method	**108**	**16**	**70**	**12**
Bluvband [154]	105	22	57	20
Zhao [156]	177	7	124	3
Pareto [157]–[159]	63	60	36	45
Boxplot [54]	96	29	50	24

In both the case studies, the method proposed by Zhao identifies the highest RPN threshold, on the other hand the 80-20 Pareto principle identifies the lowest value. Such high threshold, given by the Zhao method, could not be reasonable in many safety-related applications, because it requires a risk mitigation only for few modes. While the low threshold given by the Pareto principle requires an expensive plan for the risk mitigation of the modes, that could be not applicable for many companies.

The proposed method provides intermediate results, in line with the threshold proposed by Bluvband, mostly because both start from the same idea.

The main advantage of the proposed approach is that it completely deletes the subjectivity, still present in Bluvband.

Finally, several kinds of risk mitigation actions could be taken into account in order to lower the Risk priority number above the threshold.

A very efficient improvement is to get some changes in the design of the equipment by using components with improved quality and performances, this will lower the failure rate of the component and consequently the occurrence, but it leads to a cost impact for the industry. The use of condition monitoring (sensors which monitor the state of the system) allows to monitor the health state of the system and to diagnose failure before it occurs. So the introduction of these maintenance tools lowers the detection index. Also the use of redundancy system allows to obtain a lower Risk Priority Number, but this solution needs high cost to be performed.

3.14 Final remarks

This chapter starts with the analysis of RCM which is a very useful and used technique for the maintenance planning. However the standard proposes a decision-making diagram very flexible and not unique; consequently the maintenance task chosen strongly depends on the experience and judgment of the analyst. Section 3.4 proposes a new approach based on a fuzzy FMECA and a new decision diagram which univocally leads the analyst to only one maintenance task.

FMECA is the core of RCM, and is a technique characterized by several issues widely discussed in Section 3.8. There are a lot of studies on FMECA and fuzzy FMECA, however there is not a single and easy technique which solves all the mentioned problems.

A new Fuzzy FMECA approach has been presented in Section 3.9. Thanks to weight factors it is possible to solve the problems of high sensitivity and the importance of O, S and D. Furthermmore the fuzzy logic allows to minimize the subjectivity of the method and the output dataset results to be a set of continuous RPNs and to have all unique values (solving the duplicate problem).

Finally, literature miss to consider a technique to distinguish critical and negligible failure mode in a non-subjective way. Section 3.13 introduces an analytical procedure to identify a Risk Priority Number threshold. The method allows to evaluate with a mathematical tool a threshold value considering critical all the failure modes characterized by a RPN higher than the threshold, while failure modes characterized by RPN lower than the threshold are considered negligeble.

CHAPTER 4

HUMAN FACTOR IN RAILWAY ENGINEERING

This chapter provides an introduction of the Human factor topic. It starts with the aim of human reliability, then it focuses on the evolution of HRA. HRA is developed into three generations depending on the year of publication. Second generation techniques try to overcome the limitation of the first generation while third generation introduces dynamic models and novelties to overcome the second generation. The final part of the chapter is dedicated to an exhaustive literature review of the HRA in railway in the last two decades. [1,2,3]

[1] Part of this chapter has been published as "L. Ciani, G. Guidi, G. Patrizi, and D. Galar, Improving Human Reliability Analysis for railway systems using fuzzy logic, *IEEE Access*, vol. 9, pp. 1–1, 2021".

[2] The other part has been published as "M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, An enhanced SHERPA (E-SHERPA) method for human reliability analysis in railway engineering, *Reliab. Eng. Syst. Saf.*, vol. 215, p. 107866, Nov. 2021".

[3] The literature review of the last two decades has been published as "L. Ciani, G. Guidi, and G. Patrizi, Human reliability in railway engineering: literature review and bibliometric analysis of the last two decades", Safety Science, article in press, 2022".

4.1 Human Reliability: what and why?

There are many disasters of the modern era caused by human error or by the combination of it with system failures. For instance, Seveso (1976), Three Mile Island (1979), Bhopal (1984) and Chernobyl (1986), are among those that have most shaken public opinion. The list of accidents attributable to human error is very long, estimates indicate that the errors committed by operators are responsible for 60-90% of accidents, depending on the industrial sector taken into account, while the remaining 40-10% is attributable to technical, structural and failure deficiencies [166]–[168].

Disasters and accidents are the most obvious result of human error, however small deviations, which do not affect safety (of the system, operator, population or environment), can seriously reduce operational performance in terms of productivity and efficiency. In fact, errors affect the rejection rate of the product, thus increasing production costs and reducing sales[169].

It is evident that human error is an extremely vast and multidisciplinary topic (involving psychology, medicine, engineering, etc.) of fundamental importance for the railway industry from safety, performance and economic revenues point of views. It is therefore plausible the interest in the need to carry out interventions that tend to neutralize or minimize the occurrence of the following scenarios in which a human error could onset accidental events compromising their own safety and / or that of others:

- Behavior characterized by non-compliance with regulatory rules.
- Negligent behavior by incompetent operators.
- Uninformed operators.
- Distracted operators.
- Operators not very sensitive to their responsibilities.

This strong interest about the study of human errors has led to the birth of the Human Reliability Analysis (HRA). HRA was firstly introduced in the nuclear energy sector, where human error can cause very serious accidents [167]. The main objective of HRA is the calculation of the probability that an operator can perform a given operation incorrectly [170], leading to the concept of Human Error Probability (HEP). The HRA allows to maximize human performance within the system, with the aim of decreasing the probability of error occurrence in order to maintain and improve the safety of the system itself. Therefore, it represents a very important and critical part of the entire

RAMS (Reliability Availability Maintainability Safety) process.

The definition of reliability of a system or component reads "probability that a device will maintain its performance unchanged over time, fixed the conditions of use"[171]. In HRA this concept has been extended also to the human being. In fact, the operator must be seen as an integral part of the system and thus it is subjected to failure. Furthermore, it is important to pooint out that the conditions of use are critical in reliability analysis both for the system (temperature, humidity, vibrations, thermal gradients, etc.) and for the operator (ergonomics of the spaces, time available, microclimate, etc.).

The railway transport is a very complex transport system in which many technological aspects involve human intervention, in terms of design, construction, operation, management, maintenance and regulation. As in other industrial sectors, it is difficult to study the impact of human performance, as every accident arises from the combination of numerous errors and shortcomings that include organizational policy, procedures, human actions and equipment. It is important to underline that, very often, the systems used by the Conduct Personnel have integrated solutions for correction or mitigation of human error (ATP - Automatic Train Protection), in this case it therefore becomes highly unlikely to cause an accident. The human errors that are decisive for the safety of the system lie mainly in the design and/or installation and/or verification phases of the safety and driving assistance systems [172].

4.1.1 Human error classification

Human error is a phenomenon that has been extensively analyzed by scholars of cognitive science. James Reason, in his book "Human Error" gives the following operational definition: *"... error will be understood as a generic term to encompass all cases in which a planned sequence of physical or mental activities fails its purpose, and when this failure cannot be attributed to the intervention of some random agent."*

At the same time, Reason provides a model for the classification of human errors. This model is based on the assumption that an action is considered correct when three conditions occur:

- The user intended to act.
- The action is processed as desired.
- The action has achieved its purpose.

If all these conditions do not occur, then an error has occurred. Reason has identified four basic types of errors [173]:

- Intentional but wrong action ("errors" or "mistakes"): occurs when the user acted with intention, the action took place as he had planned, but did not achieve the intended purpose. In essence, the user performed an action believing that it led to a certain result, but this was not the case.
- Unintentional action ("lapsus" or "slips"): A lapsus occurs when one action is involuntarily performed in place of another. Lapses are very frequent and can occur especially when the correct action and the wrong action "resemble each other". For example when two buttons are physically close. Or when two different tasks have in common an initial sequence of actions, and the final sequence in one case is performed infrequently, and in the other very often. Lapses can be avoided (or otherwise made unlikely) by designing the system so that these situations do not occur.
- Spontaneous action: in this case, the action is carried out intentionally, but without the user having previously intended to act. For example, when someone suddenly throws an object at us and, almost by an automatic reflex, we grab it on the fly, or protect ourselves with our hands. The action was not planned, but we found ourselves in the need to carry it out. A spontaneous action is not necessarily classified as an error, it is such only when it produces undesirable effects.
- Involuntary action: in this case, the action is completely unintentional (for example, involuntarily bumping into a person or object).

Despite the Reason classifications is detailed and structured, in recent literature the widest used classification model is the one provided by Jens Rasmussen in his volume "Skill, Rule and Knowledge Model". According to the Rasmussen model, three types of behavior must be considered [174]:

- Skill-based behavior: routine behavior based on learned skills. The cognitive effort required is very low and the reasoning is unconscious, that is, the action of the operator in response to an input is carried out almost automatically.
- Rule-based behavior: behavior guided by rules that the operator has to

follow performing a known task. It is a matter of recognizing the situation and applying the appropriate procedure for the execution of the task. Cognitive engagement is higher with respect to the previous case since it implies a certain level of known reasoning.

- Knowledge-based behavior: behavior aimed at solving problems in the presence of non-habitual and known situations. That is new or unexpected scenarios for which there are no specific reference rules or procedures. This type of behavior is called knowledge-based precisely because it requires a high cognitive commitment in the search for an effective solution.

From the combination of the studies carried out by Reason and Rasmussen originates the modern classification of the types of human error. It divides errors into seven different categories, as shown in Fig.4.1.

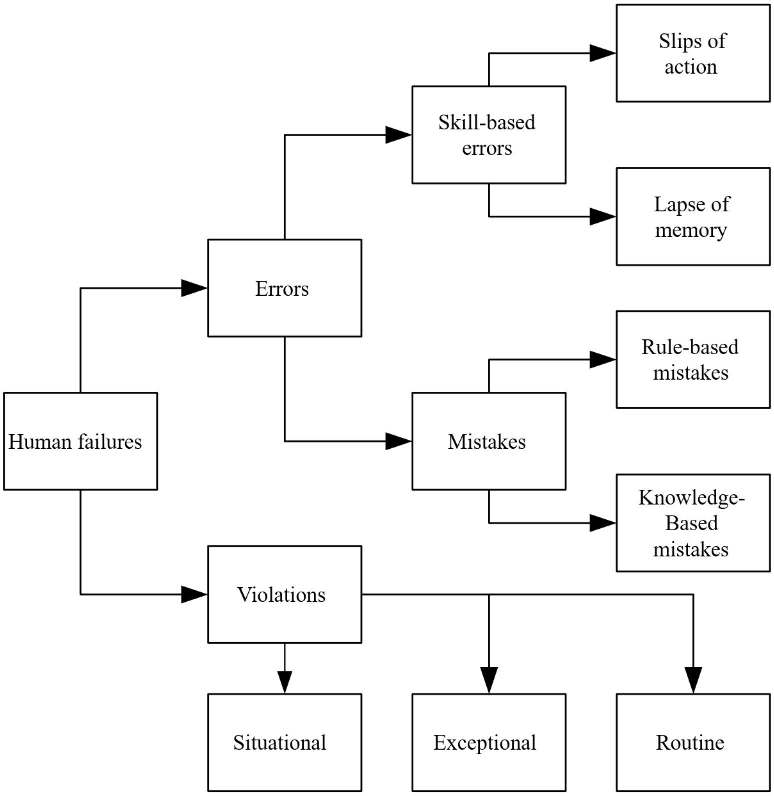


Fig. 4. 1 - Error classification based on Reason-Rasmussen theory.

According to the Reason-Rasmussen model in Fig. 4.1 human failures can be classified as:

1. **Error**: An unintentional action that compromises the execution of a task. The "errors" can be distinguished in [174]:

   a) **Skill-based errors**: failure in the execution of a scheduled action. Specifically, it refers to the application of routine skills, according to previously assimilated rules or in well-known situations. An error in this area takes the form of:

      - Lapsus in the execution of an action ("**slips**"): action performed differently than planned.
      - Memory lapses ("**lapses**"): "empty" memory (the operator forgets to perform a certain operation).

   b) **Mistakes**: "failure" in the design of a task (even if the scheduled tasks were executed correctly, it would not be possible to achieve the desired result).

      - **"Rule-based" mistakes**: errors due to the choice of a wrong rule due to a wrong perception of the situation, or in case of a mistake in the application of a rule. The operator is faced with a situation in which the focus is on a problem of decision making or the creation of a solution. However, these are known situations, which the person has been trained to cope with. Therefore, the error takes the form of an incorrect assessment of the situation or solution.
      - **"Knowledge-based" mistakes**: errors due to lack of knowledge or their incorrect application. The negative result of the action lies in the erroneous knowledge that determined it. This type of error is inherent in the limited rationality or in any case in the difficulty of giving answers to problems that present a wide range of possible choices.

2. **Violations**: deliberate transgression of a rule, procedure, norm, etc. This is the case of all those circumstances in which the procedures established for the execution of a certain task are deliberately

"circumvented" (and considered correct to carry out what was planned in the best possible way), instead of putting them into practice as planned. Violations are classified as follows [174]:

a) **Routines**: violations that have become part of a person's routine, but generally tolerated because they generally have no significant consequences (for example, slightly exceeding the speed limit while driving).
b) **Situational**: violation caused by the conditions in which the operator performs his work (such as excessive pressure to which the operator is subjected while has to complete an operation, or difficulty in complying with a certain rule in specific circumstances).
c) **Exceptional**: unusual and tendentially extreme violations, associated with non-negligible consequences.

4.2 Human Reliability Analysis techniques

The study of HRA was born in the sixties and since then it has always been a hybrid discipline involving reliability engineers, human factors specialists and psychologists [175]. The objectives of HRA techniques were defined by Swain and Gutterman for THERP (Technique for Human Error Rate Prediction) analysis, one of the first HRA techniques that has been developed.

The main objective concerns the evaluation of the contribution of the human factor on the overall reliability of the system. This is carried out through the identification of human errors, the estimation of the probability of occurrence and, if necessary, with the introduction of countermeasures aimed at its reduction [176].

To achieve this goal, HRA techniques estimate the human error probability (HEP) defined by the ratio of the number of errors made to the total number of actions in which an error could have occurred.

In the calculation of the HEP, the Worst-Case Analysis must be taken into account so as not to underestimate the risk. In the literature there are various techniques for the analysis of human reliability, aimed at assessing the work risk deriving from human error. These techniques were created to meet the needs of probabilistic risk assessment (PRA) in order to quantify the contribution of human error to the occurrence of an accident. In this perspective, the HRA approach can be seen as a specialization of the PRA on the relevant factors of human reliability, an approach that provides a more detailed assessment of the risks inherent in the system associated with the human factor. These methods differ mainly in how the probability of human error is estimated, in the cognitive model assumed, in the taxonomy of wrong actions and in the way in which Performance Shaping Factors (PSFs) can influence the probability of error.

Different techniques for Human Error Probability (HEP) estimation have been proposed in literature. Usually, HRA can be classified into one of three different categories:

- First-generation techniques are simple approaches which consider a human being the same as an electric/mechanic component (i.e. it is only capable to succeed or fail).
- Second-generation techniques introduce cognitive models and focus on the role of the context in the HEP evaluation. The aim of these techniques is to include the human cognition within the evaluation of the human performances.
- Third-generation techniques introduce simulator to generate data for the analysis. These methods aims to develop new HRA methods or modifying existing HRA techniques to consider the dynamic progression of human behavior which leads to a human error [177].

The following subsections summarizes the most important and widest used HRA techniques for each one of the above-mentioned generations, focusing on advantages and shortcomings of every method.

4.2.1 First generation techniques

The first-generation of HRA techniques (1970-1990) suggest for the first time to divide a human work into a set of multiple tasks. Then the Human Error Probability (HEP) depends on the impact of the task and also on some factors, such as available time, stress, and working time. The common points of the first-generation methods are:

- Generally, these methods classify errors as omission (when the operator fails to carry out a task) or commission (when the operator carries out a task incorrectly or do something that is not required).

- The identification of Performance Shaping Factors (PSF) which are covariates that could affect the performance of the operators in HRA (for more information about PSF see [178]–[181]).
- Simple cognitive model are implemented in these methods such as the Rasmussen operator performances classification (skill-based, rule-based or knowledge-based) [174].
- The HEP is calculated weighting the base error probability of the task with one or more Performance Shaping Factor (PSF).

Tables 4.1 summarizes the main HRA techniques of the first generation pointing out the field of application, the year of publication and the central points of each method.

Tab. 4. 1 - State of the art of Human Reliability Analysis: summary of the main first generation techniques

TECHNIQUE	FIELD	YEAR	MAIN POINTS
THERP [182] (Technique for Human Error Rate Prediction)	Nuclear	1983	• Most popular first-generation technique. • The human error probability values are assessed through expert judgments and field data. • Event tree analysis used to associate a positive or negative result to each event performed by the operator.
HCR [183] Human Cognitive reliability	Nuclear	1984	• Use Rasmussen subdivision to determine nominal HEP • Time-reliability curve parametrized for the decision-making type • The main disadvantage is that a small variation in the task assessment produce difference in the HEP also up to two orders of magnitude.
SLIM [184] Success Likelihood Index Method	Nuclear	1984	• It calculates a Success Likelihood Index for each task based on importance weight and scaled rating of different PSFs. • Uncertainty bound analysis and cost-effectiveness analysis
HEART [185] Human Error Assessment and Reduction Technique	General purpose	1985	• The HEP of each task is influenced by one or more EPC (Error Producing Condition). • It provides useful suggestions to reduce the occurrence of errors. • It relies extensively to the expert opinion.

Technique for Human Error Rate Prediction (THERP) is the most popular first-generation technique, it was developed in 1983 in the Sandia Laboratories for the US Nuclear Regulatory Commission [182]. The HEP calculation is based on database containing the human error probability values, which are assessed through both expert judgments and field data. The main tool of THERP method is the event tree analysis which use binary logic to associate a positive or negative result to each event performed by the operator. Then a nominal HEP is assessed for each identified branch of the event tree. Finally, the HEP takes also into account performance shaping factors which modify the nominal value. Even if it is one of the most dated technique it is still in use also beyond the nuclear application.

Human Cognitive Reliability (HCR) is a cognitive approach to human reliability, the nominal HEP is determined by using the Rasmussen subdivision [174] in rule-based, skill-based and knowledge-based decision making modes [183]. It is based on a time-reliability curve parametrized for the decision making type; the main disadvantage is the high sensitivity to small change, in fact small variation in the task assessment produce difference in the HEP also up to two orders of magnitude.

Human Error Assessment and Reduction Technique (HEART), developed in 1985, is considered one of the most popular technique currently used in UK [186]. It considers the HEP of each task influenced by one or more EPC (Error Producing Condition). HEART is considered an extremely flexible technique that could be applied to various field thanks to several task options and different EPCs.

The main critic to the first-generation techniques is that the human error mainly depends on external behavior and does not consider the cognitive process and psychology. Moreover, they miss to consider some relevant PSFs and that often lead to a worsen HEP and greater uncertainty bounds. Despite the mentioned disadvantages of some first-generation technique, they are often used by many companies, because of their simplicity.

4.2.2 Second generation techniques

The second-generation technique (1990-2005) tries to overcome the limitation of the first generation by using human performance factors and cognitive models. The topic of this generation is the estimation of the human error probability including the human cognition [187]. Cognition refers to the mental processes (thinking, remembering, problem solving etc.) in order to acquire knowledge and comprehension.

Tables 4.2 summarizes the main HRA techniques of the second generation pointing out the field of application, the year of publication and the central points of each method.

Tab. 4. 2 - State of the art of Human Reliability Analysis: summary of the main second generation techniques

TECHNIQUE	FIELD	YEAR	MAIN POINTS
CREAM [170] Cognitive Reliability and Error Analysis Method	Mainly for nuclear/ chemical plants	1998	• Designed for both predictive and retrospective analysis. • Contextual Control Model (COCOM) which considers four modes of control, namely Scrambled, Opportunistic, Tactical and Strategic control. • It is clear, structured and systematic but on the other hand it results to be too complex.
ATHEANA [188] A Technique for Human Error Analysis	Nuclear	1996	• Allow to adopt preventive actions to reduce the occurrence of a human error and improve the whole level of system safety. • Qualitative method Usually performed after an accident.
SPAR-H [189] Standardized Plant Analysis of Risk-Human Reliability Analysis	Nuclear	2005	• Three-type classification for the human task, namely: action, diagnosis or both diagnosis and action. • Is one of the few methods which consider that PSF have both negative and positive influence on the error probability. • It uses eight different Performance Shaping Factor to consider the appropriate context

Cognitive Reliability and Error Analysis Method (CREAM) is designed for both predictive analysis (i.e. to predict potential human error), and retrospective analysis (i.e. to analyze and quantify error) [170]. CREAM uses the Contextual Control Model (COCOM) which considers four modes of control, namely Scrambled control, Opportunistic control, Tactical control and Strategic control. CREAM is based on the assumption that when the level of operator control rises, so does their performance reliability. This technique is clear, structured and systematic but on the other hand it results to be too complex and need more resources than other methods.

Standardized Plant Analysis of Risk-Human Reliability Analysis (SPAR-H) [189] is based on a three-type classification for the human task, namely: action, diagnosis or both diagnosis and action. The technique uses eight different

Performance Shaping Factor to consider the appropriate context. The SPAR-H is one of the few methods which consider that PSF have both negative and positive influence on the error probability.

A Technique for Human Error Analysis (ATHEANA) [188] allow to adopt preventive actions to reduce the occurrence of a human error and improve the whole level of system safety. ATHEANA is not suitable for comparative and sensitivity analysis because it is not quantitative and usually it is performed after an accident.

4.2.3 New studies and Third generation techniques

The first and second generations of HRA techniques fail to describe the natural dynamic modeling of human behavior. The third generation of HRA aims to develop new HRA methods or modifying existing HRA methods to consider the dynamic progression of human behavior which leads to a human error.

This last generation uses simulation and modeling in three different ways to generate data for the analysis.

1. Experts estimate the probability of human error. This approach is very subjective and usually experts have no access to human error data. Simulations provide a data basis for the HRA conducted by experts.
2. The simulation produces an estimate of the performance shaping factors (PSFs), which are used to calculate the HEPs.
3. The simulation is used to calculate the frequency of failure/success, it explores the range of human performances. Performance criteria (e.g. time to perform a task) are set and during the simulation the performers can succeed or fail the tasks. After some iterations the output of the simulation is the HEP frequency.

Tables 4.3 summarizes the main HRA techniques of the third generation pointing out the field of application, the year of publication and the central points of each method.

Tab. 4. 3 - State of the art of HRA: summary of the third generation techniques

TECHNIQUE	FIELD	YEAR	MAIN POINTS
NARA [190] Nuclear Action Reliability Assessment	Nuclear	2005	• Improvement of the HEART for nuclear industry. • Database of HEP including direct observation, recording, incident data and expert judgement. • It uses the APOA for each EPC.
PROCOS [191] Probabilistic Cognitive Simulator	General purpose	2007	• It integrates HAZOP and event tree. • It considers different contexts changing the PSFs and the parameters about the human performance.
CES [192] Cognitive Environment Simulation	Nuclear	1987	• It estimates how an operator responds to an emergency scenario in a nuclear power plant. • It uses AI tools to simulate the behavior of a control-room operator in a nuclear power plant.
COSIMO [193] Cognitive Simulation Model	Nuclear	1992	• It simulates the behavior of an operator during the management of accidents. • It creates a structure for every cognitive function.
MIDAS [194] Man Machine Integration Design and Analysis system	Aviation	1993	• It simulates the behavior of two operators: a pilot for civil aviation or an air traffic controller. • It uses Rasmussen's model.
SYBORG [195] Simulation System for Behavior of an Operating group	Nuclear	1995	• It identifies combinations of possible errors and plant condition that can lead to accidents. • It proposes different strategies to mitigate the error and improve the performances.
SAFPHR [196] Systems Analysis for Formal Pharmaceutical Human Reliability	Medical	2020	• It combines concepts from CREAM with probabilistic model checking. • It is based on a computational tool which automatically provides properties about complex, stochastic systems.
BN-SLIM [197] Bayesian Network SLIM	Nuclear	2020	• It uses Bayesian Network for improving the performances of SLIM in handling uncertainty arising from expert's opinion and lack of data.
Phoenix [198] **and Phoenix-PRO** [199]	Nuclear - Petroleum Refining Operations	2016 2020	• It integrates Hybrid Causal Logic model, Event Sequence Diagrams, FTA and Bayesian Networks. • It has been developed for nuclear in 2016 (Phoenix) and then extended to Oil&Gas in 2020 (Phoenix-PRO).
RANDAP [200] Reliability Analysis of Detailed Action Plans	Nuclear	2013	• It is based on RBD to model reliability of integrated automatic-operator emergency actions. • It focuses on incorporating operator's operational and cognitive errors in the reliability analysis
SHERPA [168] Simulator for Human Error Probability Analysis	General purpose	2015	• It estimates the human error probability as a Weibull function dependent from the working time. • It provides a dynamic model which allows a flexible evaluation of the human performance.

One of the third generation technique is the Probabilistic Cognitive Simulator (PROCOS), developed in 2006 [191]. It uses both HAZOP (HAZard and OPerability analysis) and event tree with cognitive human error analysis. The approach is semi-static and therefore it considers different contexts, simply changing the Performance Shaping Factors and the parameters about the equipment and the action to be simulated.

NARA (Nuclear Action Reliability Assessment) [190] represents an improvement of the HEART technique, specifically applied to the nuclear industry. NARA contains a new database for the nominal error probability collected by including direct observation, recording, simulator observation, incident data and expert judgement. It uses the Assessed proportion of affect (APOA), assessed for each identified EPC (Error Producing Condition). This factor takes into account the affect that the EPC has on successful task performance.

Cognitive Simulation Model (COSIMO) [193] technique analyzes the operator behavior in a nuclear power plant. The actions conducted by the operator are simulated through a specific model for the system and the fallible machine.

Man Machine Integration Design and Analysis system (MIDAS) [194] simulates the behavior of a pilot for civil aviation or an air traffic controller. The aim of MIDAS is to analyze the interaction between the operator and the external environment, the used model for the operator is based on Rasmussen's model.

Simulation System for Behavior of an Operating group (SYBORG) [195], simulates a group of nuclear power plant operators. The technique identifies combinations of possible errors and plant condition that can lead to accidents; then it proposes different strategies to mitigate the error and improve the performances.

A Simulator for Human Error Probability Analysis (SHERPA) [168] estimates the human error probability as a Weibull function dependent from the time. It provides a dynamic model which allows a flexible evaluation of the human performance. In particular the nominal HEP is a modified Weibull function, the technique also considers the performance shaping factors of the SPAR-H method.

In the last years, other approaches have been developed integrating different aspects within well-known techniques. For example, Abrishami et al. [197] proposes a BN-SLIM approach using Bayesian Network (BN) for improving the performance of a first-generation method called SLIM (Success Likelihood Index

Model). Aliabadi [201] integrates intuitionistic fuzzy to handle uncertainty in HEART method, while in [202] uncertainty in THERP prediction is handled using Bayesian networks. Bayesian models are also used in [203] to aggregate simulator data in dynamic model for error probability estimation. In [204] and in [205] some improvements of SPAR-H performance shaping factor are presented. Systems Analysis for Formal Pharmaceutical Human Reliability (SAFPHR) has been proposed in [177] and extended in [196] to handle the dynamic environmental elements that can impact human performance since the first and second generation techniques fail to consider this problem. Ekanem et al. [198] extensively discusses the limitations of first and second generation techniques and it proposes a qualitative method called Phoenix. Then the Phoenix method has been enhanced in [199] proposing Phoenix-PRO specifically customized for Petroleum Refining Operations. In [206] the analysis of cognitive error typical of the second generation methods has been enhanced using Bayesian network. In [207] a novel approach is proposed combining the Safety-II concept and the CART (Classification And Regression Tree) method in order to acquire dynamic HRA data considering different task contexts.

4.3 Needs for Human Reliability Analysis in railway engineering

Railway is currently one of the major forms of transportation technologies worldwide. With billions of passengers every year, it became crucial to ensure remarkable levels of reliability and safety of railway systems [208]. The European standard EN 50126 [209] regulates the Reliability, Availability, Maintainability and Safety (RAMS) assessment of every railway-related system which is installed in Europe. This standard highlights the importance of an accurate Human Reliability Analysis (HRA) in order to estimate the Human Error Probability (HEP) of every task performed by human operators in railway field. As a matter of fact, human performances play a fundamental and critical role in many different aspects of railway engineering [210], [211]. This is due to the fact that humans make errors all the time. Human errors are inevitable, and in some circumstances the consequences of these errors could lead to hazardous conditions and disastrous accidents. However, catastrophic disasters and dangerous accidents, which are the most evident result of the human error, are extremely severe but also very unlikely situations. Quite the opposite, trivial human errors that lead to minor accident without safety implication are quite common [166], [175], [212].

As it is possible to see in Table 4.1, Table 4.2 and Table 4.3, most of the HRA techniques (regardless the generation) has been developed for nuclear industry. Despite this, human reliability is a fundamental aspect in many different fields of application where human errors could lead to dangerous accidents and hazardous conditions, such as the railway industry.

In [213] the probability of failure in the communication action between driver and signaler have been analyzed. Grozdanovic [214] proposes the use of SLIM technique to analyze the human error probability of an operator working in a railway control center. In [215] the human error during a train monitoring and control system assessment has been studied. Train cab simulators have been used in [216] to collect human error probability data on train driver fault diagnosis. Some works proposes to use HEART [217] technique to estimate HEP in railway-related systems. For instance, in [218] authors uses HEART method as part of a risk assessment evaluation of existing yard switching operations and remote-control locomotive operations in the United States. However, HEART technique has not been specifically developed for railway, and consequently some adaptations are required [219]. In [220] authors introduce the concept of railway engineering among other industrial fields proposing the Analysis of Consequences of Human Unreliability (ACIH). Railway field is considered also by Human Error Risk Management for Engineering Systems (HERMES) [221]. More information about the HRA method for railway industry have been included in the following sections.

4.4 Systematic Review of the last two decades

Some literature review about HRA have been already published in the last few years covering different topics. The nuclear industry is the field which is most covered by recent reviews. For instance the human factor in nuclear safety have been reviewed in [222] while the effects of digitalization of nuclear power plant control rooms on human error probability have been published by Porthin et al. in 2020 [223]. A comprehensive and systematic bibliometric analysis of the HRA world has been published by Tao et al. in 2020 [224], by Patriarca et al. in 2020 [225] and by Hou et al. in 2021 [226].

However, there is a lack of literature review and bibliometric analysis of human reliability analysis in railway applications. As a consequence, this works aims at filling this gap providing an extensive review and a bibliometric analysis of papers published after 2000 covering the topic of human reliability and human error in railway field. Starting from the SCOPUS database a total of 268 journal works (including only research articles) have been found in the time slot from 2000 to August 2021.

After describing the research methodology and the bibliometric analysis of the 268 research articles coming out from the review, Section 4.4.3 accurately describes some of the most significant manuscript dealing with HRA in railway engineering classifying the papers in 5 different categories:

- Papers dealing with the analysis of significant railway accidents occurred in the last years all over the world.
- Manuscripts discussing the human factors in specific railway systems, such as level crossings, railway control centers, safety-critical equipment, etc.
- Paper highlighting the influence of different internal and external factors (PSF) on the probability of a human error.
- Original human reliability analysis techniques specifically developed for railway industry.
- Manuscripts dealing with the applications of already existing techniques originally developed to other industries (such as nuclear, chemical, avionics etc) with specific attention to papers contributing with enhancements and improvements of such methods.

4.4.1 Search methodology

The SCOPUS database has been used to identify the relevant scientific publications in the considered field. This database has been selected since it is widely recognized as one of the best indexing databases for high-quality and impactful scientific papers. Journals and conference proceedings from the major publisher (such as IEEE, Elsevier, MDPI, Taylor & Francis, Wiley, Emerald and many others) are rapidly indexed within SCOPUS database. The quality of the proposed review is ensured by considering only peer-reviewed journal articles and excluding books, doctoral dissertations, conference papers, editorial, letters, etc.

Fig. 4.2 highlights a schematization of the search methodology using AND/OR gates. The search starts looking for all papers that includes the key terms “human reliability” or “human error” or alternatively “human factor” in the title, abstract or keywords of the article. The terminology PRE/0 included in Fig.4. 2 is a SCOPUS operator used to specify that the first term in the query must precede the second by a specified number (0 in this case) of terms. At the end of this phase 60,013 documents have been found, as can be seen in Fig. 4.3. The database characteristics, the main subject areas and the main sources are highlighted in the right boxes in Fig. 4.3. After this first identification phase, a screening process has been applied following different criteria. Firstly, the application field has been limited to the query “railway” or “railroads”. This can be achieved using the AND gate as in Fig. 4.2. This first screening removed 59,137 documents proving how HRA has been extensively applied in several fields other than railway.

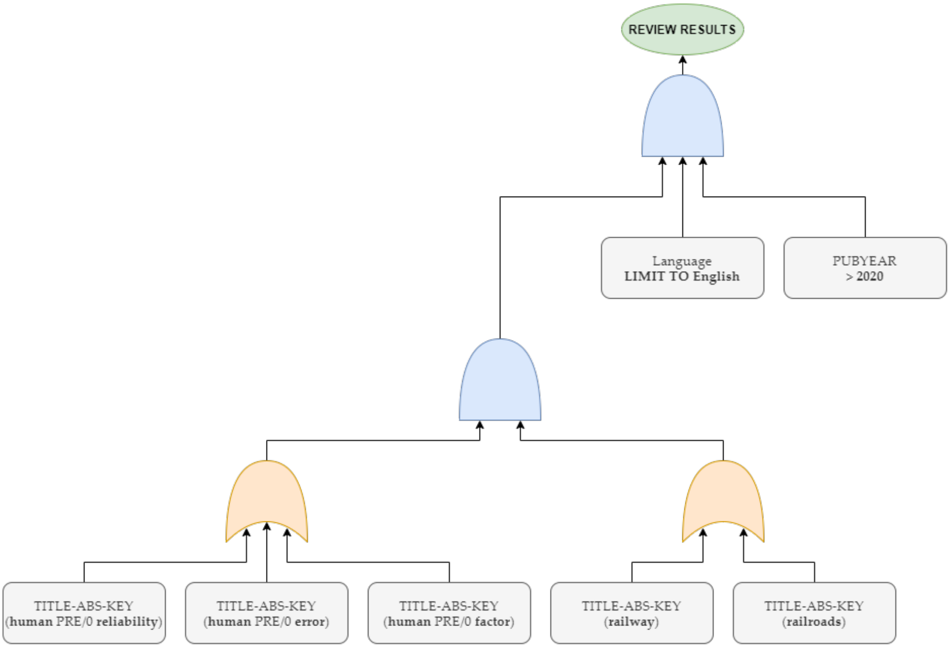


Fig. 4. 2 - Schematization of search methodology using AND/OR logic gates. The grey boxes indicate the search keys.

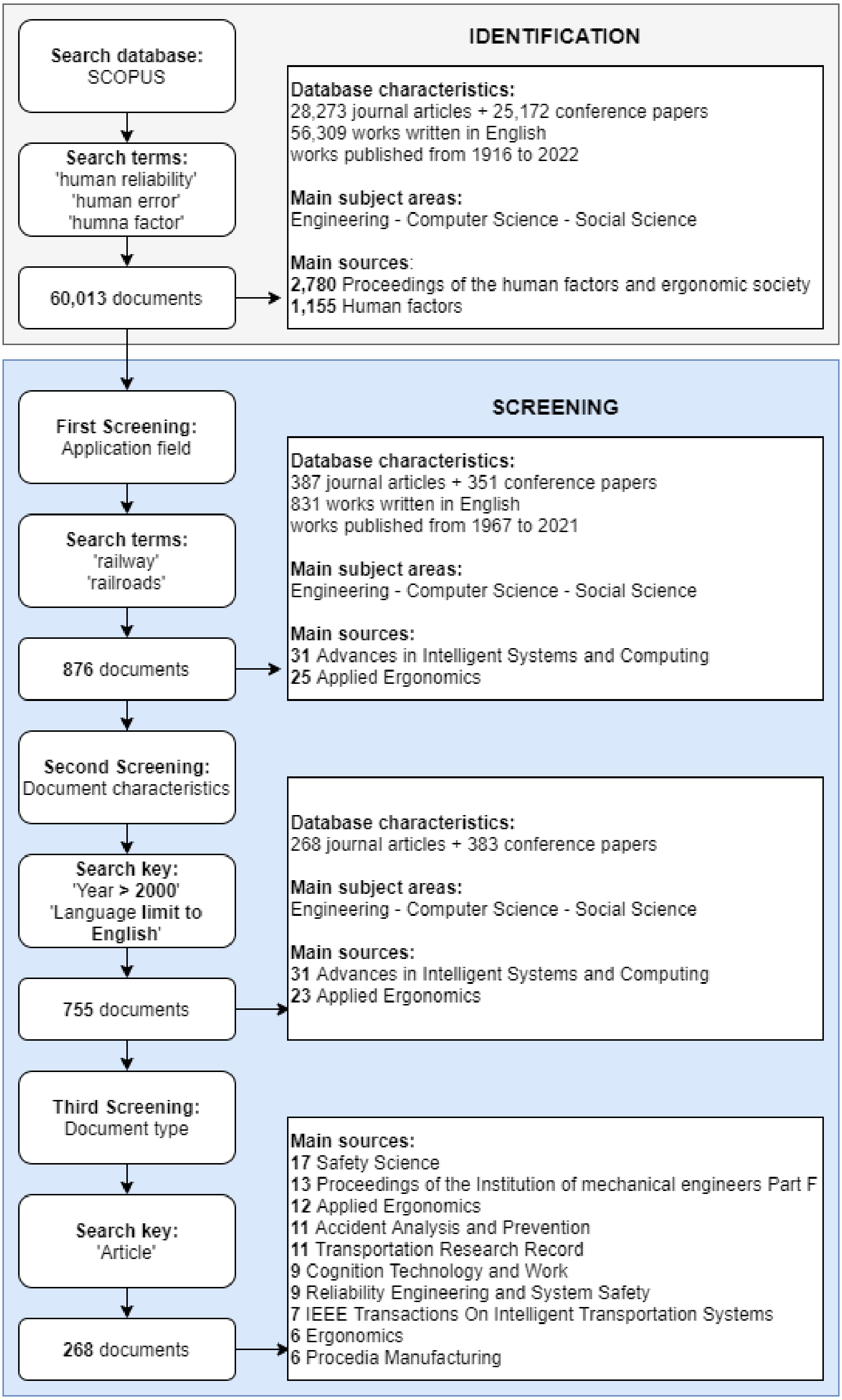

IDENTIFICATION
Search database: SCOPUS
Search terms: 'human reliability' 'human error' 'humna factor'
60,013 documents
Database characteristics:
28,273 journal articles + 25,172 conference papers
56,309 works written in English
works published from 1916 to 2022
Main subject areas:
Engineering - Computer Science - Social Science
Main sources:
2,780 Proceedings of the human factors and ergonomic society
1,155 Human factors
SCREENING
First Screening: Application field
Search terms: 'railway' 'railroads'
876 documents
Database characteristics:
387 journal articles + 351 conference papers
831 works written in English
works published from 1967 to 2021
Main subject areas:
Engineering - Computer Science - Social Science
Main sources:
31 Advances in Intelligent Systems and Computing
25 Applied Ergonomics
Second Screening: Document characteristics
Search key: 'Year > 2000' 'Language limit to English'
755 documents
Database characteristics:
268 journal articles + 383 conference papers
Main subject areas:
Engineering - Computer Science - Social Science
Main sources:
31 Advances in Intelligent Systems and Computing
23 Applied Ergonomics
Third Screening: Document type
Search key: 'Article'
268 documents
Main sources:
17 Safety Science
13 Proceedings of the Institution of mechanical engineers Part F
12 Applied Ergonomics
11 Accident Analysis and Prevention
11 Transportation Research Record
9 Cognition Technology and Work
9 Reliability Engineering and System Safety
7 IEEE Transactions On Intelligent Transportation Systems
6 Ergonomics
6 Procedia Manufacturing

Fig. 4. 3- Literature review process for the analysis of HRA in railway.

A second screening limited the works to only 755 papers removing all the documents published before 2000 (search query “AND PUBYEAR > 2000”) and all the documents published in languages other than English using the search query “AND LIMIT-TO (LANGUAGE, "English”)”. The limit on the publication year has been set in order to restrict the literature search only to relative-recent papers published in the last two decades. This will allow to draw more relevant and more useful conclusions and take-home messages for the readers. Instead, the limit on the English language has been set because English is widely recognized as the universal language of research. As a matter of fact, the majority of works published in the fields of reliability, human error, railway manufacturing and more generally all engineering subcategories are published in English. The final screening limits the results only to peer-reviewed “Research Article” excluding other 487 documents and leaving the body of knowledge with only 268 works.

4.4.2 Bibliometric analysis

This section presents the major results of the bibliometric analysis carried out on the 268 research articles discovered following the search criteria illustrated in the previous section.

This analysis starts downloading all the 268 documents come out by the review process described in the previous section. After that, the full BibTEX reference information of every paper has been exported. Then, a dedicated MATLAB tool has been specifically developed for this work to serve the following purposes:

- To import the information contained in the BibTEX file of each identified paper.
- To cluster the articles under analysis according to the year of publication, the number of citations and self-citation, the keyword used, the affiliations of the authors, etc.
- To generate a report including the most common and widely used metrics for bibliometric analysis.
- To summarizes the results of the data analysis using figures and tables.

Firstly, Fig. 4.4 compares the amount of research articles discovered against the other source types that meet all the criteria up to the second screening (i.e.

search terms, application field, language and publication year). The 268 research articles represent only the 35% of the 755 documents left after the second screening. Most of the documents are conference papers and conference reviews (covering together the 57% of the works) while very few books, books chapter, reviews and editorials have been published in this field.

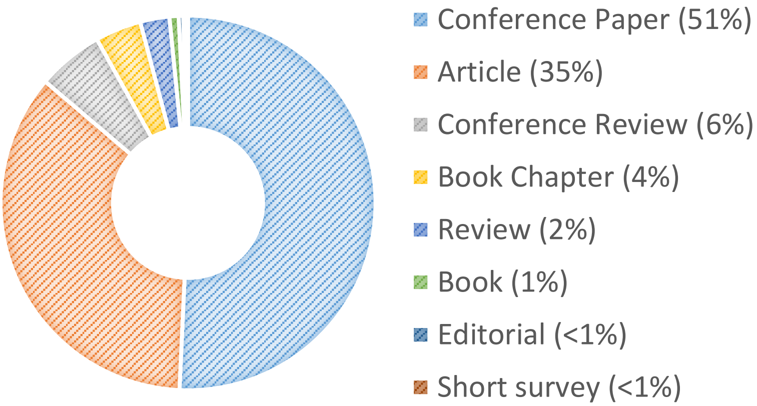


Fig. 4. 4- Comparison of type of documents after the second screening phase. The total amount of documents is 755.

Fig. 4.5 shows the number of published research article every year since 2000. It is evident the growing attention of many researchers to HRA in railway applications.

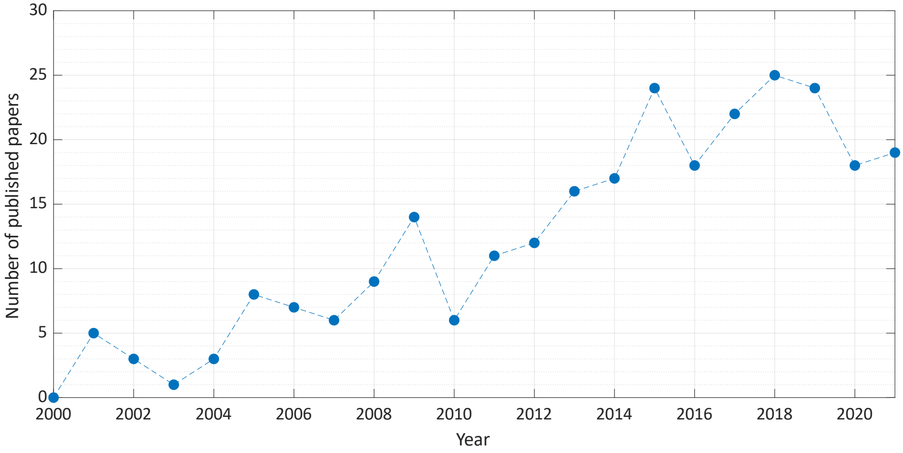


Fig. 4. 5- Trend of published papers in HRA for railway engineering considering the last two decades.

Most of the 268 research articles outcoming from the literature review have been published in the last few years, while in the early 2000s less than 10 documents per year have been found. Such increasing trend is fundamental to prevent critical railway accidents due to human errors. Another useful analysis to understand the leading impact of this topic is represented in Fig. 4.6, where the total number of citations of the considered papers every year are illustrated (blue dots).

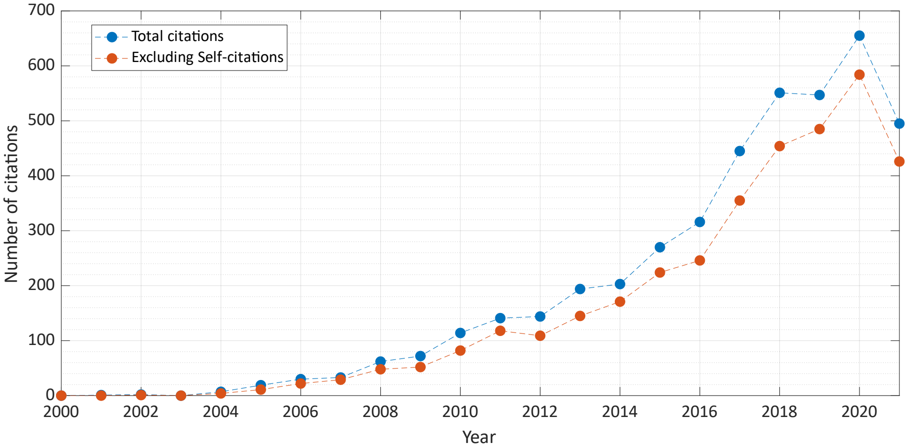


Fig. 4. 6- Number of total citations (blue dots) and number of citations excluding self-citations (red dots) of the 268 identified research articles.

The number of citations follows exactly the trend of the previous figure, as a matter of fact the increase of published paper in this field have led to a remarkable increase of number of citations. Same considerations could be drawn also for the number of self-citations illustrated using red dots in Fig. 4.6.

Obviously, an increasing trend of the number of citations is expected since the total number of published papers increases yearly. However, fitting the data in Fig. 4.5 and Fig. 4.6 by means of a linear regression model, very different results have been obtained. As a matter of fact, the slope of the fitting line in case of the total number of citations is almost thirty times greater than the slope of the fitting line used to model the total number of published papers. It is important to note that both trends in Fig. 4.5 and Fig. 4.6 are not linear, however this analysis helps to clearly emphasize how the increasing number of citations is not only caused by the increment of published paper. Instead, it proves a general growth in the interest for human reliability analysis in railway engineering.

The cloud word in Fig. 4.7 underlines the keyword co-occurrence in the considered topic. The analysis of Fig. 4.7 shows that 'Railroads' is the most used keyword in this field (used in 133 documents out of 268). Other keywords extensively chosen are: 'Railroad Transportation', 'Human Engineering', 'Railway', 'Human', 'Railroad accidents', 'Accident prevention', 'Human factor'. The most striking results to emerge from the figure is that there are no HRA methods presents in the keyword cloud word. This is due to the fact that there is only one HRA technique specifically developed for railway engineering, which is called RARA (Railway Action Reliability Assessment). Further details about this method are given in the following. As a matter of fact, the keyword co-occurrence in Fig. 4.7 highlights the general interest for human error analysis and accidents analysis and prevention in railway, with many keywords related to these topics. Quite the contrary, the estimation of human reliability of specific task carried out by human operators using innovative models seams to have a minor impact on the overall body of knowledge.

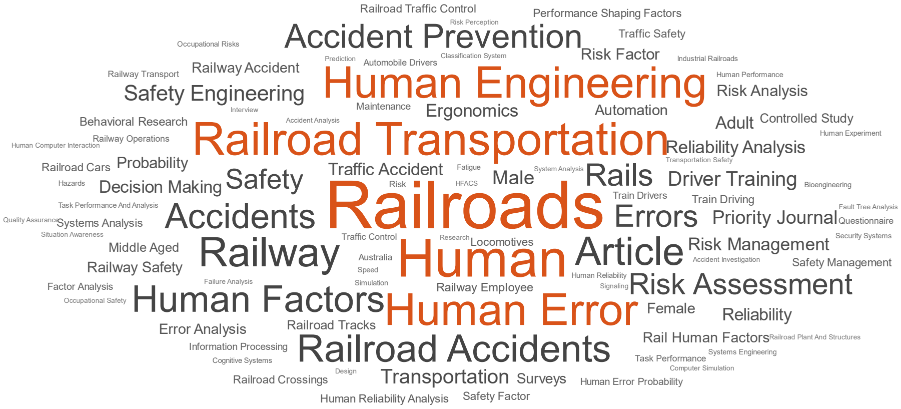


Fig. 4. 7 - Cloud word of the keyword co-occurrence in the analyzed research papers.

Fig. 4.8 and Fig. 4.9 provides data about the geographical distribution of the published paper in the research topic analyzed in this review.

A more qualitative approach is presented in Fig. 4.8, where the number of published papers per country are illustrated using blue bubbles with different sizes. The figure highlights the central role of Europe in this research topic (accounting for almost 54% of the papers), followed by USA and China. More in detail, Fig. 4.9 shows the detailed values of the country-by-country published papers.

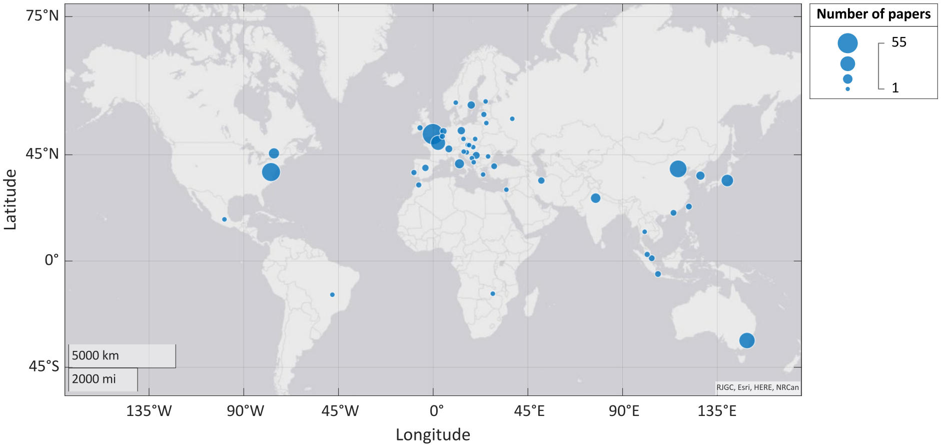


Fig. 4. 8- Qualitative evaluation of the geo-localization of published papers in the research topic under analysis.

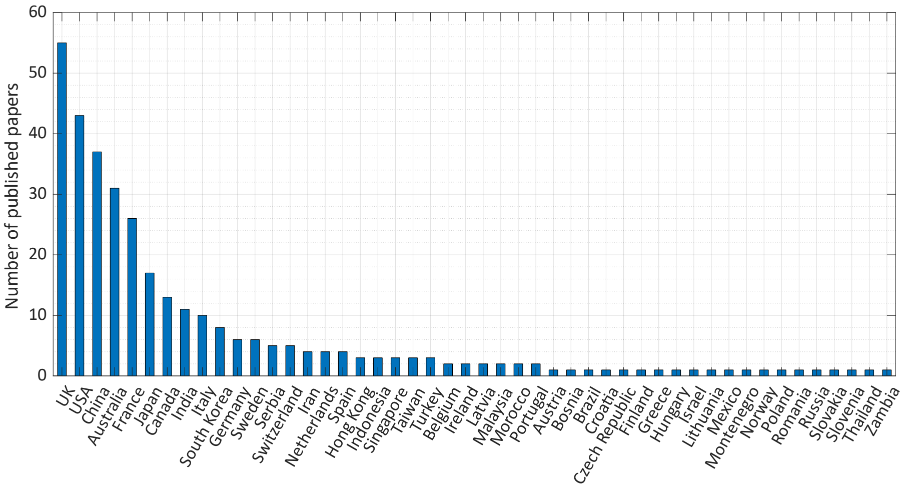


Fig. 4. 9- Detailed estimation of the country-by-country number of published papers about HRA for railway applications.

A more detailed and in-depth analysis is provided in Fig. 4.10, where the 268 discovered papers have been clustered according to the affiliations of the authors. The results of the data analysis pointed out 160 different author's affiliations from all over the world. Most of them are prestigious university from Europe, USA, China and Australia, but there are also some technical institute and research centers. For the sake of figure's readability, only affiliations with at least four published papers have been included in Fig. 4.10. The affiliations accounting for the greatest number of papers are the University of Nottingham

(UK), the British Network Rail (UK) and the Beijing Jiaotong University (China), all of them with at least ten published papers. The results shown in Fig. 4.10 confirmed what stood out in Fig. 4.9, with UK, USA, China and Australia as the leading countries on this research topic.

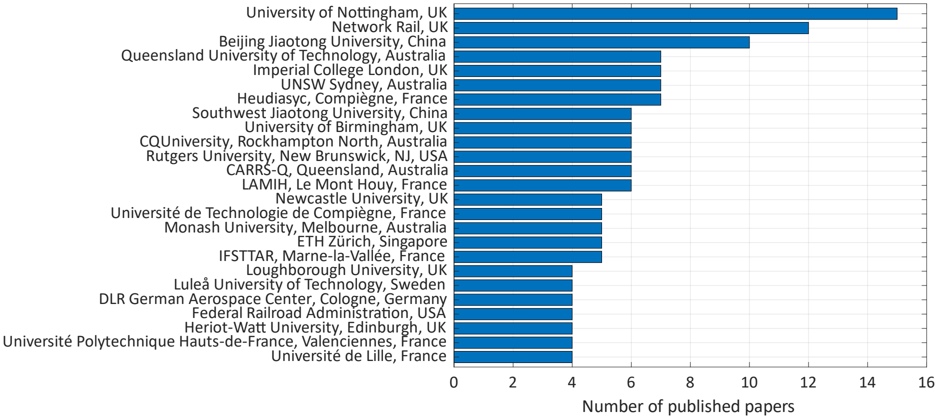


Fig. 4. 10 - Detail of the bibliometric analysis regarding the affiliations of the authors. Only affiliations with at least 4 published papers have been considered.

The latter analysis is then enhanced clustering the identified papers according to the recurrent authors. Table 4.4 highlights the most relevant authors in the considered topic summarizing all the authors who have published more than four papers in the field of human reliability and human factor in railway engineering since 2000. The most important and significant researcher in this field is Prof. John R. Wilson from the University of Nottingham (UK), who is widely considered as “the father of rail human factors”. From 2000 to 2016, Prof Wilson’s work includes 12 peer-reviewed research articles about the prediction of the workload demands upon railway signaler operators.

Another analysis of the proposed bibliometric overview is illustrated in Table 4.5 where the ranking of the ten most-cited research papers discovered in this literature review is presented. Among them, three out of ten of this research have been authored or co-authored by the above-mentioned Prof. John R. Wilson from the University of Nottingham (UK) namely “Fundamentals of systems ergonomics/human factors” [227], “Understanding the human factors contribution to railway accidents and incidents in Australia” [228] and “Classification of errors contributing to rail incidents and accidents: A comparison of two human error identification techniques” [229]. Once again, this proves the central role of United Kingdom, University of Nottingham and

Prof. J. R. Wilson in the state of the art of human reliability for railway engineering.

Tab. 4. 4 - Most relevant authors in the field of Human Reliability for Railway Engineering since 2000.

Top recurrent Authors	**Affiliation**	**Number of Papers**
Wilson, J.R.	Human Factors Research Group, University of Nottingham, Nottingham, UK	12
Kyriakidis, M.	ETH Zurich, Future Resilient Systems, Singapore - ETH Centre, Singapore	6
Liu, X.	Dept. of Civil and Environmental Engineering, Rutgers, The State University of New Jersey, Piscataway, NJ, United States	6
Majumdar, A.	Centre for Transport Studies, Imperial College London, UK	6
Sallak, M.	Department of Computer Engineering, Sorbonne Universités, Université de Technologie de Compiègne, Compiègne Cedex, France	6
Naweed, A.	Appleton Institute for Behavioural Science, Central Queensland University, Wayville, Australia	5
Ryan, B.	Human Factors Research Group, Faculty of Engineering, University of Nottingham, UK	5
Sharples, S.	Human Factors Research Group, Faculty of Engineering, University of Nottingham, UK	5
Vanderhaegen, F.	Department of Automation and Control, Université de Valenciennes et du Hainaut-Cambrésis, Valenciennes, France	4
Larue, G.S.	Centre for Accident Research and Road Safety, Queensland University of Technology, Brisbane, Australia	4
Golightly, D.	Human Factors Research Group, University of Nottingham, Nottingham, UK	4
Lenné, M.G.	Accident Research Centre, Monash University, Clayton, Australia	4
Ochieng, W.Y.	Centre for Transport Studies, Imperial College London, London, UK	4
Read, G.J.M.	Centre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Maroochydore, Australia	4
Schön, W.	Department of Computer Engineering, Sorbonne Universités, Université de Technologie de Compiègne, Compiègne Cedex, France	4
Shigemori, M.	Safety Psychology Laboratory, Human Science Division, Japan	4
Zhang, Z.	Department of Civil and Environmental Engineering, Rutgers, The State University of New Jersey, Piscataway, NJ, United States	4

Tab. 4. 5 - 10 top-cited research articles in the field of human reliability analysis for railway engineering.

TITLE	SOURCE	REF.	YEAR	CIT. N°
Handoff strategies in settings with high consequences for failure: Lessons for health care operations.	International Journal for Quality in Health Care	[230]	2004	366
Fundamentals of systems ergonomics/human factors.	Applied Ergonomics	[227]	2014	227
Application of a human error framework to conduct train accident/incident investigations.	Accident Analysis and Prevention	[218]	2006	171
Deep Multitask Learning for Railway Track Inspection.	IEEE Transactions on Intelligent Transportation Systems	[231]	2017	170
Understanding the human factors contribution to railway accidents and incidents in Australia.	Accident Analysis and Prevention	[228]	2008	168
Analysis of causes of major train derailment and their effect on accident rates	Transportation Research Record	[232]	2012	143
The crash at Kerang: Investigating systemic and psychological factors leading to unintentional non-compliance at rail level crossings.	Accident Analysis and Prevention	[233]	2013	102
Classification of errors contributing to rail incidents and accidents: A comparison of two human error identification techniques.	Safety Science	[229]	2009	83
Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway traffic supervision.	Reliability Engineering and System Safety	[234]	2011	78
Shared situation awareness as a contributor to high reliability performance in railroad operations.	Organization Studies	[235]	2006	70

Figure 4.11 compares the published papers per different publication journals. It is possible to note that “Safety Science” is the journal with more papers, followed by “Proceedings of the institution of mechanical engineers part F” and “Applied ergonomics”. Other important journal in the field of safety engineering is included, such as “Reliability Engineering and System Safety” and “Accident Analysis and Prevention”.

Moreover, there are also some high-quality journals in the field of transportation and railway, such as: “IEEE Transactions on Intelligent

Transportation Systems" and "Journal of rail transport planning & management".

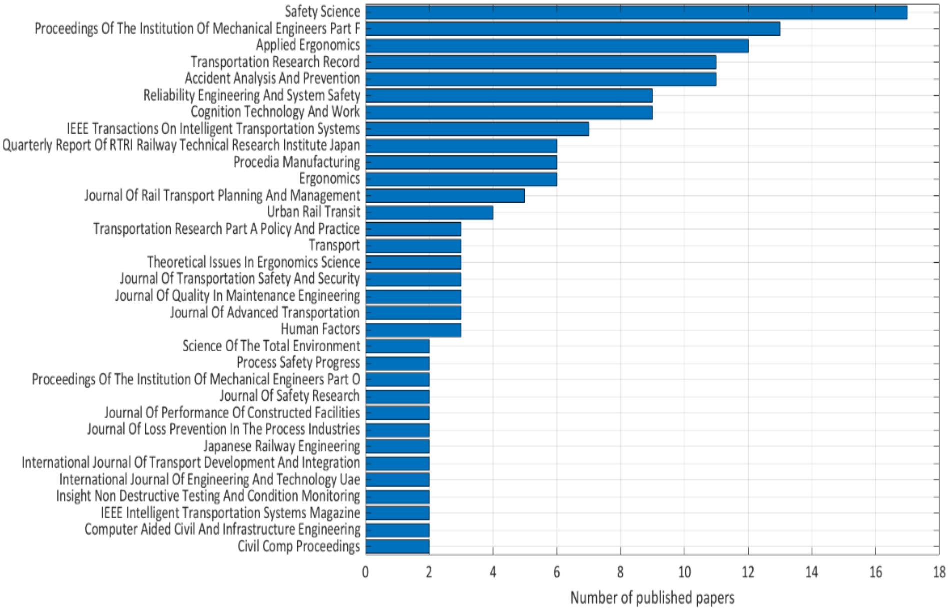


Fig. 4. 11 - Comparison of the number of published papers divided per journal source.

4.4.3 Most significant document

Only few authors conduct studies to analyze the impact of human error in railway, while only one railway specific HRA has been developed [236]. Gibson, in [213], analyses the error probabilities in the communication action between driver and signaler. Then, this study has been extended in [216] using train cab simulators to collect human error probability data on train driver fault diagnosis. In [237] Bayesian network has been used to study the impact of human error in derailments.

Despite it is not customized on railway engineering, HEART technique is sometimes implemented to estimate human error probability in railway-related tasks. For example, Reinach et al [218] have applied the HEART technique as part of a comparative risk assessment of existing yard switching operations and remote-control locomotive operations in the United States. More recently, a hybrid HEART method has been proposed in [238] to estimate the HEP in locomotive driving process. However, there are indications that the HEART technique requires extensive adaptation to the railway context [219]. Another first-generation technique enhanced in order to meet the railway requirements is Success Likelihood Index Methodology. SLIM has been combine with empirical study and network analysis in [239] to estimate HEP in a railway driving process. In [240] SLIM is integrated with Analytic Network Process to present a new approach called Human Performance Railway Operational Index (HuPeROI).

In the following subsection, the most relevant papers in the field of HRA for railway engineering are briefly discussed in order to compare how human reliability and human factor are dealt with in different works.

a) Analysis of significant accidents

Most of the papers discovered in this literature review deal with the analysis of significant railway accidents of the recent past involving human errors by different perspectives. A recurrent topic in the accident analysis is the investigation of accident at rail level crossing. For instance, in 2001 Wigglesworth [241] analyses the causes of several accidents with casualties occurred at railway crossings between train and motor vehicles in Australia. Few years later, another major accident at an Australian railway crossing have been investigate in [233] providing insight into the factors that contributed to the incident while in [242] the causes of heavy vehicle-level crossing incidents have been investigated questioning 17 train drivers and 26 heavy vehicle drivers. Incidents at active and passive level crossing have been compared taking the Australian [243] and Finnish [244] railroads as case studies. Strictly related to rail level crossing, also accidents caused by railroad trespassing have been studied in [245] by means of AI.

Another widely investigated topic is represented by incidents related to metro and subway units (see for instance [246] dealing with Taipei Metro Rapid Transit). The historical incident record from 2011 to 2013 of UK metro has been reviewed in [247] while individual incidents at the interface between subway platform, train and tracks from 1984 to 2018 have been discussed in [248].

The Federal Railroad Administration (FRA) database provides useful data used in many recent papers dealing with HRA in railway field. For instance, Lin et al. [249] discovered that derailments and collisions are the major sources of accidents using the FRA databases. Train derailment data from the FRA for the interval 2001 to 2010 were analyzed in [232]. Similarly, train derailments and collisions occurring between 2000 and 2016 in the U.S. have been studied based on FRA data in [250]. The same database and the same time interval have been investigated also in [251] dealing only with restricted-speed train accidents. However, other national databases have been used in recent papers. For instance, the effects of long shifts in terms of consecutive driving hours on the causes of accident have been investigated in [252] considering data coming from the Taiwan railroads from 1996 to 2006. 40t railway accidents occurred in China from 2003 to 2014 have been analyzed in [253] while the Iran rail network have been used as case study in [254]. The incidents reported in Queensland, Australia by the Rail Safety Regulator have been studied in [255] as well as 14 rail crack incidents on Hong Kong's mass transit railway from 2008 to 2011 have been studied in [256]. By an accident analysis point of view, Australian railway is a relevant case study widely discussed in many works. Prof. J. R. Wilson co-authored two significant highly-cited works on this topic. In the first one [228] the authors emphasized the importance of resource management, organizational climate and organizational processes in order to reduce accidents/incidents caused by human errors after the review of forty Australian rail safety investigation reports. In their following work [229] the authors revised existing tools for complete and consistent error classification taking nineteen Australian rail safety investigation reports as a case study.

Railway accidents involving lookouts have been reviewed in [257] based on Australian and UK rail incidents from 2006 to mid-2018. Accidents classified as Signal Passed At Danger (SPAD) have been reviewed firstly in [258] referring to the Ladbroke Grove rail crash in 1999 (near London) and then in 2019 an indirect cost assessment in case of SPAD has been presented [259].

The leading causes of incidents in rail transportation of dangerous materials and goods have been studied firstly considering 300 accident causes according to the FRA [260], then a discussion about the Canadian railway industry has been presented in [261] taking 42 track derailments and collisions as a case study.

Other papers deal with the analysis of one or few famous catastrophic accidents. For instance, Braut et al. [262] studied the two major railway accidents occurred in Norway, namely the Tretten accident in 1975 and the Åsta accident in 2000. Beale in [263] review the press and accidents reports of some high profile accidents happened in UK between 1996 and 2001. Niwa [264] presents a new accident analysis method taking the most serious railway accident in Japan as a case study (known as the JR Amagasaki derailment occurred on April, 25th 2005 near Osaka city).

Summarizing, most of the works available in literature about human error in railway engineering are discussion and analysis of significant incidents/accidents occurred in the recent past. The FRA database, Australian safety reports and UK safety reports are the most common sources used in these papers as a starting point of the accident analysis. This group of works is significantly setting the research direction in this field. Unfortunately, there are several railway accidents every year worldwide, and as pointed out in Table 1.1 and Fig. 1.2 human error represent a significant cause to the occurring of such accidents. Thus, it is easily to understand why the analysis of such accident and the classification of error contribution is a relevant, growing, and fundamental topic. However, there are some gaps that are currently not considered by the state of the art. The analysis of such accidents and the investigation of human factor contribution in worldwide accidents should be used to improve the human error probability database of the HRA technique available in literature. An interesting aspect that could be investigated in future works is the merging of accident analysis with HRA techniques in order to use the recent accidents to improve the HEP estimation of railway tasks and prevent future hazardous conditions before they cause critical incidents/accidents.

b) Discussion about human error in specific systems

Some papers analyze the risk analysis and the overall RAMS assessment of different complex systems used in railway applications, with specific considerations about safety requirements and human errors.

A detailed risk assessment of two-half-barrier level crossings and four-half-barriers level crossings is presented in [265]. This study considers the railway and road traffic as well as the risk due to human factors by means of an innovate approach used to quantify the risk values. Level crossings have been studied also by Larue et al. [266] investigating the potential negative effects of assistive technologies and intelligent transport systems on driver cognitive load. However, the outcomes of the presented experiments and questionnaires highlight no significant changes in cognitive load of 58 drivers approaching level crossing in presence of three different assistive technologies. Strictly linked to this research, several studies deal with the effects of different safety systems used as support of the drivers estimating the impact of a human error in case such safety-related systems are implemented. For instance, Senesi et al. [267] introduce the contribution of a human factor within the risk assessment of an Italian Automatic Train Protection (ATP) system called SSC (Italian acronym for supporting system for the driver). Similarly, the impact of human errors in risk assessment of Positive Train Control (PTC) systems is studied in [268].

Some studies also present innovative systems/approaches/procedure to optimize the safety equipment used as drovers' supportive technologies minimizing the human error probability. For instance, a new configuration method is presented in [269] to decrease the probability of a human error automatically configuring the functional logic of safety-critical systems. An innovative system able to measure the distance between trains and to generate movement authority for approaching trains in present of failure of the main ATP has been presented in [270]. This system allows to increase the safety demanding decrease the responsibility of the drivers when ATPs are out of service with a consequent increase of human reliability.

Obviously, there are also some studies dealing with another important unit highly subjected by human error, i.e. the traffic control center. Roets et al. [271] proposed a nonparametric framework to realistically model the efficiency of personnel working in Belgian traffic control centers. The coordination between rail traffic center and trin drivers of Swedish railway have been studied in [272] by a cognitive perspective, while cognitive abilities are used to predict safety performances of high-speed railway dispatcher in China [273]. The European Rail traffic Management System (ERTMS) has been studied in [274] including human factor as causes of error as well as network failures, common cause failures and imprecise failures.

Summarizing, only few of the 268 discovered works deals with the analysis of human error and human reliability regarding specific systems or specific tasks. Level crossings and ATPs are the most investigated case studies since they are some of the most critical railway systems by a safety point-of-view. However, the few discovered papers are not enough to establish a proper line of research.

It is the author opinion that this field of work should be further investigated in order to discover criticalities and risky/hazardous scenarios that are not already recognized by companies and researchers in railway field. To fill this needs, future works should deal with the improvements and enchantment of the existing papers on traffic control centers and ATPs management. Other fundamental topic that requires to be investigated are the analysis of other systems and tasks/operations found particularly critical by the latest UIC safety reports that have not been adequately discussed, such as the installation and maintenance of track, switch, rolling stock and more generally of all the railway infrastructure.

c) Influence of internal and external factors

The literature review carried out on HRA in railway engineering highlighted a significant set of manuscripts dealing with the influence of external and internal factors on human performances by an error probability point of view. In [275] a specific taxonomy of Performance Shaping Factors (PSF) for railway field is introduced. The paper emphasizes that safety culture, communication teamwork and distraction (e.g., loss of concentration vigilance or situational awareness) are the most important and most common PSF accounting for the great part of railway incidents and accidents. Other significant PSFs identified in [275] are system design (i.e., ergonomics), fatigue, quality of procedures, risk perception, training/experience and familiarity with the task. The PSFs proposed in [275] have been then extended to generic applications in [276]. Another set of PSFs specifically developed for railway engineering is presented in [181] within the context of PRELUDE (Performance shaping factor-based human reliability assessment using valuation-based systems).

In this case, a four-level scenario (i.e., good, nominal, poor, insufficient information) has been introduced for seven different PSFs (namely, Training, Experience, Communication, Situational awareness, Task load, Timo load and Quality of human system interface).

The researchers at University of Nottingham presents in 2009 a Rail Ergonomics Questionnaire (REQUEST) to survey attitudes and opinions of railway workers on a range of human factors issues [277]. Using a set of questions specifically tuned for rail workers the REQUEST is used to understand what are the main factors that influence the human error probability by the workers point of view. The results of a large survey on 3889 worker is presented by the same authors in [278].

Other individual internal end external influence factors have been detailed analyzed in several papers, as reported in the following:

- Mental workload has been discussed in [279], [280]. Mental workload is one of the most critical factors that influence the performance of rail workers. To guarantee that the tasks performed by the operator will be completed safely and effectively it is essential to maintain the mental workload below certain threshold. Studies about mental workload PSF are fundamental in order to evaluate the level of mental workload and develop specific tools for practical assessment. However, there is a considerable lack in current literature on this field. All the works that have been found mainly focus on the effects of mental workload on signaling workers. Further study should be carried out also for other types of safety-critical rail tasks, such as the operators on traffic control centers and drivers.

- The effects of time available for task and punctuality on drivers error probability is studied in [281] with the aim of evaluate if drivers tend to 'take shortcuts' and make mistakes carrying out security procedures with limited available time. This study is extremely helpful since drivers are almost always under pressure of punctuality. This should lays the ground to further research to investigate the effects of shortage of available time for other rail workers, such as signaling workers or operator of traffic control centers.
- Stress and Fatigue have been analyzed in [282], [283] in relationship with work schedules and sleep patterns on different railroad employees. A significant contribution in relationship with stress has been brought by Catelani et. al [284] from University of Florence (Italy) introducing the concept of Eustress (i.e., beneficial level of stress) within the classical assessment of Stress PSF. The Yerkes-Dodson law describes the relationship between stress and performance of the operator and identifies an intermediate optimal level of stress to ensure the optimal performances. Despite the concept of Eustress is widely known between psychologist and human behavior researchers, Catelani et al. [284] is the only work available in literature that integrates it within a complex technique for human reliability analysis in railway field. Thus, it is the authors believe that this critical study about the stress PSF should be considered more in future papers.
- The quality and amount of sleep is the topic of two articles, as in [285], [286]. Both papers discuss the results of a great survey conducted on male train drivers in South Korea. The case study presented in the papers are promising and convincing, however the boundaries set on the survey (only South Korean male train drivers are considered) does not allow to generalize the results. Further works should focus on the extension of this survey to other rail workers.

- Non-technical skills are studied in [287] with the aim of improving the railroad safety systems. The authors propose seventeen non-technical skills establishing that Indian Railway should pay more attention on these factors evaluating human error probability.
- The effects of ergonomics on human errors are presented in [227]. This work is widely considered a milestone in human reliability engineering presenting with clear examples six rail ergonomics/ human factors. Despite this study is the state of the art in the field, further work should focus on the interactions between these ergonomics considerations and the practical assessment of a numerical affect value to be used in HRA techniques.
- The effect of time of day on railroad personnel injuries have been investigated in [288] analyzing 15654 injuries of rail workers from the FRA database. The paper is remarkable, and the discussion of the results is really useful and convincing, especially since installation and maintenance operations on railway tracks is usually performed at night. However, the work lacks a numerical evaluation of such affect essential to introduce the impact of time of day in HEP estimation methods.
- The Perception of work as complex or easy task is studied in [289] with particular reference to situation awareness of railroad workers. However, this PSF is critical also in case of operators working in traffic control centers.
- The effect of environmental conditions on railway operations are dealt with in [290] using Bayes theory to evaluate the risk associated to a human error under different environmental conditions. The analysis of this PSF should be further investigated to understand and quantify if environmental factors have different impacts on the several tasks performed outdoor by rail workers.
- The impact of high-automation levels has been studied in [291].

In summary, several influence factors have been studied and investigated by many works in recent literature. By a qualitative point of view, the body of knowledge seems to be quite covered in this topic, with different analysis concerning several PSFs. However, what stands out by an in-depth review is that a proper evaluation of the intercorrelations between different influence factors is currently missing. Furthermore, most of the study focuses only on a single type of workers, without taking into account that the railway industry is a complex environment characterized by many different types of tasks. This gap should be filled trying to estimate a quantitative assessment of each PSF for different rail workers, such as operators on traffic control centers, train and metro drivers, signaling workers and maintenance operators.

d) Original approaches

The above-mentioned papers discussed different aspect of human factors in railway engineering, by analyzing accident reports, by studying the human performances in presence of specific systems or by evaluating the effects of different PSFs. However, none of the above paper introduce an innovative HRA technique with the aim of calculating the Human Error Probability (HEP) of tasks performed by railway operators.

One of the first original HRA approaches developed for railway application is a non-probabilistic technique known as ACIH (a French acronym for Analysis of Consequences of Human Unreliability) developed by Vanderhaegen in 2001. This method introduced a simplified cognitive model to describe the leading causes of human errors. To assess the system safety, the ACIH method integrates two separated steps: a prospective analysis including the study of the functions, of the context, of the task and of the error consequences; a retrospective analysis including the study of accident reports. The work is interesting since it has been developed specifically for railway engineering, however there is a lack of results validation which is essential for this kind of works.

Few years late, Wreathall et al. in 2004 [215] built an expert elicitation process upon the FRA database to estimate the HEP of several railroad tasks. This technique uses data coming from FRA database but it completely misses to consider internal and external factors that influence human performances.

Since almost all of the HRA method available in literature up to this point were developed to assess HEP in other field of application, Shigemori et al. in 2006 [292] introduces six human error tasks specifically developed for railway engineering. However, the paper does not provide the base HEP associated to each task, making the application of this tasks to quantify the human error probability of other railway systems extremely challenging. Furthermore, also in this case there are no PSFs taken into account to model the effects of internal and external factors on human error probability.

The most important original technique specifically developed for railway application is RARA (Railway Action Reliability Assessment) published in 2012 by the RSSB (the UK Rail Safety and Standards Board) [236]. RARA introduces 8 railway tasks called Generic Task Types (GTTs) and 27 Error Producing Conditions (EPCs). EPCs represents the internal and external factor influencing the human performances that other methods call PSFs. EPCs are used to weight the base human error probability of the selected GTT in order to evaluate the HEP of the considered operation. A qualitative parameter called APOA (Assessed proportion of affect) is used to estimate the impact of each EPC on the human performances.

The main advantages of RARA technique are:

- The introduction of a complete and structured methodology for HEP estimation in railway.
- The definition of 8 tasks specifically developed for rail workers and the evaluation of base error probability for each task validated with field data.
- The evaluation of 27 different influence factors and the numerical estimation of the maximum affect that each factor could have on the human performances.

Despite RARA is without any doubt the most important and widest used original technique for railway HRA assessment, it suffers two major drawbacks. The first one is the fact that it provides a range of possible HEP numerical values for each task, but it does not clearly state how to select a single value within this ranges. The second one is the presence of a highly subjective parameter (i.e., the APOA) to quantify the exact value of affect for each influence factor. Thus, further works concerning the enhancement and improvements of such methodologies are required in order to establish the optimal procedure for railway tasks. With the aim of filling this gap, an improved RARA method has been presented in [293] and then applied also in [294] on a different case study to generalize the approach. The improved RARA uses linguistic variables assessment and fuzzy logic theory to efficiently and effectively assess the human error probability starting from the RARA database. A detail comparison between the classical RARA and the proposed improved technique is presented in the works in order to validate the achieved results. The proposed fuzzy RARA is a powerful and easy tool able to precisely quantify the HEP of railway tasks with a minor impact of subjectivity, reducing (or even deleting) the major drawbacks of classical RARA. Despite the method has been validated by comparison with RARA results, future works concerning the validation of the improved fuzzy RARA using field data and reports on actual incidents from rail safety committees worldwide are required.

e) Application and improvements of existing techniques originally developed for other industries

As seen in the previous subsection, there are only few original methods available in literature specifically developed for HRA in railway. Quite the opposite, many works that have been discovered in this review propose some improvements to extend the range of applicability of other methods originally developed for different application fields. Most of the time, the starting technique is a first-generation or a second-generation method extended to overcome the limitations discussed in literature.

For instance, HEART has been applied to estimate human error during rail transportation of ammonia in Malaysia [295] and to evaluate the HEP of maintenance tasks in railway [296]. An hybrid HEART method is proposed in [238] based on evidence theory and Monte Carlo simulation. A locomotive driving process has been taken as a case study to test the performance of the proposed hybrid HEART. The HEART method is the base of another integrated approach applied to high-speed railway dispatching tasks in [297]. In this case, the GTTs and EPCs proposed by RARA are integrated within the HEART method along with FANP (fuzzy analytic network process). FANP is used to handle uncertainties in expert's judgments removing the critical task of APOA assessment. HEART is a quite common approach for numerical assessment of HEP in many fields. However, it wasn't developed to model rail workers, and thus in the author opinion it requires major adaptations and significant changes before it can be successfully applied to railway operators. As a consequence, the only improved HEART able to provide a consistent HEP evaluation is the one proposed by Wang et al. in [298] thanks to the integration of the RARA task within the HEART technique.

Another technique extensively studied and improved in recent literature is the second-generation CREAM method. In [299] a fuzzy approach based on CREAM and FANP is introduced and applied on human operation in urban railway. Fuzzy-based CREAM have been presented also in [300] (applied to a collision between a commuter train and a train at rest while waiting to pull into a station) and in [301] (applied to high-speed train operations). Similarly to fuzzy approaches, a modified CREAM based on 2-tuple linguistic term sets to describe the cognitive processes of the operator is presented in [302] with an application to high-speed railway dispatchers. CREAM has been applied also by Lombardi et al. [303] to maintenance operations performed on railway systems within the context of an overall system safety analysis. CREAM can be easily integrated with fuzzy logic to reduce subjectivity and thus improve the HEP assessment, as stated by several works mentioned above. The cognitive aspects introduced by CREAM is an important and crucial part of HEP assessment which is usually neglected by the approach for railway industry found in literature. Thus, the extension of CREAM to study rail workers is a fundamental topic and an interesting ongoing line of research. However, it is crucial to tailor the CREAM starting database with railway-specific data about the error probability in order to provide consistent results. This represents the major literature gap in this field.

Quite similar considerations can be drawn for the techniques that improve SLIM methodology. One of the main drawbacks of the SLIM method is the dependencies in the assessment of different PSFs. Trying to solve this issue, an hybrid SLIM integrated with empirical studies and complex network have been applied to railway driving process in [239]. SLIM is also the core of another integrated approach called HuPeROI (Human Performance Railway Operational Index) [240] where Analytic Network Process (ANP) and SLIM are combined to estimate the error probability in case of regional, high-speed and underground trains. A more simple tool is presented in [214] where SLIM is applied to a Serbian railway traffic.

One of the most recent paper published about HRA in railway deals with the improvements of the SHERPA technique (originally developed based on HEART task) proposing an E-SHERPA (Enhanced SHERPA) method [284] applied on maintenance operations performed on ATP systems. The E-SHERPA provides a significant contribution to the body of knowledge since it is one of the very few works that improves and extends an existing technique integrating tasks and error probability data specifically developed for railway systems. Furthermore, E-SHERPA provides the results as a time-dependent model varying during the work shift of the rail operator. The technique uses customized functions to simulate the variation of the likelihood of error before and after a lunch break taking into account an increment in performances when the operator is not working. Furthermore, the E-SHERPA considers the concept of Eustress introduced by the Yerkes-Dodson law to model the stress PSF and the assessment of the error probability. The above-mentioned features make the E-SHERPA one of the most interesting and powerful tool to evaluate the human error probability of rail operators performing different kinds of tasks. However, the authors in [284] applied the E-SHERPA method only to maintenance operations performed on balises used in ATP systems. Thus, the method should be applied and validated with actual failure/incident data to other railway-related activities.

Along with the widely known HRA methods used to evaluate the HEP there are also other approach used to analyses the causes of accidents by a human factor point of view. The Human Factors Analysis and Classification System (HFACS) is a method used for accident analysis and investigation published in 2003 for avionic applications [304]. This method has been successfully applied to railway after several improvements. It has been integrated with the Systems–Theoretical Accident Modelling and Processes (STAMP) in [305], while the ANP and the Decision Making Trail and Evaluation (DEMATEL) method are used in [306] to present a HFACS-Ras (HFACS-Railway Accidents). A modified version of the latter has also been applied to SPAD event in Australian railroads [307], to minor safety accidents in UK rail lines [308] and to American railroads by means of the FRA database [218].

4.5 Railway Action Reliability Assessment

The Rail Safety and Standards Board [309] developed the only rail-specific human reliability assessment in 2012. RARA (Railway Action Reliability Assessment) is the most common HRA technique in railway engineering since it is the only one developed only for this kind of application. RARA classifies the human activities in railway within eight different Generic Task Types (GTTs) grouped into three categories:

- More automated and skill-based processes, simple and well-known activities by the operator that require minimal mental involvement;
- More effortful and rule-based processes, activities that require mental involvement in order to apply rules and tasks for which the operator has been trained;
- Thinking outside procedures, activities that require high mental involvement aimed at solving problems never faced before.

Table 4.6 illustrates the complete list of all GTTs. For each GTT the method provides a range of variation of the human error probability and a nominal value within this range. GTTs describe in a generic way the type of task that the operator must perform. To obtain a more precise result, the nominal HEP value is modeled using Error Producing Conditions (EPC). These are the factors that adversely affect human performance and are used to adapt the generic task to the real one. EPCs increase the HEP associated with a GTT based on operating conditions. RARA considers 27 different Error Producing Conditions (EPCs) to take into account the internal and external factor that influence the human behavior.

Tab. 4. 6 - RARA Generic Task Type list

Area	**GTT**	**HEP**	**Bounds**
More automated and skill-based processes	**R1**. Respond correctly to system command even when there is an automated system providing accurate interpretation of system state.	0.00002	0.000006-0.0009
	R2. Completely familiar, well designed, highly practiced task which is routine.	0.0004	0.00008-0.007
	R3. Simple response to a dedicated alarm and execution of actions covered in procedures.	0.0004	0.00008-0.007
	R4. Skill-based tasks (manual, visual or communication) when there is some opportunity for confusion.	0.003	0.002-0.004
	R5. Fairly simple task performed rapidly or given insufficient or inadequate attention.	0.09	0.06-0.13
More effortful and rule-based processes	**R6**. Restore or shift a system to original or new state, following procedures with some checking.	0.003	0.0008-0.007
	R7. Identification of situation requiring interpretation of alarm patterns.	0.07	0.02-0.17
Thinking outside procedures	**R8**. Complex task requiring a high level of understanding and skill.	0.16	0.12-0.28

Tab. 4. 7 - Error Producing Conditions list

Area	**Ref**	**EPC**	**MA**
Task design	T1	Unfamiliarity with a situation which is potentially important, but which only occurs infrequently, or which is novel.	17
	T2	A shortage of time available for error detection and correction.	11
	T3	A need to unlearn a technique and apply one which requires the application of an opposing philosophy.	8
	T4	The need to transfer specific knowledge from task to task without loss.	5.5
	T5	An impoverished quality of information conveyed by person/person interaction.	3
	T6	Little or no independent checking or testing of output.	3
	T7	A conflict between immediate and long-term objectives.	2.5
	T8	Unclear allocation of function and responsibility.	1.6
	T9	A danger that finite physical capabilities will be exceeded.	1.4
	T10	Prolonged inactivity or highly repetitious cycling of half hour low mental workload tasks.	1.1
Interface	ln1	A low signal-noise ratio.	10
	ln2	A means of suppressing or over-riding information of features which is too easily accessible.	9
	ln3	No means of conveying spatial and functional information to operators in a form which they can readily assimilate.	8
	ln4	A mismatch between an operator’s model of the world and that imagined by a designer.	8
	ln5	No obvious means of reversing an unintended action.	8
	ln6	A channel capacity overload, particularly one caused by simultaneous presentation of non-redundant information.	6
	ln7	Poor, ambiguous or ill-matched system feedback.	4
Competence	C	Operator inexperience.	3
Procedures	PR1	Ambiguity in the required performance standard.	5
	PR2	An impoverished quality of information conveyed by procedures.	3
Person	P1	A mismatch between perceived and real risk.	4
	P2	Fatigue from shift and work patterns.	2.6
	P3	High level emotional stress.	2
	P4	Little opportunity to exercise mind and body outside the immediate confines of a job.	1.8
	P5	Little or no intrinsic meaning in a task.	1.4
	P6	Low workforce morale.	1.2
Environment	E	A poor or hostile environment.	8

The complete list of the EPC is illustrated in table 4.7. For each EPC the technique provides the Maximum Affect (MA) that this will have on the operator.

The 27 different EPCs proposed by RARA are grouped into six main sections:

- Task design: EPCs related to the characteristics of the task.
- Interface design: EPCs related to the human-machine interface. They also take into account all the objects that the operator uses.
- Competence management: EPCs related to the quality of staff training.
- Procedures: EPC related to the quality of the procedures and documentation necessary for the realization of a given task.
- Person: EPC related to the personnel performing the task, such as the physical, mental and psychological characteristics that affect the reliability of the operator himself.
- Environment: EPCs related to the physical environment in which the task is performed.

The MA value is weighted by means of the APOA (Assessed proportion of affect) to evaluate how much the EPC actually affects the task, as follow:

$$\mathrm{A} = (\mathrm{MA} - 1) \cdot \mathrm{APOA} + 1 \tag{4.1}$$

$$APOA = \begin{cases} 1\ Full\ Affect \\ 0.9 \\ 0.8 \\ 0.7 \\ 0.6 \\ 0.5\ \ Medium\ Affect \\ 0.4 \\ 0.3 \\ 0.2 \\ 0.1\ Small\ Affect \end{cases} \tag{4.2}$$

Where the greater the APOA, the greater the affect A that the EPC will have on the task. Finally, considering:

- HEP_{nom} the error probability of the selected GTT;
- A_i the generic affect of the EPC_i;
- n the number of selected EPC;

then the RARA model calculates the human error probability HEP as follow:

$$HEP = HEP_{nom} \cdot \prod_{i=1}^{n} A_i \tag{4.3}$$

$$HEP = HEP_{nom} \cdot \prod_{i=1}^{n} [(\mathrm{MA}_i - 1) \cdot \mathrm{APOA}_i + 1] \tag{4.4}$$

Fig. 4.12 shows a graph highlighting the trend of HEP as a function of nominal HEP and the parameter that holds against EPCs. The HEP values for some GTTs with the same EPC are highlighted, we note the presence of a strong step between R4&R6 and R7.

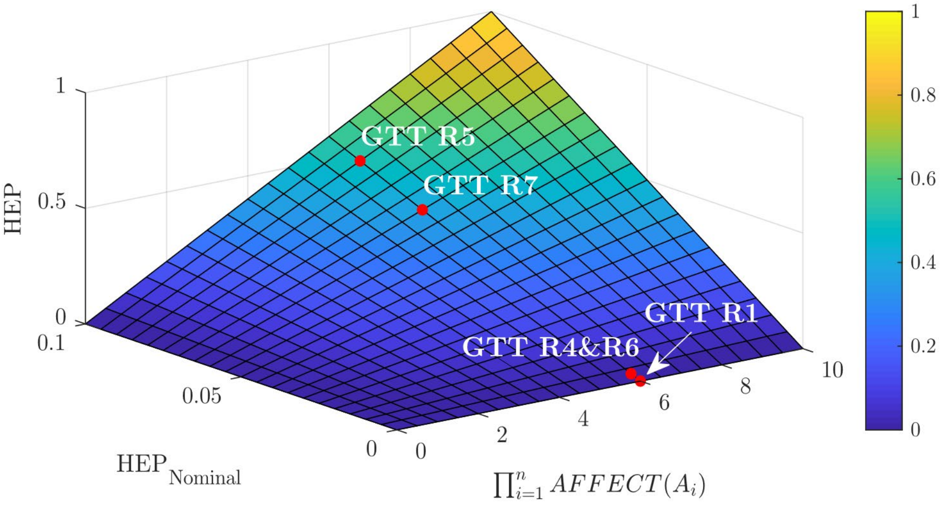


Fig. 4. 12- HEP trend in the RARA technique

RARA method is extensively used in railway engineering since it is the only approach widely recognized in this field. However, several criticalities could be found in this technique.

The first one is the impact of subjectivity of the analyst that performs the evaluation, which is not taken into account. The second one is the difficulty and complexity required for the assessment of the numerical values which represent the impact of each external factor that influence the human performances. Therefore, the quality of the estimation is extremely related to the experience of the analyst performing the assessment.

4.6 Final remarks

This chapter reviewed the state of the art of Human Reliability Analysis in railway applications. HRA is a fundamental topic which is now drawing the attention of several researchers. However, a comprehensive literature review and bibliometric analysis of HRA methodologies in railway operations is currently missing. Trying to fill this gap, this paper analyzes the body of knowledge of HRA in railway by means of the SCOPUS databases. Starting from 60,013 documents related to 'human reliability', 'human error' and 'human factor', a screening process has been used to reduce the number of papers based on the field of application (railway and railroads keywords), the publication year (from 2000 to August 2021), the language (limited to English documents) and the type of document (only peer-reviewed research article have been selected, neglecting conference papers, books, editorials, etc). The resulting 268 papers have been subjected to a bibliometric analysis highlighting a significant increase of the interest in this topic in the last few years. Both trends of number of papers and number of citations confirm this point, as well as the geographical distribution of the papers and the analysis of significant journals highlighted a widespread interest of the topic all over the world with several different publishers and journals.

The final part discusses the main contributions of the most significant articles discovered during this review. The analysis highlights that very few works deal with the proposal of innovative HRA methods specifically developed for railway. Quite the contrary, most of the papers in this field are concentrated in two macro-areas. The first one deals with the analysis of major railway accidents occurred in the last years in order to find the causes of the accidents by a human error point of view. The second one deals with the improvements of existing techniques originally developed to other fields (especially first- and second-generation techniques such as the CREAM, HEART and SLIM methods) in order to successfully apply such methodologies to railway engineering minimizing their drawbacks using fuzzy sets, ANP, Monte Carlo simulation, empirical studies, etc.

In conclusion, the research direction in HRA field for railway engineering seems to be firmly established toward the analysis and review of significant accidents and the improvements of existing techniques originally developed to other fields of application. The former topic is a widely known and well-studied line of research that is proceeding forward since new accidents/incidents reports are constantly available. The state of the art has gain great experience in this topic and it should be ready to develop integrated methodology to continuously and automatically improve the HEP database of the existing techniques using the results of the accident analysis. Quite the contrary, the latter topic needs further developments and enhancements in terms of:

- Validation of proposed methodologies with field data.
- Application of existing techniques to different types of rail workers to ensure consistent results in every different aspect of railway engineering (e.g., train drivers, operators of traffic centers, maintenance crew, installation and verification worker of railroad equipment, etc.).
- Extension of CREAM or other cognitive-based approaches to railway engineering.
- Study of the intercorrelations between different internal and external influence factors for different kinds of railway-related tasks.
- Estimation of a quantitative assessment for each PSF for different rail workers.

Last section is dedicated to RARA technique, to fully explain the method and the assessment. RARA is the only recognized method designed for railway, however it presents some drawbacks due to the subjectivity of the assessment and the complexity of the method.

Chapter 5

Proposed improvements in HRA for railway

This chapter provides a contribution for the HRA il railway proposing a fuzzy-HRA method. Human error in railway is mostly assessed by using the Railway Action Reliability Assessment (RARA), this technique presents a complex and very subjective assessment. Starting from this issue an innovative HRA based on RARA and fuzzy theory is proposed. This new technique is very useful in case of failure data are seldom available (which is a very common situation in HRA). The proposed method provides as output a range of possible HEP values (Fuzzy HEP) and a unique crisp value (defuzzified HEP) by means of centroid defuzzification. The linguistic approach of fuzzy inference and a dedicated tool facilitates the assessment of the operator.

[1] The proposed HRA method has been published as "L. Ciani, G. Guidi, G. Patrizi, and D. Galar, "Improving Human Reliability Analysis for railway systems using fuzzy logic, *IEEE Access*, vol. 9, pp. 128448–128662, 2021".

5.1 Introduction

Railway engineering is a complex field in which many aspects of work are performed by human operators throughout the complete system life cycle. Starting from design and construction of the system up to the functioning, management and maintenance, human operators play a fundamental role in the life cycle of most of the railway-related systems [310]. Several papers and technical reports (see for instance [5], [172], [210], [211]) agree that most of railway accidents are caused by human error or by the combination of human errors with hardware/software failure. Therefore, Human Reliability Analysis represents a challenging research field fundamental for industry management to ensure high safety level, to maximize the performances and minimize the operation and maintenance cost.

In railway field, most of the time the errors of the train driver are detected by safety systems, therefore the probability of accident caused by an error of the driver is extremely low.

Train integrates several devices used to correct and/or mitigate the effects of an error of the operator. These systems are called Automatic Train Protection (ATP) and represents a design requirement in every railway infrastructure.

Thus, the most critical human errors which could cause catastrophic events or terrible accidents are committed during the design, installation and maintenance phases.

As detailed explained in the previous chapter, several HRA techniques are available in literature. However, only one technique, specifically developed for railway engineering, has been published. The Rail Safety and Standards Board proposes a customized technique called Railway Action Reliability Assessment (RARA) in 2012 to evaluate the human error probability in railway field [236]. RARA method is extensively used in railway engineering since it is the only approach widely recognized in this field. However, several criticalities could be found in this technique. The first one is the impact of subjectivity of the analyst that performs the evaluation, which is not taken into account. The second one is the difficulty and complexity of the numerical assessment for the model parameters. Therefore, the quality of the estimation is extremely related to the experience of the analyst which perform the assessment. Trying to solve these needs, this chapter proposes an innovative approach for Human Error Probability (HEP) estimation specifically customized for railway engineering. The proposed approach is based on fuzzy logic and interval arithmetic to estimate the HEP reducing the drawbacks of RARA method. The use of fuzzy concept against the determinist cases provides several benefits. For example, it simplifies the assessment of the HEP using linguistic variables to describe both the probability of error and the affect level of each external factor. Moreover, it provides a range of possible HEP instead of a single value which is a fundamental feature in case of uncertain data. Finally, fuzzy logic also allows to minimize the subjectivity of the evaluation and the impact of analyst experience accurately balancing precision and results significance.

5.2 Review of fuzzy methods for HRA

Human Reliability Analysis requires failure data to achieve quantitative analysis. However, it is not always possible to fully obtain this data due to unavailability of observations and consequent scarcity of statistical data about errors and failures [23]. Therefore, some works introduce fuzzy set theory to handle reliability evaluation under conditions of uncertainty.

Some papers in literature deal with a fuzzy cognitive reliability and error analysis method - fuzzy CREAM [300], [311]. This method uses fuzzy logic for the calculation of human error probability from if-then rules and a defuzzification procedure. The main disadvantages of this method are time-consuming processes to develop the rules and risk of using contradicting rules. To overcome these problems Rotshtein et al. [312] proposes a procedure which introduced membership functions of fuzzy perfection of performance conditions and the theory of decision-making in CREAM. To validate the approach five scenarios have been considered. Zhou in [313] uses the fuzzy logic to model the uncertainty and ambiguity of the Common Performance Conditions (CPCs) as well the control modes in CREAM. The probability distribution of each control mode and consequently the human error probability are evaluated by means of a Bayesian network and the membership function of the CPCs. Another work [314] develops a fuzzy Bayesian network (BN) approach to improve the quantification of organizational influences in HRA (human reliability analysis) frameworks. Kumar in [315] presents Fuzzy HEART and Expert elicitation for performing quantification of human error probability with an application to refueling operation in an refueling station. This approach integrates the fuzzy membership function during the assessment of the Error Producing Conditions.

Finally, they validate their new approach comparing the result obtained with the CREAM assessment. Bayesian networks and fuzzy logic are used also in [316].

5.3 First proposed method: fuzzy-based approach

This section illustrates the proposed fuzzy-based approach used to evaluate the human error probability for railway engineering. The new approach is based on fuzzy logic and interval arithmetic to estimate the HEP reducing the drawbacks of RARA method

The major advantages of this new procedure are:

- The use of linguistic variables to describe both the probability of error and the affect level of each external factor, reduce the complexity and the subjectivity of the assessment.
- The resulting HEP is provided as a range of possible HEP instead of a single value which is a fundamental feature in case of uncertain data.
- Fuzzy logic also allows to minimize the subjectivity of the evaluation and the impact of analyst experience accurately balancing precision and results significance.

Taking the database of the RARA method, the proposed approach consists in several steps in order to calculate the HEP in a simpler way for the analyst with consistent results. Since data regarding human failure are not always available, the proposed approach starts with the validated data provided by RARA. Then, fuzzy logic is used to combine the base human error probability and the external affect conditions in order to estimate the probability of committing an error during the work shift. The fuzzy logic helps mitigating the effects of uncertainty data, as well as it is able to minimize the subjectivity of the human reliability evaluation by means of linguistic variable instead of numeric values. In this way, the analyst that carry out the evaluation must choose between different membership functions and their associated linguistic variable instead of picking a value within the range of the HEP or choosing an APOA value to quantify the Affect A_i of each EPC. The steps required to calculate the HEP using the proposed fuzzy approach are illustrated in fig. 5.1.

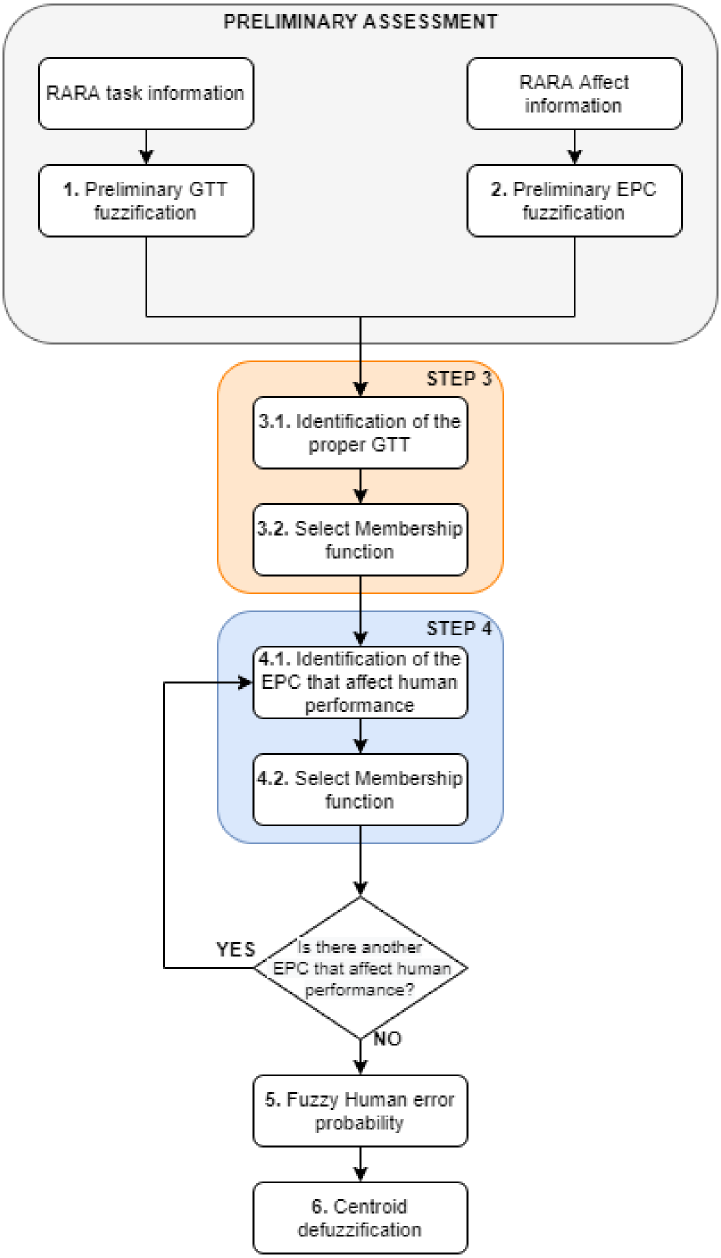

PRELIMINARY ASSESSMENT
RARA task information
RARA Affect information
1. Preliminary GTT fuzzification
2. Preliminary EPC fuzzification
STEP 3
3.1. Identification of the proper GTT
3.2. Select Membership function
STEP 4
4.1. Identification of the EPC that affect human performance
4.2. Select Membership function
YES
Is there another EPC that affect human performance?
NO
5. Fuzzy Human error probability
6. Centroid defuzzification

Fig. 5. 1- Flowchart of the proposed Fuzzy-based approach used to estimate the human error probability in railway engineering.

More in detail:

1. Preliminary GTT fuzzification.

1.1. Use HEP_{min}, HEP_{max} and HEP_{nom} provided by RARA for each GTT to identify the domain of the fuzzy set.

1.2. Identify 3-5 membership functions for each fuzzy set of the GTT.

2. Preliminary EPC fuzzification.

2.1. Calculate minimum (APOA=0.1) and maximum (APOA=1) value of any affect considered by RARA.

2.2. Create a domain of the fuzzy set for each affect.

2.3. Define 5 membership functions for each affect.

3. Identification of the proper GTT.

3.1. Select a Generic Task Type (GTT).

3.2. Select a membership function for the considered GTT.

4. Identification of the EPC.

4.1. Select any Error Producing Conditions i which are relevant to the task being assessed.

4.2. Select a membership function for each EPC.

5. Calculate the Human Error Probability $\widetilde{HEP}$.

6. Defuzzification of the fuzzy $\widetilde{HEP}$ using centroid method.

RARA method is based on eight different GTTs. For each one of them RARA provides a minimum value of the error probability HEP_{min}, a maximum value HEP_{max} and a nominal value HEP_{nom} which correspond to the most probable error probability for the considered task [236] (For more information see Section 4.5). The list of all GTTs and the corresponding minimum, maximum and nominal HEP is illustrated in Table 5.1.

Step 1 of the proposed procedure uses these values to calculate the fuzzy human error probability associated to each GTT. More in detail, a fuzzy base human error probability $\widetilde{HEP}_{b_i}$ will be associated to each kind of task i as follow:

$$\widetilde{HEP}_{b_i} = \left\{ \left(x, \mu_{GTT_i}(x) \right) \mid x \in D_{GTT_i} \right\} \tag{5.1}$$

$$\mu_{GTT_i}(x) : D_{GTT_i} \rightarrow [0, 1] \tag{5.2}$$

$$D_{GTT_i} = \left[HEP_{min_i} , HEP_{max_i} \right] \tag{5.3}$$

Where $\mu_{GTT_i}(x)$ represents the membership functions of the task i while D_{GTT_i} is the domain of possible admissible value by the fuzzy base error probability

$\widetilde{HEP_{b_i}}$ of the GTT i. As in equation (5.3) domain D_{GTT_i} is generated using the minimum and maximum value of the HEP provided by RARA for each GTT (Table 5.1).

Tab. 5. 1- Generic Task Type and Human Error Probability according to RARA technique [236].

Generic Task Type	**HEP$_{\text{min}}$**	**HEP$_{\text{nom}}$**	**HEP$_{\text{max}}$**
R1. Respond correctly to system command even when there is an automated system providing accurate interpretation of system state.	0.0006%	0.002%	0.09%
R2. Completely familiar, well designed, highly practiced task which is routine.	0.008%	0.04%	0.7%
R3. Simple response to a dedicated alarm and execution of actions covered in procedures.	0.008%	0.04%	0.7%
R4. Skill-based tasks (manual, visual or communication) when there is some opportunity for confusion.	0.2%	0.3%	0.4%
R5. Fairly simple task performed rapidly or given insufficient or inadequate attention.	6%	9%	13%
R6. Restore or shift a system to original or new state, following procedures with some checking.	0.08%	0.3%	0.7%
R7. Identification of situation requiring interpretation of alarm/ indication patterns.	2%	7%	17%
R8. Complex task requiring a high level of understanding and skill.	12%	16%	28%

The result of this preliminary fuzzification step is shown in fig. 5.2, where the fuzzy sets developed for each GTT are illustrated. Inside the domain D_{GTT_i} of each task a different number of trapezoidal membership functions (three, four or five) have been located depending on the extension of the domain itself. To each MF of each GTT have been assigned a linguistic variable which intuitively describes the probability of error of the considered GTT.

Six different linguistic variables with increasing probability values have been developed, namely: $\{Very\ Low;\ Low;\ Moderate;\ Medium;\ High;\ Very\ High\}$ Along with minimum and maximum value of HEP for each GTT, RARA also provides a nominal value which according to the original technique is the most probable value within the range. To take into account also this information the membership function that encloses the RARA nominal HEP has been developed larger than the others, with more values with maximum degree of membership.

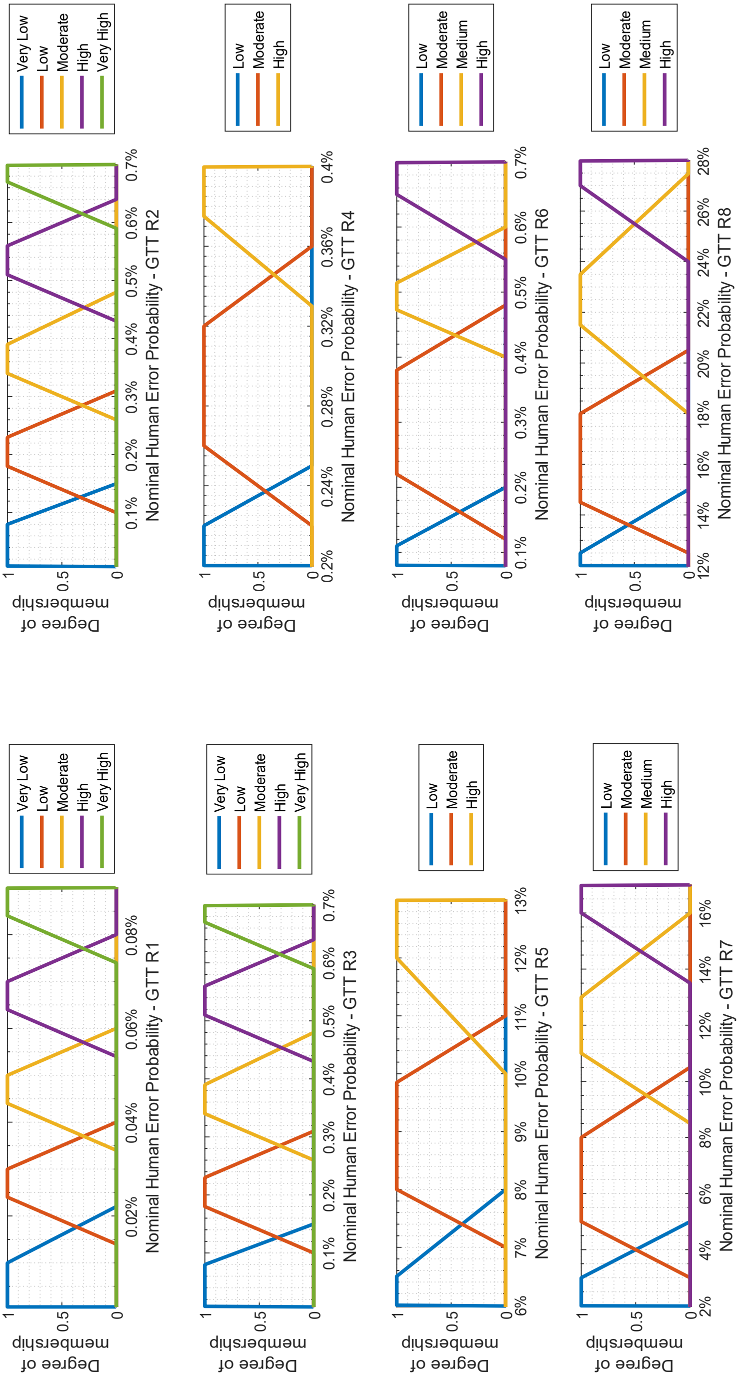


Fig. 5. 2- Membership functions proposed to estimate the HEP of each Generic Task Type (GTT) included in the procedure.

The second step is quite similar to the first one. The objective of the fuzzification this time is the value of the affect of each EPC j. RARA evaluates the affect of each EPC by means of the Maximum Affect MA and the APOA value as in Equation (4.4). The proposed method introduces linguistic variables instead of the APOA value to estimate the level of affect. More in detail, the fuzzy affect $\widetilde{A_J}$ of each EPC j is defined as follow:

$$\widetilde{A_J} = \left\{\left(z,\ \mu_{EPC_j}(z)\right) \mid z\ \in\ D_{EPC_j}\right\} \tag{5.4}$$

$$\mu_{EPC_j}(z) :\ D_{EPC_j}\ \rightarrow\ [0,1] \tag{5.5}$$

$$D_{EPC_j}\ =\ \left[A_{min_j}\ ,\ A_{max_j}\ \right] \tag{5.6}$$

Where $\mu_{EPC_j}(x)$ stands for the membership functions of the EPC j while D_{EPC_j} represents the domain of possible admissible value by the fuzzy affect $\tilde{A}_j$ of the EPC j. The minimum A_{min_j} and maximum A_{max_j} affect value of each EPC j used to generate the domain D_{EPC_j} have been evaluated setting the minimum and maximum APOA value respectively within Equations (3) and (4), as follow:

$$A_{min_j} = (\mathrm{MA}\ -\ 1)\cdot\ 0.1\ +\ 1 \tag{5.7}$$

$$A_{max_j} = (\mathrm{MA}\ -\ 1)\cdot 1\ +\ 1\ =\ \mathrm{MA} \tag{5.8}$$

For the definition of each EPC see Table 4.6 in Section 4.5. For the sake of brevity, the following notation for trapezoidal membership function have been used:

$$A_{TRAP} = (z_1, z_2, z_3, z_1) \tag{5.9}$$

Where the relationship between mathematical notation and trapezoidal membership function is explained in fig. 5.3.

Inside the domain D_{EPC_j} of each EPC five trapezoidal membership functions have been designed. To each one of them a linguistic variable has been assigned to easily describes the affect level of the considered EPC. The five corresponding linguistic variables are the following $\{Very\ Low;\ Low;\ Moderate;\ High;\ Very\ High\}$.

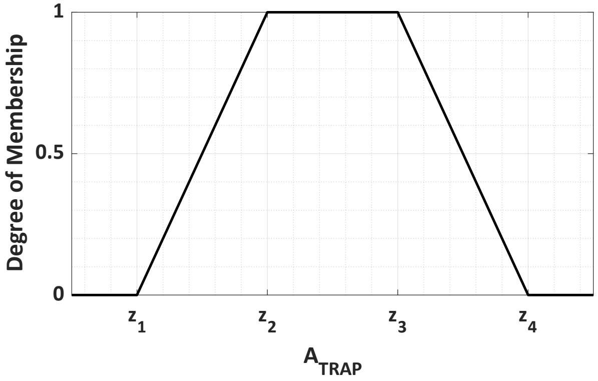


Fig. 5. 3 - Example of a generic trapezoidal membership function.

The result of this preliminary fuzzification step is shown below, where the fuzzy sets developed for each EPC are listed.

Task design:

- EPC T1 characterized by MA = 7
    - Very Low: VL = (2.6, 2.6, 2.96, 5.84)
    - Low: L = (2.96, 5.84, 6.56, 9.44)
    - Moderate: M = (6.56, 9.44, 10.16, 13.04)
    - High: H = (10.16, 13.04, 13.76, 16.64)
    - Very High: VH = (13.76, 16.64, 17, 17)
- EPC T2 characterized by MA = 11
    - Very Low: VL = (2, 2, 2.225, 4.025)
    - Low: L = (2.225, 4.025, 4.475, 6.275)
    - Moderate: M = (4.475, 6.275, 6.725, 8.525)
    - High: H = (6.725, 8.525, 8.975, 10.78)
    - Very High: VH = (8.975, 10.78, 11, 11)
- EPC T3 characterized by MA = 8
    - Very Low: VL = (1.7, 1.7, 1.857, 3.117)
    - Low: L = (1.857, 3.117, 3.432, 4.693)
    - Moderate: M = (3.433, 4.692, 5.007, 6.267)
    - High: H = (5.007, 6.268, 6.582, 7.843)
    - Very High: VH = (6.583, 7.843, 8, 8)
- EPC T4 characterized by MA = 5.5
    - Very Low: VL = (1.45, 1.45, 1.551, 2.361)
    - Low: L = (1.551, 2.361, 2.563, 3.374)

  - Moderate: M = (2.564, 3.373, 3.576, 4.386)
  - High: H = (3.576, 4.387, 4.588, 5.399)
  - Very High: VH = (4.589, 5.399, 5.5, 5.5)
- EPC T5 characterized by MA = 3
  - Very Low: VL = (1.2, 1.2, 1.245, 1.605)
  - Low: L = (1.245, 1.605, 1.695, 2.055)
  - Moderate: M = (1.695, 2.055, 2.145, 2.505)
  - High: H = (2.145, 2.505, 2.595, 2.955)
  - Very High: VH = (2.595, 2.955, 3, 3)
- EPC T6 characterized by MA = 3
  - Very Low: VL = (1.2, 1.2, 1.245, 1.605)
  - Low: L = (1.245, 1.605, 1.695, 2.055)
  - Moderate: M = (1.695, 2.055, 2.145, 2.505)
  - High: H = (2.145, 2.505, 2.595, 2.955)
  - Very High: VH = (2.595, 2.955, 3, 3)
- EPC T7 characterized by MA = 2.5
  - Very Low: VL = (1.15, 1.15, 1.184, 1.454)
  - Low: L = (1.184, 1.454, 1.521, 1.791)
  - Moderate: M = (1.521, 1.791, 1.859, 2.129)
  - High: H = (1.859, 2.129, 2.196, 2.466)
  - Very High: VH = (2.196, 2.466, 2.5, 2.5)
- EPC T8 characterized by MA = 1.6
  - Very Low: VL = (1.06, 1.06, 1.074, 1.181)
  - Low: L = (1.073, 1.181, 1.209, 1.317)
  - Moderate: M = (1.209, 1.317, 1.344, 1.451)
  - High: H = (1.343, 1.452, 1.479, 1.587)
  - Very High: VH = (1.479, 1.587, 1.6, 1.6)
- EPC T9 characterized by MA = 1.4
  - Very Low: VL = (1.04, 1.04, 1.049, 1.121)
  - Low: L = (1.049, 1.121, 1.139, 1.211)
  - Moderate: M = (1.139, 1.211, 1.229, 1.301)
  - High: H = (1.229, 1.301, 1.319, 1.391)
  - Very High: VH = (1.319, 1.391, 1.4, 1.4)
- EPC T10 characterized by MA = 1.1
  - Very Low: VL = (1.005, 1.005, 1.006, 1.015)
  - Low: L = (1.006, 1.015, 1.017, 1.026)
  - Moderate: M = (1.017, 1.026, 1.029, 1.038)
  - High: H = (1.029, 1.038, 1.04, 1.049)

  - Very High: VH = (1.04, 1.049, 1.05, 1.05)

Interface:

- EPC In1 characterized by MA = 10
  - Very Low: VL = (1.9, 1.9, 2.103, 3.722)
  - Low: L = (2.102, 3.723, 4.127, 5.748)
  - Moderate: M = (4.127, 5.747, 6.152, 7.772)
  - High: H = (6.152, 7.772, 8.178, 9.798)
  - Very High: VH = (8.178, 9.797, 10, 10)
- EPC In2 characterized by MA = 9
  - Very Low: VL = (1.8, 1.8, 1.98, 3.42)
  - Low: L = (1.98, 3.42, 3.78, 5.22)
  - Moderate: M = (3.78, 5.22, 5.58, 7.02)
  - High: H = (5.58, 7.02, 7.38, 8.82)
  - Very High: VH = (7.38, 8.82, 9, 9)
- EPC In3 characterized by MA = 8
  - Very Low: VL = (1.7, 1.7, 1.857, 3.117)
  - Low: L = (1.857, 3.117, 3.432, 4.693)
  - Moderate: M = (3.433, 4.692, 5.007, 6.267)
  - High: H = (5.007, 6.268, 6.582, 7.843)
  - Very High: VH = (6.583, 7.843, 8, 8)
- EPC In4 characterized by MA = 8
  - Very Low: VL = (1.7, 1.7, 1.857, 3.117)
  - Low: L = (1.857, 3.117, 3.432, 4.693)
  - Moderate: M = (3.433, 4.692, 5.007, 6.267)
  - High: H = (5.007, 6.268, 6.582, 7.843)
  - Very High: VH = (6.583, 7.843, 8, 8)
- EPC In5 characterized by MA = 8
  - Very Low: VL = (1.7, 1.7, 1.857, 3.117)
  - Low: L = (1.857, 3.117, 3.432, 4.693)
  - Moderate: M = (3.433, 4.692, 5.007, 6.267)
  - High: H = (5.007, 6.268, 6.582, 7.843)
  - Very High: VH = (6.583, 7.843, 8, 8)
- EPC In6 characterized by MA = 6
  - Very Low: VL = (1.5, 1.5, 1.613, 2.513)
  - Low: L = (1.612, 2.513, 2.737, 3.638)
  - Moderate: M = (2.737, 3.638, 3.862, 4.763)

  - High: H = (3.862, 4.763, 4.987, 5.888)
  - Very High: VH = (4.987, 5.888, 6, 6)
- EPC In7 characterized by MA = 4
  - Very Low: VL = (1.3, 1.3, 1.367, 1.908)
  - Low: L = (1.368, 1.908, 2.042, 2.583)
  - Moderate: M = (2.043, 2.583, 2.718, 3.258)
  - High: H = (2.718, 3.258, 3.393, 3.933)
  - Very High: VH = (3.393, 3.933, 4, 4)

Competence Management:

- EPC C characterized by MA = 9
  - Very Low: VL = (1.2, 1.2, 1.245, 1.605)
  - Low: L = (1.245, 1.605, 1.695, 2.055)
  - Moderate: M = (1.695, 2.055, 2.145, 2.505)
  - High: H = (2.145, 2.505, 2.595, 2.955)
  - Very High: VH = (2.595, 2.955, 3, 3)

Procedure:

- EPC PR1 characterized by MA = 5
  - Very Low: VL = (1.4, 1.4, 1.49, 2.21)
  - Low: L = (1.49, 2.21, 2.39, 3.11)
  - Moderate: M = (2.39, 3.11, 3.29, 4.01)
  - High: H = (3.29, 4.01, 4.19, 4.91)
  - Very High: VH = (4.19, 4.91, 5, 5)
- EPC PR2 characterized by MA = 3
  - Very Low: VL = (1.2, 1.2, 1.245, 1.605)
  - Low: L = (1.245, 1.605, 1.695, 2.055)
  - Moderate: M = (1.695, 2.055, 2.145, 2.505)
  - High: H = (2.145, 2.505, 2.595, 2.955)
  - Very High: VH = (2.595, 2.955, 3, 3)

Person:

- EPC P1 characterized by MA = 4
  - Very Low: VL = (1.3, 1.3, 1.367, 1.908)
  - Low: L = (1.368, 1.908, 2.042, 2.583)
  - Moderate: M = (2.043, 2.583, 2.718, 3.258)
  - High: H = (2.718, 3.258, 3.393, 3.933)
  - Very High: VH = (3.393, 3.933, 4, 4)

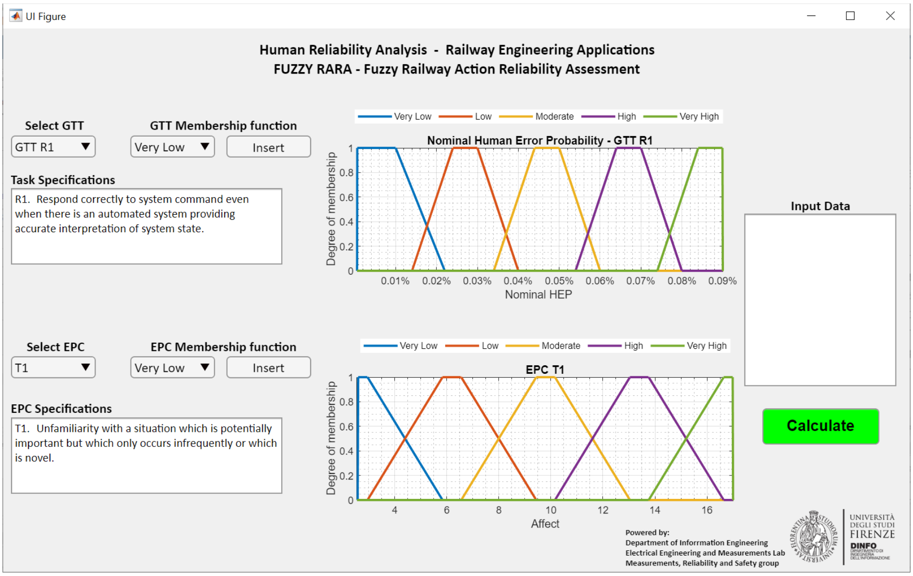
- EPC P2 characterized by MA = 2.6
    - Very Low: VL = (1.16, 1.16, 1.196, 1.484)
    - Low: L = (1.196, 1.484, 1.556, 1.844)
    - Moderate: M = (1.556, 1.844, 1.916, 2.204)
    - High: H = (1.916, 2.204, 2.276, 2.564)
    - Very High: VH = (2.276, 2.564, 2.6, 2.6)
- EPC P3 characterized by MA = 2
    - Very Low: VL = (1.1, 1.1, 1.123, 1.303)
    - Low: L = (1.123, 1.303, 1.348, 1.528)
    - Moderate: M = (1.347, 1.528, 1.573, 1.753)
    - High: H = (1.572, 1.752, 1.797, 1.978)
    - Very High: VH = (1.797, 1.978, 2, 2)
- EPC P4 characterized by MA = 1.8
    - Very Low: VL = (1.08, 1.08, 1.098, 1.242)
    - Low: L = (1.098, 1.242, 1.278, 1.422)
    - Moderate: M = (1.278, 1.422, 1.458, 1.602)
    - High: H = (1.458, 1.602, 1.638, 1.782)
    - Very High: VH = (1.638, 1.782, 1.8, 1.8)
- EPC P5 characterized by MA = 1.4
    - Very Low: VL = (1.04, 1.04, 1.049, 1.121)
    - Low: L = (1.049, 1.121, 1.139, 1.211)
    - Moderate: M = (1.139, 1.211, 1.229, 1.301)
    - High: H = (1.229, 1.301, 1.319, 1.391)
    - Very High: VH = (1.319, 1.391, 1.4, 1.4)
- EPC P6 characterized by MA = 1.2
    - Very Low: VL = (1.02, 1.02, 1.024, 1.06)
    - Low: L = (1.024, 1.06, 1.069, 1.105)
    - Moderate: M = (1.069, 1.105, 1.114, 1.15)
    - High: H = (1.115, 1.151, 1.159, 1.196)
    - Very High: VH = (1.159, 1.196, 1.2, 1.2)

Environment:

- EPC E characterized by MA = 8
    - Very Low: VL = (1.7, 1.7, 1.857, 3.117)
    - Low: L = (1.857, 3.117, 3.432, 4.693)
    - Moderate: M = (3.433, 4.692, 5.007, 6.267)
    - High: H = (5.007, 6.268, 6.582, 7.843)

- Very High: VH = (6.583, 7.843, 8, 8)

The two above-described steps are preliminary phases carried out only one time. It is not necessary to repeat the GTT and EPC fuzzification every time that a human error probability is assessed by means of the proposed method. Therefore, a suitable tool has been specifically developed using MATLAB R2020b to automatize the assessment using the proposed method. A screenshot of the Graphical User Interface is reported in fig. 5.4. The top left panel of the developed software allows to select the Generic Task Type that better describes the task that the operator under analysis has to perform. Then the panel also allows to select the membership function, that according to the analyst performing the assessment is the optimal choice (Step 3). The top figure in the center of the tool illustrates the membership functions of the selected task within the proper domain D_{GTT_i}.



UI Figure

Human Reliability Analysis - Railway Engineering Applications
FUZZY RARA - Fuzzy Railway Action Reliability Assessment

Select GTT: GTT R1

GTT Membership function: Very Low

Task Specifications

R1. Respond correctly to system command even when there is an automated system providing accurate interpretation of system state.

Select EPC: T1

EPC Membership function: Very Low

EPC Specifications

T1. Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel.

Input Data

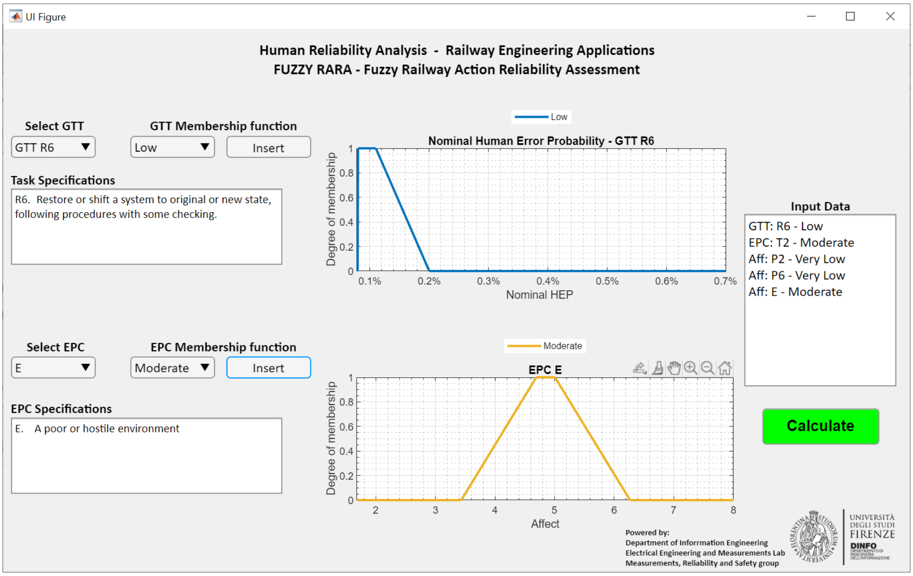
Powered by:
Department of Information Engineering
Electrical Engineering and Measurements Lab
Measurements, Reliability and Safety group

Fig. 5. 4- MATLAB Graphical User Interface developed to rapidly implement the proposed HRA approach. The screenshot represents the dialog box for data entry.

The bottom left panel of the software allows to select the EPC that affect the performances of the operator. It also allows to select the membership function using the linguistic variable that better describe the affect level of the selected EPC (Step 4). The bottom figure in the center of the tool illustrates the membership functions of the selected task within the proper domain D_{EPC_j}.

Step 4 could be repeated several times selecting different EPCs. The right panel in the developed tool resumes the selected task and the selected EPC with their relative membership functions.

Fig. 5.5 shows the data entry dialog box of the developed software after the selection of GTT and all EPCs. The top subplot in the box illustrates the selected membership function of the proper GTT (in this case task R6, membership function “Low”). The bottom subplot shows the last chosen EPC, while the complete list of EPC is reported in the right panel.



UI Figure

Human Reliability Analysis - Railway Engineering Applications

FUZZY RARA - Fuzzy Railway Action Reliability Assessment

Select GTT: GTT R6

GTT Membership function: Low

Insert

Task Specifications

R6. Restore or shift a system to original or new state, following procedures with some checking.

Select EPC: E

EPC Membership function: Moderate

Insert

EPC Specifications

E. A poor or hostile environment

Input Data

GTT: R6 - Low
EPC: T2 - Moderate
Aff: P2 - Very Low
Aff: P6 - Very Low
Aff: E - Moderate

Calculate

Powered by:
Department of Information Engineering
Electrical Engineering and Measurements Lab
Measurements, Reliability and Safety group

Fig. 5. 5- Screenshot of the proposed GUI after the selection of GTT and EPC. The input data are collected inside the right panel. The charts show the selected task and the last chosen EPC.

The following step (Step 5) consists in the evaluation of the fuzzy human error probability $\widehat{\text{HEP}}$ by means of fuzzy arithmetic. To perform fuzzy arithmetic operations, the α-cut theory has been taken into account.

Any fuzzy set can be described by specifying its α-cut. More in detail, a fuzzy set can be obtained as upper envelope of its α-cut, where the α-cut of a fuzzy set X is a crisp set X_α that contains all elements in the domain that have membership degree greater than or equal to α.

Considering two fuzzy sets X and Y described using the following trapezoidal membership functions $\mu_X(z)$ and $\mu_Y(z)$ respectively [317], [318]:

$$\mu_X(z) = \begin{cases} \dfrac{z - a_X}{b_X - a_X} & \text{if } a_X < z < b_X \\ 1 & \text{if } b_X \leq z < c_X \\ \dfrac{d_X - z}{d_X - c_X} & \text{if } c_X \leq z < d_X \\ 0 & \text{otherwise} \end{cases} \tag{5.10}$$

$$\mu_Y(z) = \begin{cases} \dfrac{z - a_Y}{b_Y - a_Y} & \text{if } a_Y < z < b_Y \\ 1 & \text{if } b_Y \leq z < c_Y \\ \dfrac{d_Y - z}{d_Y - c_Y} & \text{if } c_Y < z < d_Y \\ 0 & \text{otherwise} \end{cases} \tag{5.11}$$

Then the α-cut of the fuzzy set X and Y are given by [319], [320]:

$$X_\alpha = [X_{\alpha-L}, X_{\alpha-R}] \tag{5.12}$$

$$X_\alpha = \left[a_X + \alpha^{1/n}(b_X - a_X), d_X - \alpha^{1/n}(d_X - c_X)\right] \tag{5.13}$$

$$Y_\alpha = [Y_{\alpha-L}, Y_{\alpha-R}] \tag{5.14}$$

$$Y_\alpha = \left[a_Y + \alpha^{1/n}(b_Y - a_Y), d_Y - \alpha^{1/n}(d_Y - c_Y)\right] \tag{5.15}$$

The multiplication of two fuzzy set could be achieved using interval arithmetic, as follow [321]–[323]:

$$T_\alpha = X_\alpha \odot Y_\alpha = [T_{\alpha-L}, T_{\alpha-R}] \tag{5.16}$$

$$\begin{aligned} T_{\alpha-L} = \mathit{min}(&X_{\alpha-L} \cdot Y_{\alpha-L},\ X_{\alpha-L} \cdot Y_{\alpha-R}, \\ &X_{\alpha-R} \cdot Y_{\alpha-L},\ X_{\alpha-R} \cdot Y_{\alpha-R}) \end{aligned} \tag{5.17}$$

$$\begin{aligned} T_{\alpha-R} = \mathit{max}(&X_{\alpha-L} \cdot Y_{\alpha-L},\ X_{\alpha-L} \cdot Y_{\alpha-R}, \\ &X_{\alpha-R} \cdot Y_{\alpha-L},\ X_{\alpha-R} \cdot Y_{\alpha-R}) \end{aligned} \tag{5.18}$$

Where the operator ⊙ is the multiplication between two fuzzy sets performed by means of α-cut and interval arithmetic.

Finally, according to [319] the membership function $\mu_T(z)$ of the fuzzy set $T_\alpha = [T_{\alpha-L}, T_{\alpha-R}]$ achieved after multiplication of two fuzzy sets is given by:

$$\mu_T(z) = \begin{cases} f_1(z) & \text{if } a_X a_Y < z < b_X b_Y \\ 1 & \text{if } b_X b_Y \leq z \leq c_X c_Y \\ f_2(z) & \text{if } c_X c_Y < z < d_X d_Y \\ 0 & \text{otherwise} \end{cases} \tag{5.19}$$

The functions $\mathrm{f}_1(z)$ and $\mathrm{f}_2(z)$ are not linear relationships as in Equation (5.10) or Equation (5.11). Instead, the effect of the multiplication by α-cut is the alteration of the trapezoid shape into semi-trapezoid shape where the linear increase and decrease from $\mu_T = 0$ to $\mu_T = 1$ and vice versa become a square root function.

The above-mentioned theory of fuzzy multiplication has been used to evaluate the fuzzy human error probability $\widetilde{\mathrm{HEP}}$ (Step 5). In particular, the latter is given by the product of the fuzzy membership function of the selected task $\widetilde{\mathrm{HEP}_{\mathrm{b}_1}}$ (selected during Step 3) with an overall weighting factor $\widetilde{\mathrm{W}}$. Thus, the fuzzy human error probability is given by:

$$\widetilde{\mathrm{HEP}} = \widetilde{HEP_b} \odot \widetilde{\mathrm{W}} \tag{5.20}$$

The weighting factor $\widetilde{\mathrm{W}}$ is a fuzzy set which takes into account every affect $\widetilde{\mathrm{A}_\mathrm{J}}$ selected during Step 4. The following equation is used to obtain this factor:

$$\widetilde{\mathrm{W}} = \widetilde{\mathrm{A}_1} \odot \widetilde{\mathrm{A}_2} \odot \ldots \odot \widetilde{\mathrm{A}_\mathrm{p}} = \prod_{j=1}^{p} \widetilde{\mathrm{A}_\mathrm{J}} \tag{5.21}$$

Where p is the number of selected EPC during the several repetition of Step 4. The product symbol $\prod$ in (5.21) represents the fuzzy product $\odot$ of a sequence of factors. Consequently, substituting Equation (5.21) into Equation (5.20) the fuzzy $\widetilde{\mathrm{HEP}}$ is given by:

$$\widetilde{\mathrm{HEP}} = \widetilde{HEP_b} \odot \prod_{j=1}^{p} \widetilde{\mathrm{A}_\mathrm{J}} \tag{5.22}$$

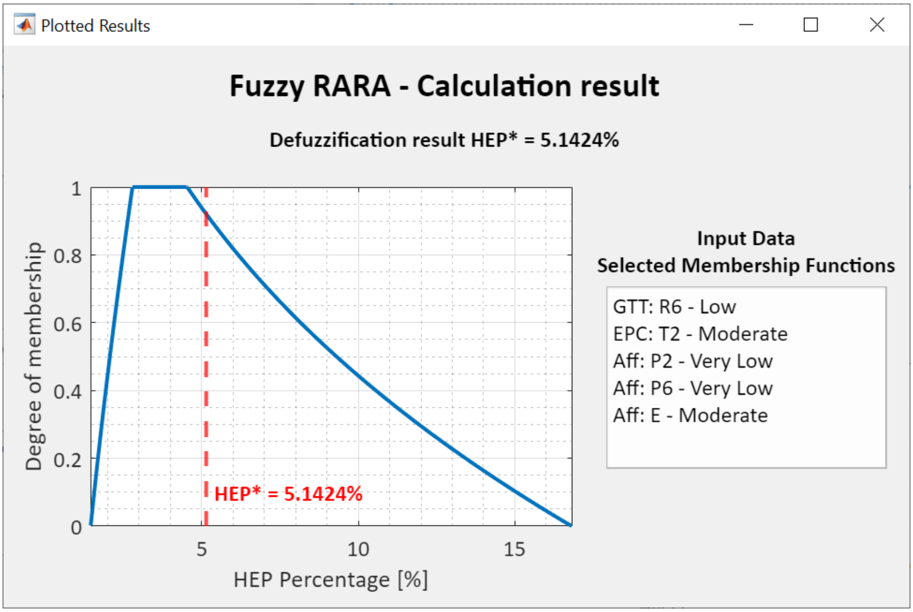
$\widetilde{\mathrm{HEP}}$ is the fuzzy human error probability described by the membership function $\mu_{HEP}(z)$.

Finally, Step 6 consists in the defuzzification of the obtained fuzzy human error probability using the centroid method. Starting from a fuzzy number and its corresponding membership function the defuzzification procedure is the process of generating a crisp logic value related to the starting fuzzy value. The centroid defuzzification is one of the most implemented defuzzification method in reliability engineering [23]. It returns HEP^* which is the center of gravity of the fuzzy number described by the membership function $\mu_{HEP}(z)$ as follow [36]:

$$\mathrm{HEP}^{*} = \frac{\int \mathrm{z} \cdot \mu_{HEP}(\mathrm{z})\,\mathrm{dz}}{\int \mu_{HEP}(\mathrm{z})\,\mathrm{dz}} \tag{5.23}$$

The developed tool automatically implements Step 5 and Step 6 after the selection of the base HEP and the affect value of the proper EPCs. The output box of the developed tool is illustrated in Fig. 5.6, where both fuzzy human error probability $\widetilde{\mathrm{HEP}}$ and defuzzified HEP^{*} are shown.

The developed software allows an easy and rapid implementation of the fuzzy-based approach. The analyst is able to perform the HEP assessment in a few simple steps without dealing with number estimation. The linguistic variables used in the tool allows to easily carry out the assessment in a way that is more suitable to human reasoning, decreasing subjectivity and possibility of error during the evaluation.



Defuzzification result HEP* = 5.1424%

Input Data
Selected Membership Functions

GTT: R6 - Low
EPC: T2 - Moderate
Aff: P2 - Very Low
Aff: P6 - Very Low
Aff: E - Moderate

Fig. 5. 6- Output box of the developed MATALB Graphical User Interface. The software provides the fuzzy HEP and the defuzzification result, along with a note with the selected membership functions used to evaluate the HEP.

Furthermore, this procedure allows to easily simulate different scenarios for the considered task changing the membership functions of the selected EPCs or simply introducing or removing one or more EPCs.

5.4 Validation of the proposed method

5.4.1 Human activities performed on ATP

Automatic Train Protection systems are reliable and safe equipment used to correct the train driver errors. Therefore, it is improbable that a driver error will lead to an accident if ATP are properly used. Consequently, the human activities significant for the safety of the railway systems mainly reside in the design, installation, verification and maintenance phases of the ATP itself. Table 5.2 includes the most critical human activities performed by specialized operator on the ATP under analysis.

Tab. 5. 2- Human Operations performed on the Ground unit of an Automatic Train Protection system.

OPERATION	DESCRIPTION
Balise Laying	It requires several operations: track ballast removal, positioning and fixing of the support, laying of the connection cable, and finally laying of the balise. Strict design requirements are required in term of tolerance of the installation angle and positioning of connection cable. A nearby metal-free zone is required.
Balise configuration	It is performed connecting the balise to a computer through a connection cable.
Maintenance	It requires several operations: fault detection, fault isolation, configuration of a new balise, replacement of the failed balise. Several measuring instruments are generally used.
Encoder wiring	It requires the correct connection of the cables to the encoder. It is a critical task since incorrect connection could lead to the transmission of incorrect information to the train.

These activities have been studied in the next subsections in order to estimate the human error probability of each operation in different scenarios.

5.4.2 Human error probability estimation

After the preliminary steps 1-2 automatically performed by the developed tool, step 3 of the proposed procedure consists in the selection of the proper task for the considered human operation. The four above-described human operations have been studied considering:

- Balise Laying: GTT R3 since it is a simple action performed following suitable well-defined procedures. The selected membership function is the lowest admissible “Very Low” since it is a standardized procedure carried out by well-trained operator.
- Balise Configuration: GTT R4 since it is a skill-based task performed by a well-trained operator. The operation is simple, but there is some possibility of confusion due to the programming of several identical balises. Therefore, the selected membership function is the lowest admissible “Low”.
- Maintenance: GTT R6 is the task of RARA specifically developed for maintenance actions following a procedure. The selected membership function is the lowest admissible “Low” since it is a standardized procedure carried out by experienced operator.
- Encoder wiring: GTT R3 since it is a simple action performed following suitable well-defined procedures. The selected membership function is “Low” which is a bit higher than the balise laying since it requires a higher mental involvement.

Once selected the GTT and its membership function, some scenarios of the external and internal conditions are proposed. In particular, for each one of the operation two different scenarios are taken into account:

1. Optimal case is the most likely situation.
2. Stressed and Fatigued when the operators are tired and stressed because of previous work or personal reasons.

Both scenarios consider the same EPCs as follow:

- T2: “a shortage of time available for error detection and correction”. To perform the operations on ATP, the railway line must have been blocked. Consequently, to minimize the railroad unavailability the operators have to work quickly.
- P2: “fatigue from shift and work patterns”. Represents the likelihood that operators are tired from the previous works.

- P6: “low workforce morale”. Consequence of the fatigue and stress from the work shift.
- E: “a poor or hostile environment”. These operations have to be performed outdoor on the track and generally at night, moreover sometimes the work locations are accessible only by walking. Therefore, to consider all these aspects, this EPC has been taken into account.

Some important EPCs which are usually taken into account during this kind of analysis has been neglected thanks to fundamental information provided by the company that manage operation and maintenance of the ATP under analysis. In particular, EPCs related to experience of the operator and perceived risk have been neglected since the operator that perform the task are experienced and well-trained regarding the risk of their work. Moreover, detailed documentation regarding the specific task is provided by the company to the operator allowing the analyst to neglect several others EPCs.

Table 5.3 summarizes all the scenarios considered. For the sake of representation, only the first letter of each linguistic variable has been used, namely VL=Very Low, L=Low, M=Moderate, H=High and VH=Very High.

The four operations are evaluated with the above EPCs and considering both stressed and non-stressed operators (Scenario 1. And 2. Respectively). The EPCs P2 and P6 related to stress and fatigue conditions have been set “Very Low” for all the tasks in the Optimal scenario, while have been set “Very High” for all the tasks in the second scenario. This option allows to easily quantify the effect of a stressed and fatigued operator on the human error probability. The environment-related EPC (E) has been set “Moderate” in case the operation has to be performed on the tracks (Balise laying and Maintenance), while it has a slightly minor effect (“Very Low”) in case the task is performed near the tracks (Balise configuration and Encoder wiring). Finally, the T2 EPC related to the available time has been set considering the average task duration of each operation.

Tab. 5. 3- Input data used to calculate the Human Error Probability of the four considered operations in two different scenarios.

Operation	**Selected Task**	**Scenario**	**EPC**			
			T2	**P2**	**P6**	**E**
Balise laying	GTT R3 "Very Low"	1. Optimal Case	M	VL	VL	M
		2. Stressed and Fatigued	M	VH	VH	M
Balise configuration	GTT R4 "Low"	1. Optimal Case	VL	VL	VL	L
		2. Stressed and Fatigued	VL	VH	VH	L
Maintenance	GTT R6 "Low"	1. Optimal Case	M	VL	VL	M
		2. Stressed and Fatigued	M	VH	VH	M
Encoder wiring	GTT R3 "Low"	1. Optimal Case	L	VL	VL	L
		2. Stressed and Fatigued	L	VH	VH	L

The results of the Human Error Probability assessment (Step 5 and Step 6) are illustrated in Fig. 5.7.

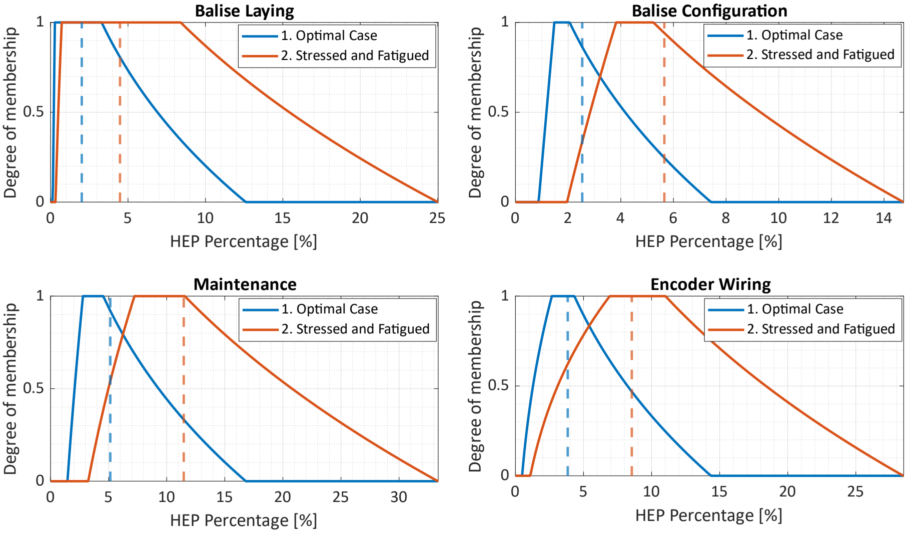


Fig. 5. 7- Results of the proposed approach. Fuzzy Human Error Probability and Defuzzified HEP in two different scenarios (Optimal case in blue and Stressed and Fatigued in red). Each plot illustrates the results of a different activity.

Each subplot shows fuzzy human error probability $\widetilde{\mathrm{HEP}}$ (continuous trend) and defuzzified HEP^* (vertical dotted line) of a single task in both the considered scenarios. The Optimal case is illustrated using blue lines, while the red color stands for the Stressed and Fatigued scenario. Analyzing Fig. 5.7 is clear that the P2 and P6 EPCs related to the stress and fatigue condition of the operator deeply affect the human performances. Both fuzzy $\widetilde{\mathsf{HEP}}$ and defuzzified value HEP^* shows a remarkable increase when the second scenario is taken into account. That remarks the importance of stress management to ensure a low error probability. Furthermore, companies should develop the working shift and the maintenance operation taking into account the negative effect of fatigue and long consecutive shifts. In order to better compare the results of the proposed approach, Fig. 5.8 illustrates a bar chart of the defuzzified HEP^*. Each set of bar stands for a different operation. The optimal case is illustrated using blue bars, while the red bars stand for the Stressed and Fatigued scenario. What stands out from the figure is that the Maintenance Operation is the most challenging task for the ATP under analysis in both the analyzed scenarios. This is mainly due to the fact that the maintenance operation requires a sequence of different activities involving fault diagnosis, control and verification. Another critical task is the encoder wiring which provides the second highest HEP^* due to the high number of cables to be connected. Balise laying and balise configuration result to be less critical and challenging, with a lower human error probability.

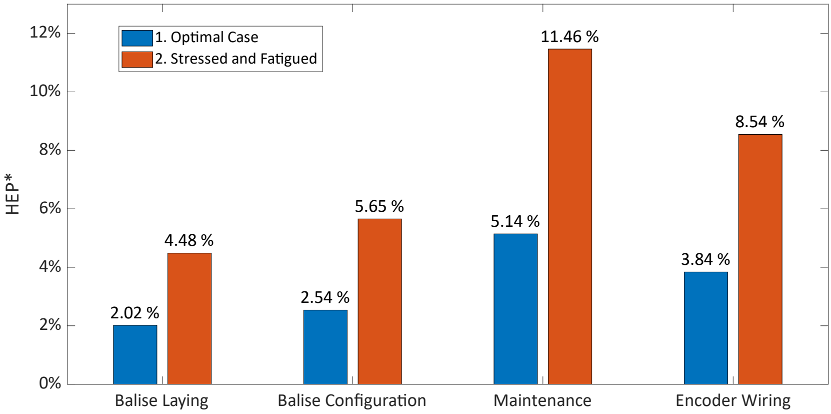


Fig. 5. 8- Bar chart of the defuzzified HEP obtained using the proposed approach considering four different tasks and two simulation scenarios (1. Optimal case using blue and 2. Stressed and Fatigued using red).*

5.4.3 Comparison with the classical RARA approach

In order to test and validate the effectiveness of the fuzzy-based proposed approach the results of the previous analysis are compared with a human error probability estimation achieved using the RARA method.

Table 5.4 summarizes the input data required by the RARA method for each one of the considered tasks.

Tab. 5. 4- Input Data used to calculate the Human Error Probability using the RARA method

Operation	**Scenario**	**Parameters**	**EPC**			
			T2	**P2**	**P6**	**E**
Balise laying GTT R3 HEP_{nom}=0.05%	1. Optimal Case	MA	11	2.6	1.2	8
		APOA	0.6	0.1	0.1	0.6
		Affect	7	1.16	1.02	5.2
	2. Stressed and Fatigued	MA	11	2.6	1.2	8
		APOA	0.6	0.9	0.9	0.6
		Affect	7	2.44	1.18	5.2
Balise configuration GTT R4 HEP_{nom}=0.2%	1. Optimal Case	MA	11	2.6	1.2	8
		APOA	0.2	0.1	0.1	0.3
		Affect	3	1.16	1.02	3.1
	2. Stressed and Fatigued	MA	11	2.6	1.2	8
		APOA	0.2	0.9	0.9	0.3
		Affect	3	2.44	1.18	3.1
Maintenance GTT R6 HEP_{nom}=0.11%	1. Optimal Case	MA	11	2.6	1.2	8
		APOA	0.6	0.1	0.1	0.6
		Affect	7	1.16	1.02	5.2
	2. Stressed and Fatigued	MA	11	2.6	1.2	8
		APOA	0.5	0.9	0.9	0.6
		Affect	7	2.44	1.18	5.2
Encoder wiring GTT R3 HEP_{nom}=0.1%	1. Optimal Case	MA	11	2.6	1.2	8
		APOA	0.4	0.1	0.1	0.4
		Affect	5	1.16	1.02	3.8
	2. Stressed and Fatigued	MA	11	2.6	1.2	8
		APOA	0.4	0.9	0.9	0.4
		Affect	5	2.44	1.18	3.8

For the sake of comparison, the GTT and the EPCs selected in the RARA assessment are the same one used in the proposed approach. The nominal HEP of each task has been selected within the range of the admissible value provided by RARA following the guidelines of the company that manage operation and maintenance of the ATP under analysis. The APOA value of each EPC has been assessed following the same considerations of the previous analysis. Each Affect is calculated using Equation (4.1), while the resulting HEP is evaluated with Equation (4.3).

The results of the comparison of RARA and proposed fuzzy-based approach is shown in Table 5.5, where the HEP of the four operation is reported considering both scenarios. The difference between the Human Error Probability provided by RARA (literature comparison) and proposed approach is negligible leading to comparable results of all the studied operations. Therefore, the proposed approach is validated by the comparison with the widest used technique in railway engineering.

Tab. 5. 5- Comparison between Classical RARA method and Proposed Fuzzy-based Approach.

OPERATION	1. OPTIMAL CASE		2. STRESSED AND FATIGUED	
	PROPOSED APPROACH	LITERATURE (RARA)	PROPOSED APPROACH	LITERATURE (RARA)
Balise Laying	2.0153%	2.1534%	4.4833%	5.2401%
Balise Configuration	2.5365%	2.2008%	5.6543%	5.3553%
Maintenance	5.1424%	4.7375%	11.4646%	11.5283%
Encoder Wiring	3.8386%	2.2481%	8.5443%	5.4705%

The proposed algorithm allows to achieve results fully comparable with the RARA model available in literature with a simpler, less complex and more intuitive approach. The main advantages of the proposed fuzzy-based method respect to the HRA literature in railway field are the following:

- The proposed approach provides a range of possible HEP with different degree of membership. This is a fundamental skill since HRA is not an exact science and therefore is not recommended to consider a crisp HEP value.
- Fuzzy logic is the most suitable approach in case of incomplete and

uncertain data. In fact, data regarding human error in railway are not always available, especially in case of near miss.

- Comparing the required input data for the proposed approach and the RARA method is extremely evident how the parameter assessment is easier using the proposed approach. In fact, the use of linguistic variables to assess the input data is closer to human intuition than numbers assessment.
- Fuzzy minimizes subjectivity of the assessment as well as it accurately balances the tradeoff between precision and significance.

5.5 Final remarks

Human errors are one of the primary causes of accidents in railway. Despite several different techniques are available to study human reliability, Railway Action Reliability Assessment (RARA) is the only method specifically developed for railway industry. In this paper an innovative fuzzy-based approach has been presented to evaluate the human error probability in railway engineering. The database of RARA has been used as a starting point for the proposed procedure. Then, fuzzy logic has been implemented to overcome the subjectivity of the assessment and to deal with the uncertain data that characterize human reliability analysis. The α-cut theory and fuzzy interval arithmetic are used to calculate the human error probability.

To test and validate the performances of the proposed approach, the procedure has been applied to four human operations performed on an automatic train protection system. The method shows full compatibility of the results provided by literature, without necessity to select number and values during the assessment. Therefore, this procedure could be performed also by non-expert analysts with minimum subjectivity.

Chapter 6

Dynamic HRA: An innovative approach for railway industry

This chapter introduces an innovative third generation HRA technique for the assessment of the human error probability. Third generation techniques are not developed in railway field therefore the proposed E-SHERPA has been specifically designed for this type of application taking into account operational tasks dedicated to railway operators. Furthermore, other significant contributions of the proposed method are the ability to take into account a time-dependent model, the ability to introduce one or more breaks during the time-shift and the introduction of the Yerkes-Dodson law used to model the Eustress concept (i.e. beneficial level of stress).

[1] The proposed HRA method has been published as "M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, "An enhanced SHERPA (E-SHERPA) method for human reliability analysis in railway engineering, *Reliab. Eng. Syst. Saf.*, vol. 215, p. 107866, Nov. 2021".

6.1. Second proposed method: Enhanced-SHERPA (E-SHERPA)

There are several techniques to evaluate the human error probability. Each technique is classified into one of three different generations, based on its characteristic. The first-generation techniques are milestones, they consider a human being the same as a component which is only capable to succeed or fail. Despite their obsolescence they are still in use in many fields of application. The second generation represents the evolution of the previous one and focuses on the contribution of cognitive action in an accident situation, by considering the role of the context. Finally, the third generation focuses on the dynamic relationship and dependence between the factors which affect the human performances.

Even if there are several HRA (Human Reliability Analysis) techniques only few procedures for human error analysis specifically developed and customized on railway engineering are available. The most implemented method is a first generation technique developed by Rail Safety and Standards Board in 2012 known as Railway Action Reliability Assessment (RARA) [236]. This technique provides positive results in terms of human error probability, but it does not simulate different scenarios as well as it does not take into account a time-dependent behavior of the operator. Furthermore, most of the third-generation techniques available in literature focuses on nuclear applications [168], [169] (except for a method developed for avionics field) leaving a critical sector such the railway engineering completely unstudied by the most accurate, innovative, leading-edge third-generation techniques.

Therefore, the aim of this chapter is to develop an innovative method for human reliability analysis in railway engineering integrating the error probability of the RARA technique into a SHERPA-based time-dependent model (SHERPA is the acronym of Simulator for Human Error Probability Analysis). The Weibull probability density function is used to simulate the time-dependent model of the human error probability during the work shift. The main contributions of this chapter are the following:

- Introduction of the first third-generation HRA technique specifically developed and customized on railway engineering integrating the task provided by RARA within a SHERPA-based simulator.
- Accurate and detailed proof of the identification of the optimal Weibull parameter that best describe the human behavior.

- Time-dependent model of the human error probability varying during the work shift which takes into account the fatigue cumulated during the shift by the operator and the beneficial effects of a break on the probability of committing an error. Both coffee break and lunch break are considered within the proposed method.
- Introduction of the Yerkes–Dodson curve describing the relationship between stress and performances in case of a difficult task. The Eustress concept (beneficial stress which increases the performance of the operator) is taken into account within the proposed procedure to model the performance shaping factor accordingly.

The proposed method is called Enhanced SHERPA (E-SHERPA) because it starts from the structure and the main findings of the SHERPA method [168]. The novelties introduced in the approach regard the introduction of some factors and parameters to improve the estimation and to ensure the correct application to railway industry. The E-SHERPA is characterized by four main points which corresponds to the main extension and contribution respect to the regular SHERPA [168]:

A. According to the regular SHERPA the nominal HEP follows a time-dependent trend described by Weibull distribution. The proposed technique introduces the use of the Generic Task Type specifically designed for the railway industry to simulate the human behavior in compliance with the RARA model.
B. The PSF of the SPAR-H technique are implemented to shape the human error probability based on internal and external factor. The result of this operation is called Contextual HEP.
C. The contextual HEP is modified introducing the concept of Eustress described by the Yerkes-Dodson law.
D. The simulation provides the possibility of considering one or more breaks in the work shift. This final step allows to simulate the HEP based on the duration of the break.

6.2. Structure of the proposed E-SHERPA

6.2.1 Nominal HEP

The first step of the E-SHERPA is the evaluation of the nominal HEP. RARA suggests classifying the human operation in railway engineering according to a set of eight generic task types. RARA provides a generic description of a task and a bound of the human error probability for each generic task type. To estimate the nominal HEP, the first step that should be performed is the selection of the GTT which best matches the studied task.

The Skill, Rule and Knowledge (SRK) based classification developed by J. Rasmussen [174] has been used to group the GTTs as follow:

- "More automated and skill-based processes" includes operations that requires little conscious effort, such as simple and/or well learnt tasks.
- "More effortful and rule-based processes" includes the operations that require more mental involvement. At the same time, usually operators are trained so that they can apply previously learned rules when implementing this kind of task.
- "Thinking outside procedures" includes all the operations that require considerable mental involvement because of an unusual situation is occurred. This group is characterized by a high HEP values because dealing with novel or unusual situations is considered the most probable cause of accidents.

Table 4.5 shows the eight GTTs grouped into three categories and the respectively HEP bounds. The HEP data included in Table 4.5 are in compliance with RARA approach [236]. In the proposed method the RARA dataset has been used since no other sources regarding human errors in railway field are currently available. $HEP_{n,min}$ represents the minimum value of the n-th GTT, while $HEP_{n,max}$ stands for the maximum value of the n-th GTT. In particular the eight possible GTTs included in the proposed E-SHERPA are the following:

R1. Respond correctly to system command even when there is an automated system providing accurate interpretation of system state.

R2. Completely familiar, well designed, highly practiced task which is routine.

R3. Simple response to a dedicated alarm and execution of actions covered in procedures.

R4. Skill-based tasks (manual, visual or communication) when there is some opportunity for confusion.

R5. Fairly simple task performed rapidly or given insufficient or inadequate attention.

R6. Restore or shift a system to original or new state, following procedures with some checking.

R7. Identification of situation requiring interpretation of alarm/ indication patterns.

R8. Complex task requiring a high level of understanding and skill.

Di Pasquale et al. [168] demonstrates that Weibull function is the best approximation of the human performances. The Weibull probability density function $f_{weib}(t)$ is described by the following equation [324], [325]:

$$f_{weib}(t) = \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \tag{6.1}$$

Where α is called scale parameter and β is called shape parameter. The Weibull cumulative distribution function $F_{weib}(t)$ is given by [324], [325]:

$$F_{weib}(t) = \int_0^t f_{weib}(u)\,du = 1 - e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \tag{6.2}$$

In reliability field, the cumulative distribution function $F_{weib}(t)$ represents the unreliability, which is the probability of committing an error. Thus, in HRA $F_{weib}(t)$ stands for the human error probability.

$$HEP_{nom}(t) \; = \; F_{weib}(t) = 1 - e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \tag{6.3}$$

However, as pointed out in [168], the classical Weibull distribution needs some modifications to best fit the human work-shift behavior. In fact, the classical Weibull error probability increases with time and has a minimum at time t=0 [325]. In other words, Weibull distribution considers the minimum level of HEP (and consequently the maximum human reliability) at the initial time of the work shift. Despite this, according to [168], the natural behavior and performance of an operator is a bit different. Humans are characterized by a natural process of adaptation to a given operation. This results in a higher error probability in the initial part of the shift. In this transient phase the human error probability decreases to reach the minimum value in the first hour of processing. Consequently, the Weibull function needs to be adjusted to these requirements (a HEP trend that first decreases reaching the minimum at the first hour and then start increasing).

Considering the probability bound included in table 4.5 it is possible to associate a Weibull function to each one of the GTT, as follow:

$$HEP_{nom}(t) = \begin{cases} 1 - k \cdot e^{-\alpha \cdot (1-t)^{\beta}} & \forall t \in [0; 1] \\ 1 - k \cdot e^{-\alpha \cdot (t-1)^{\beta}} & \forall t \in (1; t_{max}) \end{cases} \tag{6.4}$$

Where:

- $HEP_{nom}(t)$ is the nominal time-dependent human error probability.
- k is set to obtain a distribution with minimum value of HEP after 1 working hour.
- α is the scale parameter of the Weibull distribution. It is set to obtain a distribution with maximum value of HEP at the end of the working shift ($t = t_{max}$).
- β is the shape parameter of the Weibull distribution. According to [168] the optimal solution is β=1.5.

Eq. (6.4) has been validated in [168] in order to update the model of the classical Weibull distribution to best fit the dynamic performances of a human operator. In fact, using eq. (6.4) the human error probability starts decreasing until it reaches the minimum value after 1 working hour to consider the human process of adaptation described above. Moreover, according to eq. (6.4) the HEP starts increasing after 1 h until it reaches the maximum value at the end of the working shift. This situation is the more plausible one due to the cumulative fatigue along the working shift. Furthermore, the attention of the operator tends to decrease approaching the end of the working shift, proving once more why the worst condition is obtained at the end of the shift.

Table 6.1 illustrates the k, α and β values for all the GTT calculated according to the proof included in Annex A.

Fig. 6.1 shows all the nominal HEP trends obtained using (6.1) and Table 6.1 for all the GTTs.

Tab. 6. 1–Generic Task Type and corresponding parameter values evaluated as proof included in Annex A

GTT	k	α	β
R1	0.999994	0.00004829	1.5
R2	0.99992	0.0003750	1.5
R3	0.99992	0.0003750	1.5
R4	0.998	0.0001083	1.5
R5	0.94	0.0041785	1.5
R6	0.9992	0.0003361	1.5
R7	0.98	0.0089700	1.5
R8	0.88	0.01083520	1.5

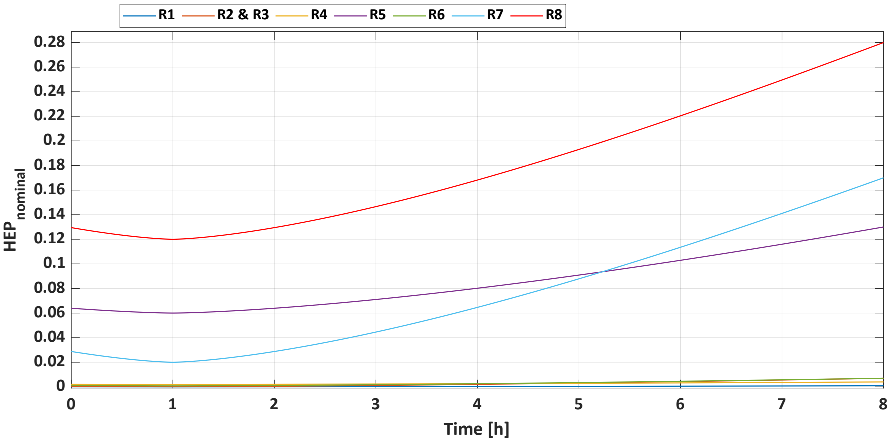


Fig. 6. 1-Nominal HEP calculated as a Weibull function using equation (6.1) for each of the GTT.

The greatest error probability is represented by the HEP of the task R8. Also, tasks R5 and R7 are characterized by high error probabilities. Quite the opposite, R1, R2, R3, R4 and R6 are characterized by lower value of HEP and thus the trend is not completely visible in the scale used in fig.6.1.

The time indicated in Fig. 6.1 represents the work shift of the operator under analysis. Thus, only a time interval of 8 h has been considered since it is the usual time duration of most works. However, it is not always ensured a work shift of 8 h. For this reason, the time variable t in eq. (6.4) could assume values from 0 to t_{max}, where t_{max} is a generic variable which is not necessarily equal to 8 h. As a matter of fact, in case of extended work shift longer than 8 h, the trends of the nominal HEP in Fig. 6.1 continues to increase following the model in eq. (6.4). Consequently, extended work shifts could lead to higher human error probabilities.

6.2.2 Contextual HEP

The contextual HEP is an extension of the nominal HEP which represents the human error probability updated using the factors that improves or decreases human performances.

In compliance with SHERPA method, the proposed E-SHERPA uses the Performance Shaping Factor (PSF) of the SPAR-H method. The benefits of this choice are manifold:

- It provides a reasonable number of PSF.
- It is easy to implement, and it contains PSF which are realistic in railway engineering.
- It is one of the few HRA methods that includes PSF that influence the human performance both positively (corresponding to a PSF value less than one) and negatively (corresponding to a PSF value higher than one).

SPAR-H considers eight PSFs, namely: available time, stress, complexity, experience and training, procedures, ergonomics, fitness for duty and work process.

The impact of the context is assessed using the following equation:

$$HEP_{cont}(t) = \frac{HEP_{nom} \cdot \prod_{i=1}^{m} PSF_i}{HEP_{nom} \cdot (\prod_{i=1}^{m} PSF_i - 1) + 1} \tag{6.5}$$

Where $HEP_{cont}(t)$ is the time-dependent contextual HEP, and m is the number of selected PSF ($1 \leq m \leq 8$).

SPAR-H provides a guide for the selection of the correct multiplier of the PSF; all the values are reported in Table 6.2 and Table 6.3.

Tab. 6. 2–PSFs of the proposed method and corresponding multiplier value. Part A. Source [189].

SPAR-H PSF	**Ref**	**PSF level**	**Multiplier**
Available time	A1	Inadequate time	P(failure)=1
	A2	Time available=time required	10
	A3	Nominal time	1
	A4	Time available > 5x time required	0.1
	A5	Time available > 50x time required	0.01
	A6	Insufficient information	1
Stress	S1	Extreme	5
	S2	High	2
	S3	Nominal	1
	S4	Insufficient information	1
Complexity	C1	Highly complex	5
	C2	Moderately complex	2
	C3	Nominal	1
	C4	Insufficient Information	1
Experience training	E1	Low	3
	E2	Nominal	1
	E3	High	0.5
	E4	Insufficient information	1
Procedures	PR1	Not available	50
	PR2	Incomplete	20
	PR3	Available, but poor	5
	PR4	Nominal	1
	PR5	Insufficient information	1

Tab. 6. 3– PSFs of the proposed method and corresponding multiplier value. Part B. Source [189].

SPAR-H PSF	**Ref**	**PSF level**	**Multiplier**
Ergonomics	ER1	Missing/misleading	50
	ER2	Poor	10
	ER3	Nominal	1
	ER4	Good	0.5
	ER5	Insufficient information	1
Fitness for duty	P1	Unfit	P(failure)=1
	P2	Degraded fitness	5
	P3	Nominal	1
	P4	Insufficient information	1
Work processes	W1	Poor	5
	W2	Nominal	1
	W3	Good	0.5
	W4	Insufficient information	1

A brief note regarding the Performance Shaping Factor “A1- Available Time” included in Table 3 is required. The PSF available time is intended to evaluate the effect of insufficient time to perform a task. Therefore, the PSF A1 is not related to the time variable in Eq. (6.4) and Fig. (6.1).

As a matter of fact, the time variable in Eq (6.4) represents the duration of the working shift. The available time in PSF A1 represents the amount of time that the operator has available to perform a specific task, while the required time is a reasonable amount of time required to finish the task in standard conditions. During the work shift the operator could carry out one or more task, depending on the work plan. Many times, in railway-related operations, the operator has to perform the task as quick as possible to minimize the downtime of the rail network. The greater the available time, the lower the error probability. Therefore, the A1 PSF models this effect in order to obtain a reliable HEP estimation.

According to SPAR-H [189] the use of PSF lower than 1 characterized by a positive impact on the human performance is essential to address the potential beneficial influence of the context. For example, if the operator is highly experienced, SPAR-H gives the opportunity to select the PSF E3 which is characterized by a multiplier of 0.5 leading to a positive impact on the nominal HEP regardless the selected task. Quite same considerations could be given if the available time to perform the task is greater than the required time. Both PSF A4 and A5 could be selected, and both of them have a positive impact on the nominal HEP since the operator has a lot of time to perform the task and to ensure that he has not make any mistakes.

6.2.3 Application of the Yerkes-Dodson Law to Stress PSF

One of the most interesting PSF is the stress. Several works in literature show the stress' effects on attentional processes. Psychological stress along with various forms of workload tend to tunnel attention, reducing focus on peripheral information and tasks and centralizing focus on main tasks. Hans Salye firstly introduced the term Eustress which means good/beneficial stress. Eustress stands for the positive cognitive response to a proper amount of stress [326], [327]. Yerkes and Dodson in [328], introduced a law of human performance which include the concept of Eustress along with the classical stress (distress).

According to the Yerkes-Dodson law (Y-D law), increasing the stress level the human performances progressively increase up to an optimal point. Beyond this point any further increases in stress produce a gradual decline in performances. In other words, if the psycho-physical activation is too low, the operator could undertake the task with an excessively relaxed approach. Quite the opposite, if the stress level is too high, the operator could perform the operations in a state of excessive and uncontrolled excitement, thus its behavior will probably be fraught, chaotic and fruitless. The model is described by the stress-performance curve shown in Fig. 6.2.

The Stress PSF of the classical SPAR-H included in Table 6.2 considers the reduction of human performances only in case of increase of the stress level. However, Y-D law shows the importance of taking into account also a low level of stress since it can seriously lead to an excessively relaxed behavior of the operator (that could be dangerous). Therefore, the Stress PSF has been updated considering the effect of low-level stress and the beneficial stress (Eustress).

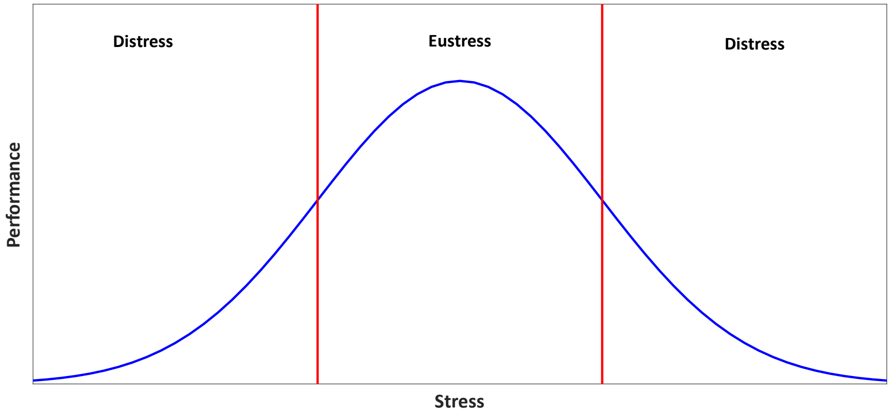


Fig. 6. 2 - Yerkes-Dodson model describing the relationship between performance and stress. The intermediate part is the Eustress or beneficial stress.

Fig. 6.3 compare the Y-D stress-performance law with the updated PSF multipliers, while Table 6.4 summarizes the multiplier of the updated Stress PSF integrating the concept of beneficial stress introduced by the Yerkes-Dodson law. The optimal stress level (S4) is characterized by a PSF value lower than 1, which decreases the HEP. That represents the introduction of the Eustress inside the model of the SPAR-H Stress PSF. The "Extremely Low" and "Low" PSF level have been introduced to model also the first section of the Y-D law.

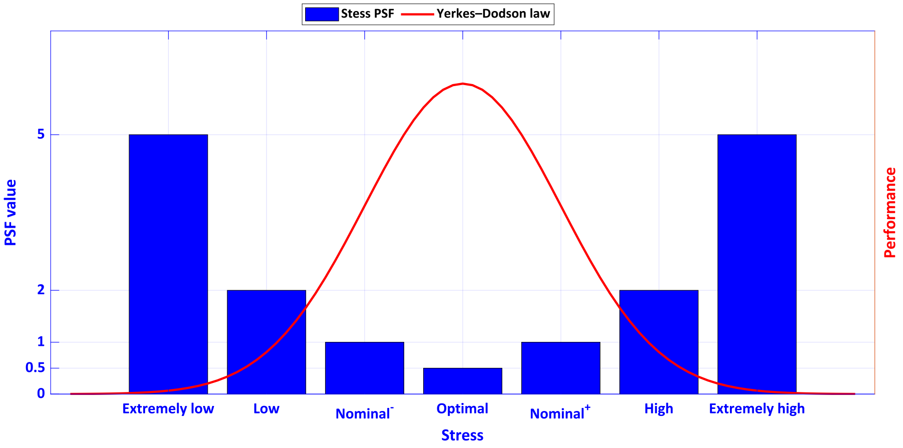


Fig. 6. 3 Multiplier of the stress PSF considering the Y-D law. The PSF levels (blue bars) are compared to the Y-D stress-performance curve.

Tab. 6. 4– Performance Shaping Factors related to Stress factor integrating Yerkes-Dodson law

PSF	Ref	PSF level	Multiplier
Stress including Y-D law	S1	Extremely high	5
	S2	High	2
	S3	Nominal^{+}	1
	S4	Optimal	0.5
	S5	Nominal^{-}	1
	S6	Low	2
	S7	Extremely low	5

To understand the implication of the Y-D law in railway-related field many technical papers and reports have been analyzed. The documents have been provided by a rail transport system manufacturer which also manages installation, operation and maintenance of railway systems. According to these papers, most of the time the human operations have to be performed at night on railroad tracks. Sometimes, the specific point of the tracks is accessible only by foot passing through mountains and woods. Other times the operator has to work adjacent to operative railroad tracks with nearby moving trains. Other times the operators have a really limited amount of time to perform the task.

All these situations influence the amount of stress that the operator has to face performing the task.

Fortunately, it is extremely improbable that more than one of the above-mentioned scenarios affect the operator in a single work shift. As a matter of fact, considering the average installation or maintenance operation performed at night on items mounted nearby railroad tracks, the amount of stress due to an operation performed at night is well described by the “S4 - Optimal” condition. According to these documents, performing the operation at night gives the right amount of stress to the operator which will be able to work at his/her optimal performances. However, if other stress sources (such as difficult to access the place, or the presence of nearby moving trains) add up, then it is likely that this high amount of stress level will produce a decrease of the operator performances. This scenario is well-described by the PSF “S3 - Nominal^{+}”, “S2 - High” or “S1 Extremely high”. Quite the opposite, if an operator is used to work in such stressful environments, when the task is performed daytime, without moving trains around and in absence of any other stress sources, then it is probable that the operator will undertake the task with an excessively relaxed approach, leading to a performance decrease. Using the Y-D law, this scenario could be described using the PSF “S5 - Nominal^{-}”, “S6 - Low” or “S7 Extremely low”.

The proposed E-SHERPA method assesses the Stress PSF using Table 6.4, while the other PSFs should be evaluated using Table 6.2.

Taking into account all the PSFs, the contextual HEP (which is also a time-dependent curve) is calculated using eq. (6.5). An example of the trend of this probability is illustrated in Fig.6.4, where the GTT R6 is implemented. It is possible to note how the trend varies with the choice of the PSFs and over time. For all the PSF value it is possible to note that the shape of the Weibull function is still present with a minimum for t = 1 h and then the HEP increases with time.

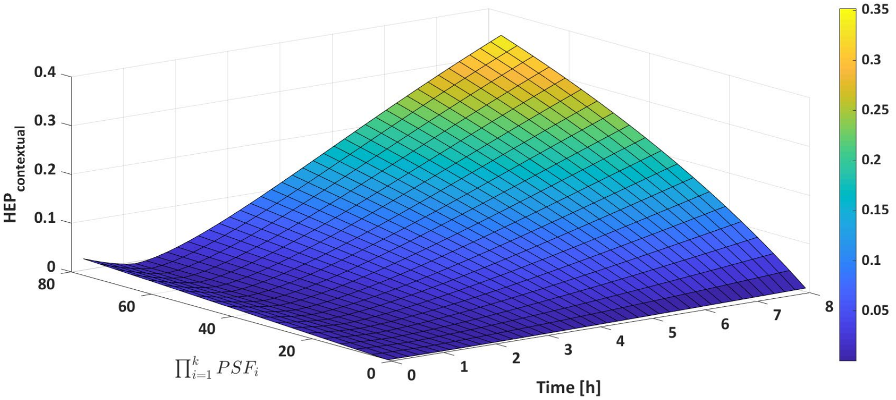


Fig. 6. 4 - 3-D trend of the contextual HEP of GTT R6 varying the working time and the PSF effects. Y-D law is included.

6.2.4 Introduction of breaks

The model proposed in the classical SHERPA does not take into account a reduction of the likelihood of error after a break, as most of the paper in literature. Despite this, it is not reasonable to simulate the HEP without introducing a performance improvement due to the break. As a matter of fact, in case no breaks are considered (or equivalently in case the beneficial effects of breaks are not considered) the following relationship is satisfied:

$$HEP_{nom}(t_{max}) = HEP_{n,max} \tag{6.6}$$

Where, as previously stated, $HEP_{n,max}$ represents the maximum value of the n-th GTT.

However, the introduction of break ensures a stress reduction and consequently it should lead to a reduction of the nominal HEP as follow:

$$HEP_{nom}(t_{max}) < HEP_{n,max} \tag{6.7}$$

In fact, the fatigue cumulated by the operator during the work shift is partially compensated by the rest and the relax time during the break. It is reasonable to assume that during a break the operator rests and thus his/her performances will increase. As a consequence, the probability of committing an error should decrease during the break before starting increase again when the shift begins.

Therefore, the central point of the proposed E-SHERPA is the introduction of one or more breaks within the 8 hours classical work shift in order to provide a more reliable simulation. The base idea is to maintain unchanged the Weibull parameters k, α and β in Table 6.1. This is due to the fact that these parameters are strictly correlated to the operator task, but they are not linked to the working hours or to the presence of breaks.

Supposing the presence of one break within the shift, the E-SHERPA nominal HEP is composed by three functions:

- A function $f_1(t)$ which describes the first part of the curve (before the break). It is the same function used to evaluate the nominal HEP in the classical SHERPA.
- A function $f_{br}(t)$ which describes the human behavior during the break. In this section, the nominal HEP decreases over time since the operator rest during the break. However, in compliance with the Y-D law, if the break is too long (e.g. over 1 h) then the behavior of the operator could be extremely relaxed leading to a decrease in performances. For these reasons, the function $f_{br}(t)$ has the same parameters of $f_1(t)$. The only differences are a time shifting and a probability increase Δ_1 set to guarantee a continuous function.
- A function $f_2(t)$ which describes the human error probability after the break. In this case, it is no more reasonable to assume a double

Weibull distribution as the one in eq. (4) used to describe $f_1(t)$. Since the natural process of human adaptation to a given operation has already taken into account, in this time slot the error probability should start increasing until it reaches the maximum value (worst condition) at the end of the shift due to the cumulated fatigue. Obviously, the function must take into account also the fatigue of the operator after the first hours of work. Thus, $f_2(t)$ is characterized by a time shifting and a probability increase Δ_2 set to guarantee a continuous function.

The mathematical model of the proposed nominal HEP is the following:

$$HEP_{nom}(t) = \begin{cases} f_1(t) & 0 \leq t \leq t_1 \\ f_{br}(t) & t_1 < t \leq t_2 \\ f_2(t) & t_2 < t \leq t_{max} \end{cases} \tag{6.8}$$

Where t_1 is the initial time of the break, $t_2$represents the end of the break and t_{max} stands for the end of the working shift. An example of nominal HEP evaluated using the proposed E-SHERPA model is illustrated in Fig. 6.5 (task GTT R8 is involved).

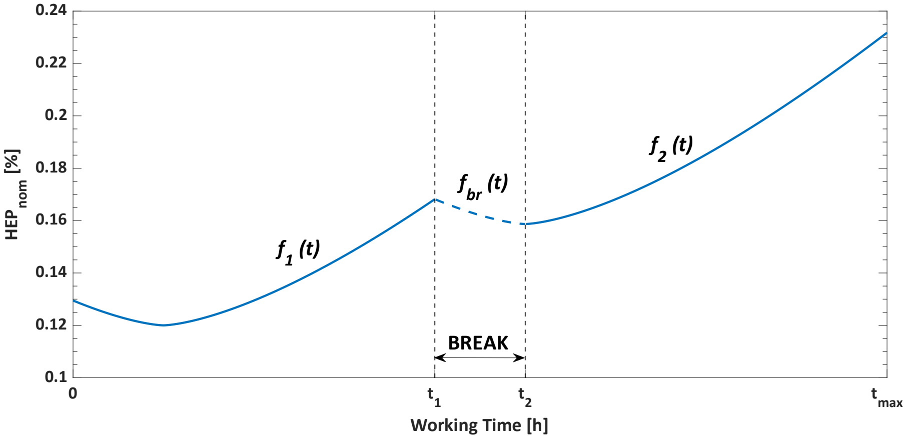


Fig. 6. 5 - Nominal HEP of the proposed E-SHERPA including a break in the middle of the working shift.

More in detail, before the break, the nominal HEP is described by the function $f_1(t)$ as follow:

$$f_1(t) = \begin{cases} 1 - k \cdot e^{-\alpha \cdot (1-t)^{\beta}} & 0 \leq t \leq 1 \\ 1 - k \cdot e^{-\alpha \cdot (t-1)^{\beta}} & 1 < t \leq t_1 \end{cases} \tag{6.9}$$

The function $f_{br}(t)$ could assume different models depending on the length of the break. The base idea is to use the modified Weibull distribution in eq. (6.4) with some small adaptation due to the initial time shifting and the necessity to ensure a continuous function. Therefore, in case the break duration is shorter than 1 hour, then $f_{br}(t)$ is described using only one Weibull function, as follow:

$$f_{br}(t) = \Delta_1 + 1 - k \cdot e^{-\alpha \cdot [1-(t-t_1)]^{\beta}} \qquad t_1 < t \leq t_2 \tag{6.10}$$

Instead, in case the break duration overcomes 1 hour long, then the Y-D law requires to modify eq. (6.10). In fact, too long breaks could lead to an excessively relaxed approach with a decrease of the operator performance and a consequent increase of the error probability. Thus, two modified Weibull functions are needed to model the HEP trend:

$$f_{br}(t) = \begin{cases} \Delta_1 + 1 - k \cdot e^{-\alpha \cdot [1-(t-t_1)]^{\beta}} & t_1 < t \leq t_1 + 1 \\ \Delta_1 + 1 - k \cdot e^{-\alpha \cdot [(t-t_1)-1]^{\beta}} & t_1 + 1 < t \leq t_2 \end{cases} \tag{6.11}$$

Where the increment Δ_1 is evaluated as follow:

$$\Delta_1 = f_1(t_1) - f_1(0) \tag{6.12}$$

$$\Delta_1 = k \cdot e^{-\alpha} - k \cdot e^{-\alpha \cdot (t_1 - 1)^{\beta}} \tag{6.13}$$

Finally, the human likelihood of error after the break is given by function $f_2(t)$ as follow:

$$f_2(t) = \Delta_2 + 1 - k \cdot e^{-\alpha \cdot (t-t_2)^{\beta}} \qquad t_2 < t \leq t_{max} \tag{6.14}$$

The function $f_2(t)$ is a modified version of the Weibull distribution in eq. (6.4) updated to ensure a monotonically increasing trend. The initial decreased behavior that lasts for the first hour of shift in function $f_1(t)$ as in eq. (6.9) is not required in this case since the human operator has already adapted to the task. Therefore, function $f_2(t)$ is used to model only the cumulative fatigue in the final part of the shift. The increment Δ_2 is evaluated requiring continuity of function, as follow:

$$f_2(t_2) \ = \ f_{br}(t_2) \tag{6.15}$$

$$\Delta_2 \ + 1 - k \cdot e^{-\alpha \cdot \, (t_2 - t_2)^{\beta}} - f_{br}(t_2) \tag{6.16}$$

$$\Delta_2 = f_{br}(t_2) \ + \ k - 1 \tag{6.17}$$

In case the break duration is shorter than 1 hour the increment Δ_2 is evaluated using eq. (6.10). Thus:

$$\Delta_2 = k + \Delta_1 - k \cdot e^{-\alpha \cdot [1-(t_2 - t_1)]^{\beta}} \tag{6.18}$$

Otherwise, in case the break duration is longer than 1 hour the increment Δ_2 is evaluated using eq. (6.11). Consequently:

$$\Delta_2 = k + \Delta_1 - k \cdot e^{-\alpha \cdot [(t_2 - t_1) - 1]^{\beta}} \tag{6.19}$$

The proposed model could be easily updated introducing two (or even more) breaks within the work shift. For instance, Fig. 6.6 shows the HEP_{nom} in case of two breaks with different break durations.

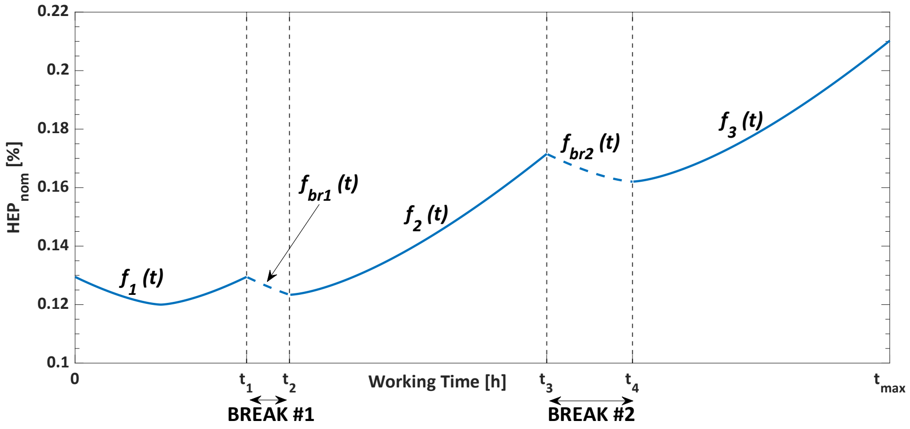


Fig. 6. 6 - Nominal HEP of the proposed E-SHERPA including two breaks within the working shift. The first break could represent a coffee break, while the second one stands for a lunch break

The mathematical description of the HEP in case of two breaks remains the same as eq. (6.8). The model is updated as follow:

$$HEP_{nom}(t) = \begin{cases} f_1(t) & 0 < t \leq t_1 \\ f_{br1}(t) & t_1 < t \leq t_2 \\ f_2(t) & t_2 < t \leq t_3 \\ f_{br2}(t) & t_3 < t \leq t_4 \\ f_3(t) & t_4 < t \leq t_{max} \end{cases} \qquad (6.20)$$

Where t_1 and t_2 are the start and end time of the first break respectively. Quite the same, t_3 and t_4 are the start and end time of the second break respectively.

Then, $f_{br1}(t)$ and $f_{br2}(t)$ describes the human error probability during the first and second break respectively, while $f_1(t)$, $f_2(t)$ and $f_3(t)$ represent the HEP during the operative hours before and after the breaks. For the sake of brevity, the mathematical models used to evaluate the above-mentioned functions in case of two breaks are not included in the paper, but they could be easily obtained updating eq. (6.9-6.19).

After the calculation of the nominal HEP using eq. (6.9-6.19), the proposed E-SHERPA requires the assessment of the contextual HEP using the eq. (6.5) and the introduction of the Eustress thanks to the Y-D law.

6.3. Validation of the proposed E-SHERPA

The Automatic Train Protection (ATP) is a safety-oriented system which continually checks that the speed of a train is compatible with the permitted speed allowed by signaling. If it is not, ATP activates an emergency brake to stop the train.

It aims to reduce or eliminate the possibility of driver error resulting in a train movement related accident by failing to obey a visually displayed line-side or in-cab signal instruction [4]. Italian railway signaling system uses different kind of ATPs, depending on the motive power (either diesel or electric), the type of line (high-speed or regional transportation) the maximum speed and the number of tracks in the line. The *"Sistema Controllo Marcia Treno"* - SCMT (Italian acronym for train running control system) is the most largely employed ATP in Italian rail network [329]. The study of SCMT is fundamental since it is the only Italian ATP harmonized with the European Railways Traffic Management System (ERTMS) which is a European standard that regulates the interoperability of railway network [330].

SCMT is based on two subunits that interact with each other: an “Onboard subsystem - SBB” and a “Ground subsystem - SST”. The SST comprises an array of transponders (called PI – Italian acronym that stands for Information Point) located on specific point of the tracks, such as a signal, a semaphore or a reduced speed zone. When a train passes over a PI, a set of antennas mounted in front of the first truck energize the PI through induction. Thus, the PI passes information about the aspect of the next signal to the SSB. The SBB used these data along with train information to evaluate a "braking curve" which specifies the train speed that must be respected approaching the further track section. Failure of observing the signal instructions causes the SSB to command emergency braking, which lasts until the speed gets below the limit.

Each PI of the SST is based on a set of balises mounted on the railroad tie in the center of the track. In order to ensure high availability and safety requirements, two nearby balises are required, as in Fig. 6.7. Generally, the “Ground subsystem - SST” also includes an encoder used to convert the signaling information from semaphores and signals into messages suitable for the balises. The whole SST is illustrated in Fig. 6.8

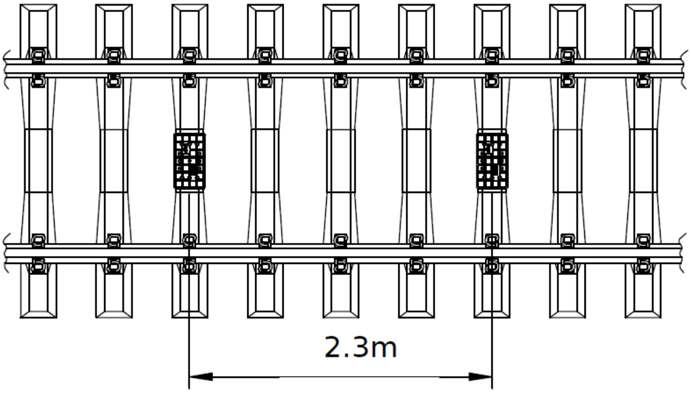


Fig. 6. 7 - Balises deployment on the railroad tie used by the SCMT to transmit information regarding the signal to the Onboard control. The distance between the balises refers to a rail track with maximum speed of 180 km/h.

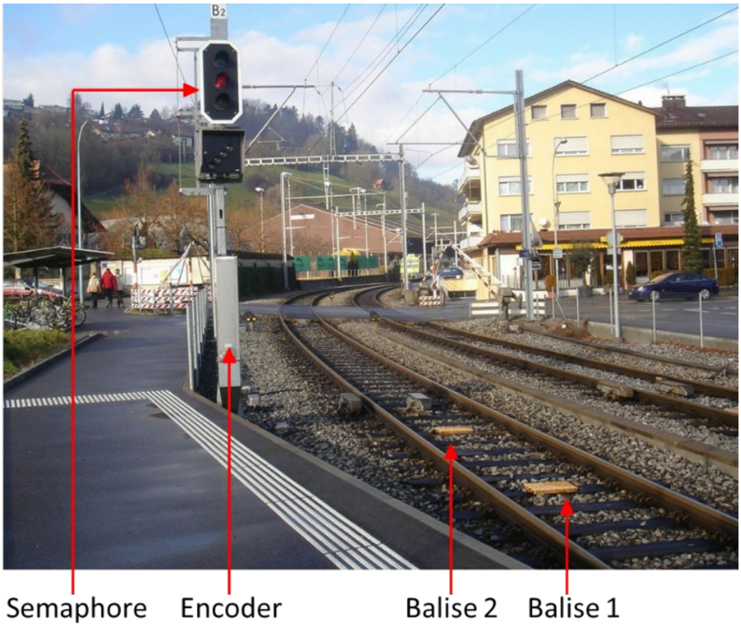


Fig. 6. 8 - Complete "Ground subsystem" of the SCMT including an encoder and two balises.

It is important to emphasize that the SCMT system (but more generally every ATP system) is a reliable and safe solution for correction or mitigation of human error during the train running, so that it becomes highly unlikely to cause an accident when such systems are used. The human errors that are significant for the safety of the railway system mainly reside in the design, installation, verification and maintenance phases of this safety-related systems. For this reason, the impact of the human factor on the aforementioned phases of the SCMT ground subsystem has been studied in this paper.

The most critical human activities are as follow:

- *Balises laying* it involves the following activities: track ballast removal, positioning and fixing of the support and laying of the connection cable. The main constrains during the balises laying are related to the low tolerance of the installation angle (tilting, pitching and yawing), to the metal-free zone nearby the balise and to the positioning of the connection cable which could generate interference problems.
- *Balise configuration:* it is a simple operation involving the programming of the PI through a computer and a suitable cable.
- *Maintenance:* it requires many activities to be performed. The first

step is the fault detection and isolation, which is followed by the configuration of a new item and the replacement of the non-functioning item. These operations require the use of many measuring instruments.

- *Encoder wiring*: it is a critical task with direct implications on safety. In fact, an incorrect wiring could lead to the transmission of incorrect information to the train (for example, the green light information could be transmitted when the light is red).

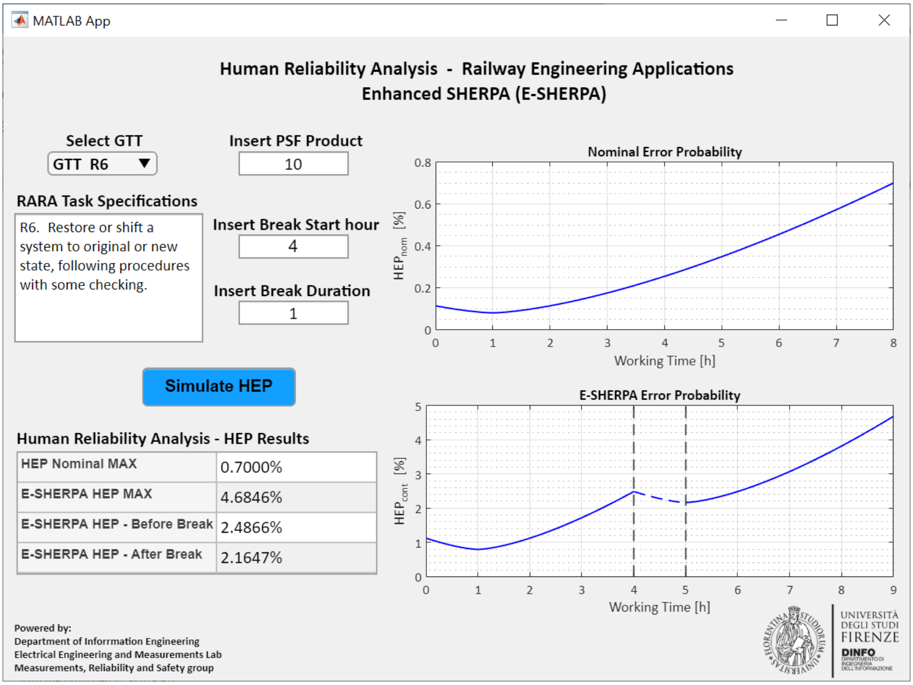
6.3.1 Railway Track Maintenance Operation

The proposed E-SHERPA method has been applied to the four tasks related to the SCMT ground subsystem explained in section 6.2. In order to simulate the HEP of the considered tasks according to E-SHERPA method a simulation algorithm and a Graphical User Interface (GUI) have been specifically developed. The proposed algorithm simulates the task performed by the operator during its working shift in railway field. The developed software evaluates the human error probability based on the performance shaping factor and the presence of breaks.

Fig. 6.9 shows the developed GUI which includes two graphs illustrating the nominal HEP without neither PSF nor break (top subplot) and the contextual HEP achieved with the proposed E-SHERPA (bottom subplot). The simulation illustrated in Fig. 6.9 refers to task GTT R6. It includes also a one-hour long break which starts after four working hours. The product of the PSF required to evaluate the contextual HEP is set equal to 6.10.

Maintenance operations result to be the most critical and challenging task. The simulations related to this activity are illustrated in this section. More in detail in case the onboard subsystem detects a transmission problem with the ground unit (or if it received an incorrect message) a maintenance operation is required to identify and isolate the failure.

The balise is a Line Replaceable Unit (LRU), which means that in case of failure this component should be replaced with a new one.



Human Reliability Analysis - Railway Engineering Applications
Enhanced SHERPA (E-SHERPA)

Select GTT: GTT R6

Insert PSF Product: 10

RARA Task Specifications

R6. Restore or shift a system to original or new state, following procedures with some checking.

Insert Break Start hour: 4

Insert Break Duration: 1

Human Reliability Analysis - HEP Results

HEP Nominal MAX	0.7000%
E-SHERPA HEP MAX	4.6846%
E-SHERPA HEP - Before Break	2.4866%
E-SHERPA HEP - After Break	2.1647%

Powered by:
Department of Information Engineering
Electrical Engineering and Measurements Lab
Measurements, Reliability and Safety group

UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Fig. 6. 9 - Proposed Graphical User Interface for the assessment of the E-SHERPA human reliability analysis. Task R6 is involved. PSF product is set equal to 10, the break starts after 4 h and the break duration is 1 h. The top subplot illustrates the nominal HEP, while the bottom subplot shows the contextual HEP achieved with the proposed E-SHERPA.

Thus, the general procedure for balise maintenance is based on the following actions:

- Fault detection and isolation.
- Configuration of a new LRU in compliance with the configuration of the faulty balise.
- Replacement of the faulty LRU with a new one.

The fault detection and isolation procedure is based on three verifications steps: balise integrity, balise correct orientation and balise correct functionalities.

The complete flowchart of the maintenance procedure is illustrated in fig. 6.10.

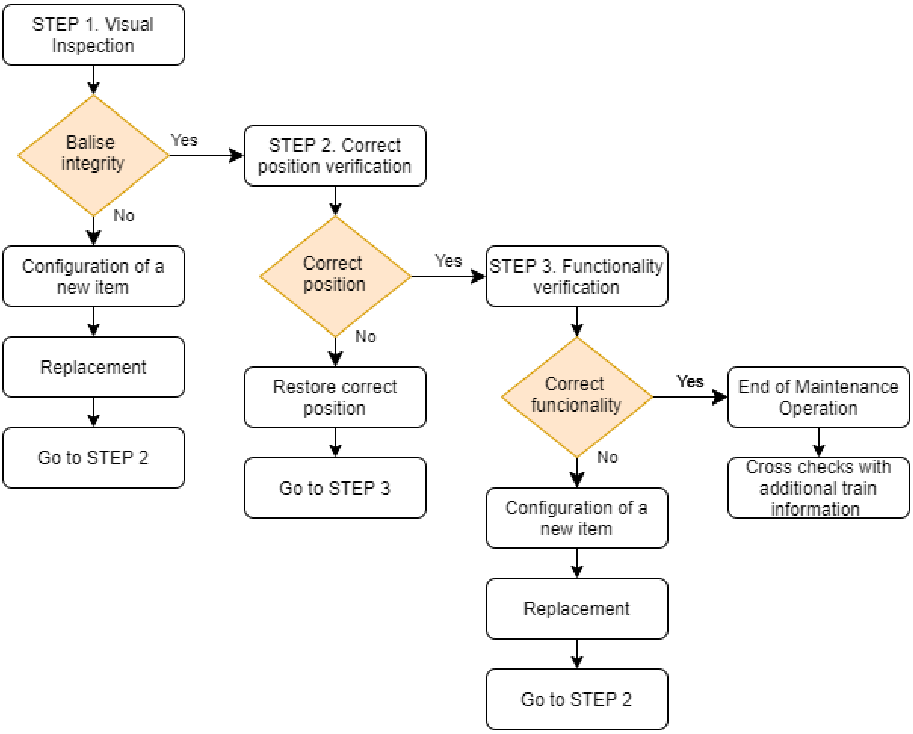

STEP 1. Visual Inspection
Balise integrity
Yes
No
STEP 2. Correct position verification
Configuration of a new item
Replacement
Go to STEP 2
Correct position
Yes
No
STEP 3. Functionality verification
Restore correct position
Go to STEP 3
Correct funcionality
Yes
No
End of Maintenance Operation
Cross checks with additional train information
Configuration of a new item
Replacement
Go to STEP 2

Fig. 6. 10 - Complete Flowchart of the balise maintenance including all the task that the operator should carry out when maintenance is required.

6.3.2 Human error probability estimation

Thus, the general task type that better describe the maintenance operation is GTT R6 (“Restore or shift a system to original or new state, following procedures with some checking”).

Table 6.1 provides the Weibull parameters used to evaluate the nominal HEP through eq. (6.8-6.19) of the maintenance task. Table 6.5 summarizes the performance shaping factors used to simulate the human behavior in four different operative contexts (called scenarios in the following). PSFs related to “Procedures” and “Work processes” are set to fixed values through the scenarios because they describe a well-structured and well-explained operation. Thus, in the simulations all the scenarios assume that the operators are fully aware of how they must proceed to complete the task.

Tab. 6. 5– PSF assessed in four different simulation scenarios.

PSF	SCENARIOS							
	(1) Optimal		(2) Real		(3) Fatigued		(4) Worst-case	
Available time	A3	1	A2	10	A2	10	A2	10
Stress	S4	0.5	S2	2	S1	5	S1	5
Complexity	C2	2	C2	2	C2	2	C2	2
Experience training	E3	0.5	E3	0.5	E3	0.5	E2	1
Procedures	PR4	1	PR4	1	PR4	1	PR4	1
Ergonomics	ER3	1	ER3	1	ER3	1	ER2	10
Fitness for duty	P3	1	P3	1	P2	5	P2	5
Work processes	W3	0.5	W3	0.5	W3	0.5	W3	0.5
PSF Product	0.25		10		125		2500	

Moreover, also the “Complexity” PSF is set to a fixed value since the task remain the same in all four scenarios. The four simulations are based on four different operative contexts:

1. Optimal: this scenario assumes the most favorable conditions for the operator, such large time to complete the task, optimal stress level (according to Y-D law), well-trained operator, etc. These extremely low PSF levels are usually not achievable since this kind of task is performed outdoor, during night shift and with low available time.
2. Real: this scenario is the most likelihood context for the maintenance task since it increases the PSFs related to stress and available time.
3. Fatigued: this scenario refers to a context in which the mental and physical conditions of the operator are degraded.
4. Worst-case: this scenario considers the most pessimistic context for the task. PSF related to time, stress and fitness for duty remain high. Moreover, this scenario assumes a not excellent training of the operator.

The PSF product included in the final row of Table 6.4 is used to evaluate the contextual HEP in different scenarios.

Fig. 6.11 illustrates the contextual HEP simulated in four different scenarios in compliance with the PSFs included in Table 6.5. The settings of the break (both start time and duration) are equal in each simulation scenario. The top left subplot (scenario 1) provides too optimistic results extremely difficult to achieve in a complex, outdoor activity. The contextual HEP is even lower than the nominal HEP due to the PSF product lower than 1. Quite the opposite, results provided by scenario 4 (bottom right subplot) are unrealistic since the probability of failure reach extremely high level (around 90%). Comparing scenarios (3) and (4) it is possible to understand the impact of a stressed and fatigues operator.

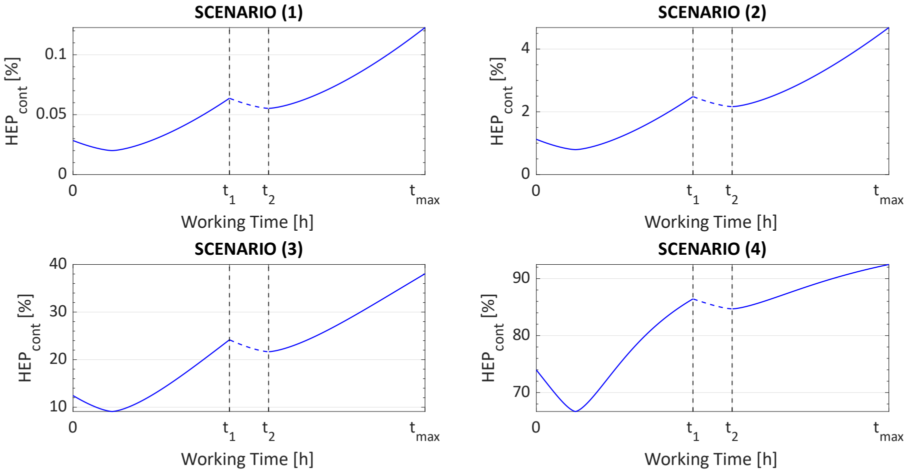


Fig. 6. 11 - Contextual HEP of the Maintenance task simulated using four different scenarios. Start time and duration of the break is set to a fixed value.

The difference obtained increasing Stress and Fitness for duty PSFs is quite remarkable, showing a consistent human error probability under these circumstances. In a safety-related environment such railway engineering the latter comparison should be useful to companies in order to take adequate countermeasures and prevent a high likelihood of accident. Companies should plan the working shifts accordingly in order to avoid fatigued operator.

Since scenario (2) represents the realistic context, the following simulations are based on its PSFs.

In order to analyze the impact of the break on the human error probability, Fig. 6.12 compares the SHERPA output with a simulation achieved using the proposed E-SHERPA. The break in the E-SHERPA method is set from the fourth to the fifth working hour in order to model a lunch break. The cumulative number of working hours is 8 in both plots. The introduction of the break provides a considerable reduction of the error probability in the final part of the work shift, allowing an optimal model of the human performances.

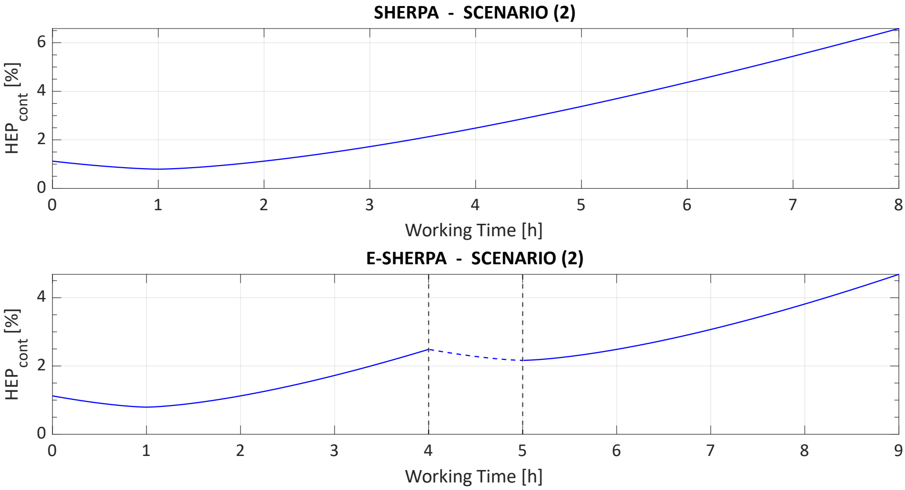


Fig. 6. 12 - Contextual HEP of the Maintenance task simulated comparing SHERPA (top subplot) and E-SHERPA (bottom subplot) methods. A one-hour long break has been set in the E-SHERPA model

The effects of different break durations are illustrated in Fig. 6.13, where the scenario (2) has been simulated with four different breaks, namely 30 min, 60 min, 90 min and 120 min. The start time of the break has been set after 4 working hours, and 8 cumulative working hours (excluding the breaks) have been considered. The simulations show that the different break durations don't have a remarkable impact on the HEP for the considered task.

As it is possible to see in the bottom subplots in Fig. 6.13 only breaks longer than 1h have a counter-productive effect.

Then, the impact of the breaks is evaluated in Fig. 6.14 comparing the HEP in case of one or two breaks.

The top subplot in Fig. 6.14 shows the E-SHERPA simulation considering a single one-hour break, while the bottom subplot shows the simulation achieved including two shorter breaks (30 minutes each). The total amount of working hour is 8 h in both cases. Even if the total amount of break is the same in both simulation (1 h overall) the contextual HEP in case of two shorter breaks is lower than the other case (on average).

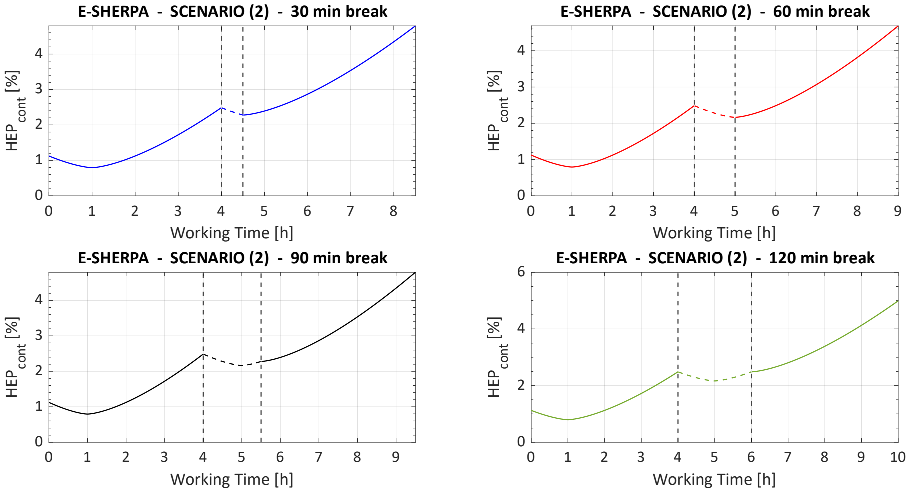


Fig. 6. 13 - Contextual HEP of the Maintenance task simulated varying the break duration (30 min – 60 min – 90 min – 120 min). Each plot shows 4 working hours before and after the break.

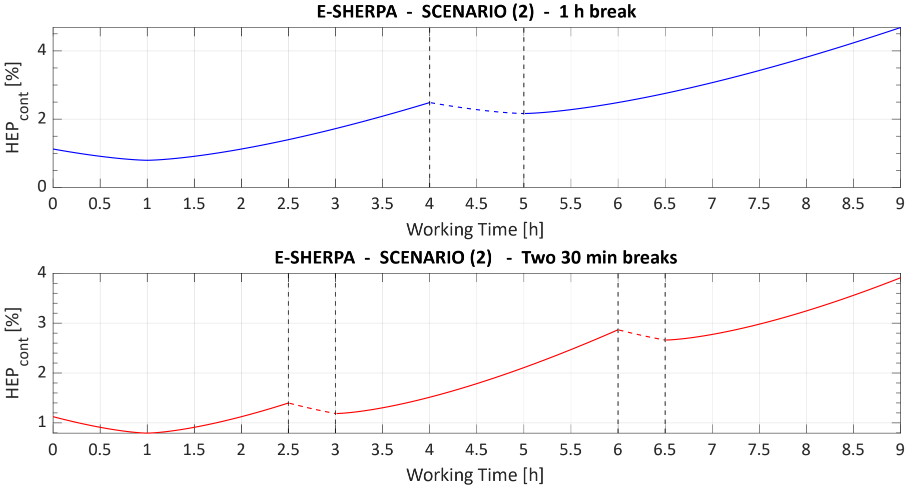


Fig. 6. 14 - Contextual HEP of the Maintenance task simulated using only one long break (top subplot) or using two shorter breaks (bottom subplot). The total amount of break minutes is the same in both simulations (60 minutes) as well as the total amount of working hours (8 h).

The proposed simulator allows designer to evaluate the human performances varying a PSF level. Fig. 6.15 highlights the importance of the Yerkes-Dodson law showing different simulation of the same task achieved with different Stress PSF (as in Table 6.3).

Extremely High or Extremely Low level of stress have a remarkable impact on the human performances increasing the error probability up to not acceptable levels. The figure also highlights the benefits achieved in case of Eustress. The blue trend (S4 = 0.5 - Eustress) is the most important introduction due to the Y-D law providing even lower HEP than the nominal case (red trend).

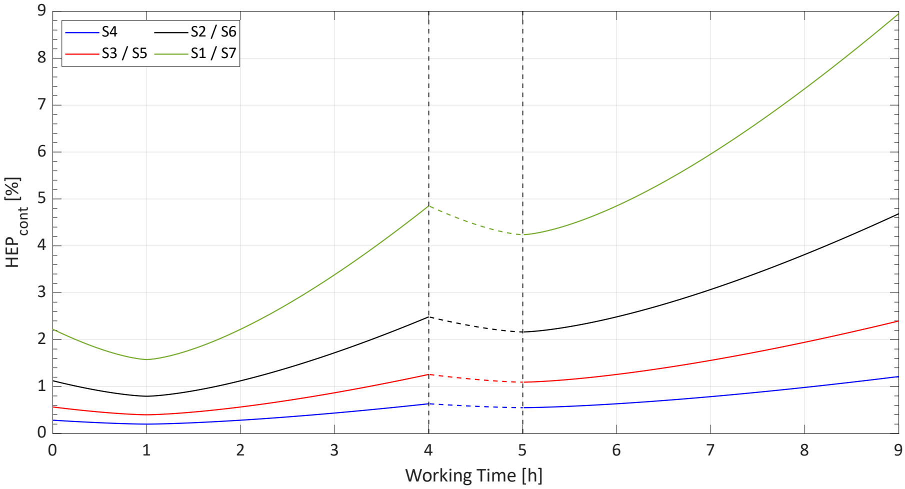


Fig. 6. 15 - Contextual HEP of the Maintenance task simulated using all the possible Stress PSF proposed in Table 4 according to the Yerkes-Dodson law.

6.3.3 Validation with empirical data

Finally, the proposed E-SHERPA approach has been validated comparing the simulated contextual HEP with a set of field data regarding the human errors during maintenance operation of railway systems.

The details of the dataset under analysis are listed in the following:

- Observation time period: 3 months.
- Involved task: maintenance operation of railway signaling systems installed nearby railroad track.
- Maintenance crew: 8 operators.
- Working days: 6 days a week.
- Shift: both daytime and nighttime work.

- Working hour per shift: 8 cumulative hours
- Breaks: a single 1-hour break in the middle of the shift

Although the complete set of field data were not available, the comparison illustrated in Fig. 6.16 highlights a significant correlation between the assessment carried out using the proposed E-SHERPA method and the observed data.

More in detail, the simulation depicted in the top subplot of Fig. 6.16 refers to the maintenance task described using "GTT R6" and considering the real operating context "SCENARIO (2)". The available field data are illustrated in the bottom subplot of Fig. 6.16 and they refer to the reported/observed human errors at four different moments of the work shift. The first bar shows the errors committed approximately after 1 working hour; the second bar stands for the error observed in the half-hour before the break; the third bar represents the errors committed by the operators approximately 1 h after the break and finally the errors observed in the final half hour of the shift are reported in the last bar.

The figure shows how very few errors are committed in the initial phase of the shift, while most of the errors are made in the final minutes of the shift. Looking more in detail what happen near the break, the number of errors observed right before the break is the same one observed 1 hour after the break.

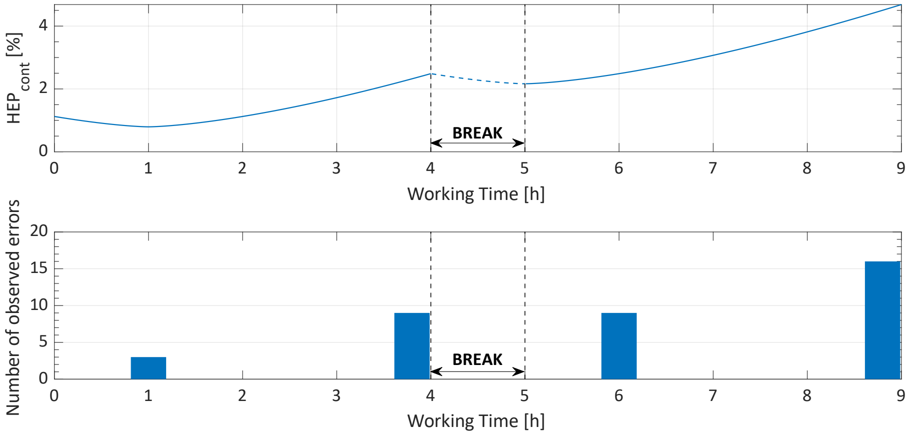


Fig. 6. 16 - Validation of the proposed E-SHERPA approach (top subplot) using field data regarding the human error observed during maintenance operation of railway signaling systems.

Thus, the field data highlight a general trend quite similar to the one provided using the E-SHERPA simulator, providing a positive feedback regarding the performances of the proposed approach.

A final consideration is required analyzing this data. It is extremely important to keep in mind that the observed errors have led to no accidents nor to potentially hazardous conditions. In fact, most of the time the errors committed by the maintenance crew are identified during the post-maintenance verification task, performed by independent operators.

6.4. Final Remarks

Several technical reports agree that human error is one of the most probable cause of accident in railway field. Despite this, only few approaches are available in literature to estimate the human performances in railway engineering.

This chapter presents an innovative human reliability analysis technique to estimate a time-dependent human error probability during the work shift. The proposed E-SHERPA enhances and improves the SHERPA method providing task specifically developed for railway, updating the PSF including the concept of beneficial stress (Eustress – Y-D law) and introducing a time-dependent estimation of the HEP during the lunch and coffee breaks. The innovative E-SHERPA method can dynamically study the entire operator work shift describing the HEP using a time-dependent model. This feature allows a proper organization of the break scheduling since it shows how the human error probability increases during the classical 8 h working shift. The proposed simulator allows to introduce one or more breaks with different duration and different start time within the work shift. Moreover, the simulator can dynamically update the HEP estimation changing the PSFs that affect the human performances in order to simulate different operating scenarios at the same time.

The maintenance operation of an Italian Automatic Train Protection system has been taken as case study to validate the performances of the proposed E-SHERPA method. The comparison between four different PSF scenarios highlights the importance of a well-trained operator aware of the procedure to maintain a low error probability and improve the performances.

Different simulation scenarios have been run to estimate the impact of different breaks on the human activities. The results highlight several points:

- The simulations prove the importance for companies to plan the working shifts in order to avoid fatigued operator. However, too long breaks could be counter-productive since they lead the operator to an excessively relaxed behavior.
- Breaks between 30 minutes and 60 minutes have a similar effect on the human performing the studied maintenance task.
- Introducing two breaks in the proposed E-SHERPA allows to ensure better results in term of human error probability respect to a single longer break.
- The comparison of the proposed approach with field data (regarding the human errors observe during maintenance operations in railway signaling systems) provides a positive feedback to validate the E-SHERPA model.

Conclusions

This thesis work focuses on Reliability, Availability, Maintainability and Safety in railway engineering. Railway field is a very standardized sector, therefore the first part of the work is dedicated to the review of the main standard for RAMS in railway. EN 50126, EN 50128, EN 50129 describes the application of a systematic RAMS management process in the railway field. The standard underlines the importance of RAMS study in railway industry with particular attention to risk assessment and human factor.

Human factor is a very important topic to consider because human factors represent one of the main causes of railway accident in the last years. Therefore, it is fundamental to study it and consider it in the assessment to reduce the impact of human error in accident.

Chapter 2 introduces the fuzzy theory and fuzzy logic to explain the topic and the idea of the mathematical theory used throughout the work. Fuzzy logic is very useful in case of uncertain data, therefore it is implemented in RAMS analysis to reduce the subjectivity thanks to the linguistic variables. Chapter 2 provides an overview on fuzzy numbers, operations between fuzzy number, defuzzification and how to use fuzzy in RAMS.

Chapter 3 analyzes one of the main topics of this work, the risk-based maintenance planning in which the maintenance policy of the complex system under analysis depends on the result of a risk assessment. One of the widest used techniques in this field is Reliability Centred Maintenance. RCM is based on a preliminary FMECA analysis followed by a prioritization of the failure modes and a decision on what maintenance task should be associates to each failure mode. The decision part is performed following a decision-making diagram included in IEC 60300-3-11. This diagram is completely generic and vague and it leave to the expertise of the analyst the maintenance choice. Therefore, after highlighting this problem this thesis aims to propose a new diagram based on a fuzzy FMECA which provides a unique choice of the maintenance task. The proposed fuzzy-based approach uses a diagnostic-oriented decision-diagram which optimize the Operation&Maintenance cost and the system availability by means of Condition-Based Maintenance techniques.

FMECA is widely used in risk analysis of railway systems despite it suffers many drawbacks listed in section 3.8. Therefore a new fuzzy FMECA approach has been introduced in section 3.9. The proposed method includes adequate fuzzy weights to allow different importance to O, S, D. Furthermore, fuzzy logic helps to mitigate the subjective assessment and the results present a continuous set of outcomes without problem of duplicates or gaps in the range. The only drawback of RPN that the proposed method is not able to solve is the ability to prioritize the mode according to a certain threshold.

Thus, Section 3.13 presents a new analytical method to find a risk priority number threshold. The procedure allows to find a threshold level and distinguish the modes lower than the threshold as negligible and higher as critical. This approach allows to be cost effective mitigating the risk of only the modes defined as critical.

The last part of the thesis focuses on human error and human reliability. Chapter 4 focuses on the literature review of HRA in railway industry. HRA is characterized by several techniques, divided into three generations depending on the year of publication and the common characteristics. However, HRA in railway is not so widespread and there are very few papers dedicated to this sector. The most used and only validated technique for railway is RARA and it is described in section 4.5. For this reason, the following chapters focuses on the improvement of a well-known technique such as RARA and the introduction of a new third-generation technique completely developed for railway.

More in detail, Chapter 5 focuses on the improvement of RARA, proposing a fuzzy procedure to solve the main drawbacks of the original technique: subjectivity and complexity of the assessment. The procedure considers a fuzzification of the GTT and EPC. Then it maintains the same mathematical expression to calculate the overall human error probability by means of α-cut theory. The resulting HEP is a fuzzy membership function which can assume all the values inside the membership interval, then the defuzzification procedure provides a crisp HEP. Comparing the results with RARA, the proposed method has proven to be effective and characterized by an easier linguistic assessment.

Finally, Chapter 6 focuses on the new HRA technique, named E-SHERPA. It is a new method for the human error assessment specifically developed for railway. E-SHERPA uses the Weibull distribution to provides a nominal HEP variable with time. The idea is that increasing the work-shift the HEP increases, with a minimum after 1 h. Nominal HEP is modified taking into account the Performance Shaping Factor of SPAR-H technique. The stress PSF is modified taking into account the Yerkes-Dodson law in order to introduce the concept of Eustress. Too high and too low level of stress provide a decreasing of the human performance and the right amount of stress which maximize the performance is in the middle (neither too high nor not too low). The last contribution of the method is the introduction of breaks to provide a more realistic HRA model. In fact this model provides the opportunity to insert one or more breaks with variable duration. Also the breaks are modeled through Weibull distribution. Finally the overall HEP will be a Weibull function depending on the task performed, the operative context, the amount of stress and the number and duration of breaks during the work-shift.

Both HRA methods developed in this thesis have been applied to the manual operations performed on Automatic Train Protection system installed nearby the railroad. The results in Chapter 5 and Chapter 6 highlights a significant contribution of the human error to the probability of accidents, emphasizing the importance of a detailed study of this problem during the system life cycle.

REFERENCE

[1] CENELEC, “50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process,” 2017.

[2] CENELEC, “EN 50126-2 - Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety,” 2017.

[3] CENELEC, “EN 50128-Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems,” 2011.

[4] EN 50129, “Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.” CENELEC - European Committee for Electrotechnical Standardization, 2018.

[5] UIC Safety Unit, “UIC Safety Report 2021. Significant accident 2020 public report.” 2021.

[6] S. C. Sugarman, *HVAC Fundamentals*, Second. Fairmont Press, 2007.

[7] A. Vedavarz, S. Kumar, and M. I. Hussain, *HVAC Handbook of Heating, Ventilation, and Air Conditioning for Design & Implementation*, Fourth. industrial press inc., 2013.

[8] F. Porges, *HVAC Engineer handbook*, no. February. Elsevier Science & Technology Books, 2001.

[9] M. Catelani, L. Ciani, V. Luongo, and R. Singuaroli, “Evaluation of the Safe Failure Fraction for an electromechanical complex system: remarks about the standard IEC61508,” in *2010 IEEE Instrumentation & Measurement Technology Conference Proceedings*, 2010, pp. 949–953.

[10] Alstom, “How does the air conditioning work in a train?,” 2020. [Online]. Available: https://3minutesstop.alstom.com/infographie/air-conditioning-work-train/. [Accessed: 17-Feb-2020].

[11] RENFE, “Manual descriptivo sistema de climatizacion - serie 121.” 2009.

[12] CENELEC, “EN 50129- Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.” 2018.

[13] P. Connor, “The Railway Technical Website,” 2019. [Online]. Available: http://www.railway-technical.com/signalling/. [Accessed: 24-Aug-2021].

[14] M. Bosschaart, E. Quaglietta, B. Janssen, and R. M. P. Goverde, “Efficient formalization of railway interlocking data in RailML,” *Inf. Syst.*, vol. 49, no. September, pp. 126–141, Apr. 2015.

[15] I. Watanabe and T. Takashige, “Advanced automatic train protection system,” in *Proceedings of IEEE Vehicular Technology Conference (VTC)*, pp. 1126–1129.

[16] M. G. Voskoglou, “Fuzzy Logic: History, Methodology and Applications to Education,” *Sumerianz J. Educ. Linguist. Lit.*, vol. 1, no. 1, pp. 2617–1732, 2018.

[17] E. H. Mamdani and S. Assilian, “An experiment in linguistic synthesis with a fuzzy logic controller,” *Int. J. Man. Mach. Stud.*, vol. 7, no. 1, pp. 1–13, Jan. 1975.

[18] J. Yen, “Fuzzy logic-a modern perspective,” *IEEE Trans. Knowl. Data Eng.*, vol. 11, no. 1, pp. 153–165, 1999.

[19] T. J. Ross and Timothy J. Ross, *Fuzzy Logic With Engineering Applications*, vol. 91. 2017.

[20] L. A. Zadeh, “Fuzzy sets,” *Inf. Control*, vol. 8, no. 3, pp. 338–353, Jun. 1965.

[21] K.-Y. Cai, *Introduction to Fuzzy Reliability.* Kluwer Academic Publishers, 1996.

[22] J. B. Bowles and C. E. Pelaez, “Application of fuzzy logic to reliability engineering,” *Proc. IEEE*, vol. 83, no. 3, pp. 435–449, Mar. 1995.

[23] S. Kabir and Y. Papadopoulos, “A review of applications of fuzzy sets to safety and reliability engineering,” *Int. J. Approx. Reason.*, vol. 100, pp. 29–55, 2018.

[24] R. Kenarangui, “Event-tree analysis by fuzzy probability,” *IEEE Trans. Reliab.*, vol. 40, no. 1, pp. 120–124, 1991.

[25] V. A, “Reliability analysis of dynamic fault tree models using fuzzy sets,” *Commun. Dependability Qual. Manag.*, vol. 9, no. 4, pp. 68–78, 2006.

[26] S. Kabir, M. Walker, Y. Papadopoulos, E. Rüde, and P. Securius, “Fuzzy temporal fault tree analysis of dynamic systems,” *Int. J. Approx. Reason.*, vol. 77, pp. 20–37, 2016.

[27] M. Braglia, M. Frosolini, and R. Montanari, “Fuzzy criticality assessment model for failure modes and effects analysis,” *Int. J. Qual. Reliab. Manag.*, vol. 20, no. 4, pp. 503–524, 2003.

[28] T. R. Moss *et al.*, “Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean,” *Expert Syst. Appl.*, vol. 40, no. 2, pp. 1–6, 2013.

[29] R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, and B. Veitch, “Handling data uncertainties in event tree analysis,” *Process Saf. Environ. Prot.*, vol. 87, no. 5, pp. 283–292, Sep. 2009.

[30] M. Kasaeyan, J. Wang, I. Jenkinson, and L. Miri, “Fuzzy consequence modelling of hydrocarbon offshore pipeline,” *J. Mar. Sci. Eng.*, vol. 1, no. 1, pp. 3–12, 2011.

[31] H.-Z. Huang, M. J. Zuo, and Z.-Q. Sun, “Bayesian reliability analysis for fuzzy lifetime data,” *Fuzzy Sets Syst.*, vol. 157, no. 12, pp. 1674–1686, Jun. 2006.

[32] Y.-F. Li, J. Mi, Y. Liu, Y.-J. Yang, and H.-Z. Huang, “Dynamic fault tree analysis based on continuous-time Bayesian networks under fuzzy numbers,” *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 229, no. 6, pp. 530–541, Dec. 2015.

[33] E. Sanchez, Konstantin E. Avrachenkov, “Fuzzy Markov Chains and Decision-Making,” *Fuzzy Optim. Decis. Mak.*, pp. 143–159, 2002.

[34] R. Kruse, R. Buck-Emden, and R. Cordes, “Processor power considerations — An application of fuzzy markov chains,” *Fuzzy Sets Syst.*, vol. 21, no. 3, pp. 289–299, Mar. 1987.

[35] M. G. Voskoglou, “Fuzzy Logic: History, Methodology and Applications to Education,” *Sumerianz J. Educ. Linguist. Lit.*, vol. 1, no. 1, pp. 2617–1732, 2018.

[36] T. J. Ross, *Fuzzy Logic with Engineering Applications*, Third. John Wiley & Sons, 2010.

[37] Y. M. Wang, K. S. Chin, G. K. K. Poon, and J. B. Yang, “Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean,” *Expert Syst. Appl.*, vol. 36, no. 2 PART 1, pp. 1195–1207, 2009.

[38] M. Hayati and M. Reza Abroshan, “Risk Assessment using Fuzzy FMEA (Case Study: Tehran Subway Tunneling Operations),” *Indian J. Sci. Technol.*, vol. 10, no. 9, pp. 1–9, Feb. 2017.

[39] N. Mogharreban and L. F. DiLalla, “Comparison of Defuzzification Techniques for Analysis of Non-interval Data,” in *NAFIPS 2006 - 2006 Annual Meeting of the North American Fuzzy Information Processing Society*, 2006, pp. 257–260.

[40] C. Wang, “A Study of Membership Functions on Mamdani-Type Fuzzy Inference System for Industrial Decision-Making,” 2015.

[41] M. Sugeno and G. . Kang, “Structure identification of fuzzy model,” *Fuzzy Sets Syst.*, vol. 28, no. 1, pp. 15–33, Oct. 1988.

[42] G. D’Emilia, A. Gaspari, and E. Natale, “Measurements for Smart Manufacturing in an Industry 4.0 Scenario A Case-Study on A Mechatronic System,” in *2018 Workshop on Metrology for Industry 4.0 and IoT*, 2018, pp. 1–5.

[43] G. D’Emilia, A. Gaspari, E. Hohwieler, A. Laghmouchi, and E. Uhlmann, “Improvement of Defect Detectability in Machine Tools Using Sensor-based Condition Monitoring Applications,” *Procedia CIRP*, vol. 67, pp. 325–331, 2018.

[44] E. Petritoli, F. Leccese, and G. S. Spagnolo, “In-Line Quality Control in Semiconductors Production and Availability for Industry 4.0,” in *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, 2020, pp. 665–668.

[45] F. Abate, M. Carratù, C. Liguori, and V. Paciello, “A low cost smart power meter for IoT,” *Measurement*, vol. 136, pp. 59–66, Mar. 2019.

[46] M. Catelani, L. Ciani, and M. Venzi, “Sensitivity analysis with MC simulation for the failure rate evaluation and reliability assessment,” *Meas. J. Int. Meas. Confed.*, vol. 74, pp. 150–158, 2015.

[47] N. Sakib and T. Wuest, “Challenges and Opportunities of Condition-based Predictive Maintenance: A Review,” *Procedia CIRP*, vol. 78, pp. 267–272, 2018.

[48] L. Ciani, G. Guidi, G. Patrizi, and M. Venzi, “System Maintainability Improvement using Allocation Procedures,” in *2018 IEEE International Systems Engineering Symposium (ISSE)*, 2018, pp. 1–6.

[49] D. Capriglione, M. Carratu, A. Pietrosanto, and P. Sommella, “Online Fault Detection of Rear Stroke Suspension Sensor in Motorcycle,” *IEEE Trans. Instrum. Meas.*, vol. 68, no. 5, pp. 1362–1372, May 2019.

[50] M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, “Maintainability improvement using allocation methods for railway systems,” *Acta IMEKO*, vol. 9, no. 1, pp. 10–17, 2020.

[51] M. Catelani and L. Ciani, “Experimental tests and reliability assessment of electronic ballast

system," *Microelectron. Reliab.*, vol. 52, no. 9–10, pp. 1833–1836, Sep. 2012.

[52] IEC 60300-3-11, "Dependability management – Part 3-11 - Application guide – Reliability centred maintenance." International Electrotechnical Commission, 2009.

[53] IEC 60812, "Failure modes and effects analysis (FMEA and FMECA)." International Electrotechnical Commission, 2018.

[54] M. Catelani, L. Ciani, D. Galar, and G. Patrizi, "Risk Assessment of a Wind Turbine: A New FMECA-Based Tool With RPN Threshold Estimation," *IEEE Access*, vol. 8, pp. 20181–20190, 2020.

[55] J. Huang, J.-X. You, H.-C. Liu, and M.-S. Song, "Failure mode and effect analysis improvement: A systematic literature review and future research agenda," *Reliab. Eng. Syst. Saf.*, vol. 199, no. January 2019, p. 106885, Jul. 2020.

[56] A. Birolini, *Reliability Engineering.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2017.

[57] H. Soltanali, A. Rohani, M. H. Abbaspour-Fard, A. Parida, and J. T. Farinha, "Development of a risk-based maintenance decision making approach for automotive production line," *Int. J. Syst. Assur. Eng. Manag.*, no. December, Dec. 2019.

[58] L. Ciani, G. Guidi, and G. Patrizi, "A Critical Comparison of Alternative Risk Priority Numbers in Failure Modes, Effects, and Criticality Analysis," *IEEE Access*, vol. 7, pp. 92398–92409, 2019.

[59] K. Fischer, F. Besnard, and L. Bertling, "Reliability-Centered Maintenance for Wind Turbines Based on Statistical Analysis and Practical Experience," *IEEE Trans. Energy Convers.*, vol. 27, no. 1, pp. 184–195, Mar. 2012.

[60] B. Lienhardt, E. Hugues, C. Bes, and D. Noll, "Failure-Finding Frequency for a Repairable System Subject to Hidden Failures," *J. Aircr.*, vol. 45, no. 5, pp. 1804–1809, Sep. 2008.

[61] L. Ciani, A. Bartolini, G. Guidi, and G. Patrizi, "Condition monitoring of wind farm based on wireless mesh network," in *16th IMEKO TC10 Conference 2019 &amp;amp;amp;amp;amp;amp;quot;Testing, Diagnostics and Inspection as a Comprehensive Value Chain for Quality and Safety&amp;amp;amp;amp;amp;amp;quot;*, 2019.

[62] C. Bhargava *et al.*, "Review of Health Prognostics and Condition Monitoring of Electronic Components," *IEEE Access*, vol. 8, pp. 75163–75183, 2020.

[63] A. Pandey and P. M. Sonwane, "Implementation of Reliability Centred Maintenance for transformer," *Int. Conf. Autom. Control Dyn. Optim. Tech. ICACDOT 2016*, pp. 578–581, 2017.

[64] M. Rafiei, M.-H. Khooban, M. A. Igder, and J. Boudjadar, "A Novel Approach to Overcome the Limitations of Reliability Centered Maintenance Implementation on the Smart Grid Distance Protection System," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 67, no. 2, pp. 320–324, Feb. 2020.

[65] K. Tirapong and S. Titti, "Reliability improvement of distribution system using Reliability Centered Maintenance," in *2014 IEEE PES T&D Conference and Exposition*, 2014, pp. 1–5.

[66] H. A. Khorshidi, I. Gunawan, and M. Y. Ibrahim, "Reliability centered maintenance using system dynamics approach," in *2015 IEEE International Conference on Industrial Technology (ICIT)*, 2015, vol. 2015-June, no. June, pp. 1932–1936.

[67] Z. Chen *et al.*, “Mission Reliability-Oriented Selective Maintenance Optimization for Intelligent Multistate Manufacturing Systems With Uncertain Maintenance Quality,” *IEEE Access*, vol. 7, pp. 109804–109816, 2019.

[68] J. T. Selvik and T. Aven, “A framework for reliability and risk centered maintenance,” *Reliab. Eng. Syst. Saf.*, vol. 96, no. 2, pp. 324–331, 2011.

[69] K. Zakikhani, F. Nasiri, and T. Zayed, “Availability-based reliability-centered maintenance planning for gas transmission pipelines,” *Int. J. Press. Vessel. Pip.*, vol. 183, no. October 2019, p. 104105, Jun. 2020.

[70] B. Yssaad and A. Abene, “Rational Reliability Centered Maintenance Optimization for power distribution systems,” *Int. J. Electr. Power Energy Syst.*, vol. 73, pp. 350–360, Dec. 2015.

[71] D. He, X. Zhang, C. Ge, and E. Chen, “A Novel Reliability-Centred Opportunistic Maintenance Strategy for Metro Train Complex System,” *IEEE Intell. Transp. Syst. Mag.*, no. September 2020, pp. 0–0, 2020.

[72] P. Afzali, F. Keynia, and M. Rashidinejad, “A new model for reliability-centered maintenance prioritisation of distribution feeders,” *Energy*, vol. 171, pp. 701–709, Mar. 2019.

[73] S. H. A. Rahmati, A. Ahmadi, and B. Karimi, “Multi-objective evolutionary simulation based optimization mechanism for a novel stochastic reliability centered maintenance problem,” *Swarm Evol. Comput.*, vol. 40, no. May 2017, pp. 255–271, Jun. 2018.

[74] D. Piasson, A. A. P. Bíscaro, F. B. Leão, and J. R. S. Mantovani, “A new approach for reliability-centered maintenance programs in electric power distribution systems based on a multiobjective genetic algorithm,” *Electr. Power Syst. Res.*, vol. 137, pp. 41–50, Aug. 2016.

[75] J.-H. Heo *et al.*, “A Reliability-Centered Approach to an Optimal Maintenance Strategy in Transmission Systems Using a Genetic Algorithm,” *IEEE Trans. Power Deliv.*, vol. 26, no. 4, pp. 2171–2179, Oct. 2011.

[76] M. Catelani, L. Ciani, D. Galar, and G. Patrizi, “Optimizing Maintenance Policies for a Yaw System Using Reliability-Centered Maintenance and Data-Driven Condition Monitoring,” *IEEE Trans. Instrum. Meas.*, vol. 69, no. 9, pp. 6241–6249, Sep. 2020.

[77] J. B. Bowles and C. E. Peláez, “Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis,” *Reliab. Eng. Syst. Saf.*, vol. 50, no. 2, pp. 203–213, 1995.

[78] Z. Yang, S. Bonsall, and J. Wang, “Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in FMEA,” *IEEE Trans. Reliab.*, vol. 57, no. 3, pp. 517–528, 2008.

[79] C. Dağsuyu, E. Göçmen, M. Narlı, and A. Kokangül, “Classical and fuzzy FMEA risk analysis in a sterilization unit,” *Comput. Ind. Eng.*, vol. 101, pp. 286–294, 2016.

[80] J. Bowles, “An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis,” *J. IEST*, vol. 47, no. 1, pp. 51–56, Sep. 2004.

[81] A. Certa, M. Enea, G. M. Galante, and C. M. La Fata, “ELECTRE TRI-based approach to the failure modes classification on the basis of risk parameters: An alternative to the risk priority number,” *Comput. Ind. Eng.*, vol. 108, pp. 100–110, 2017.

[82] S. Carpitella, A. Certa, J. Izquierdo, and C. M. La Fata, “A combined multi-criteria approach to support FMECA analyses: A real-world case,” *Reliab. Eng. Syst. Saf.*, vol. 169, no. June 2016, pp. 394–402, 2018.

[83] M. S. Upadhya, “Fuzzy Logic-Based Failure Mode Effect and Criticality Analysis – A Case Study of Water Filters of a Company,” *J. Comput. Appl.*, vol. VI, no. 4, pp. 89–93, 2013.

[84] Y.-M. Wang, K.-S. Chin, G. K. K. Poon, and J.-B. Yang, “Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean,” *Expert Syst. Appl.*, vol. 36, no. 2, pp. 1195–1207, Mar. 2009.

[85] K.-H. Chang and C.-H. Cheng, “Evaluating the risk of failure using the fuzzy OWA and DEMATEL method,” *J. Intell. Manuf.*, vol. 22, no. 2, pp. 113–129, Apr. 2011.

[86] A. C. Kutlu and M. Ekmekçioğlu, “Fuzzy failure modes and effects analysis by using fuzzy TOPSIS-based fuzzy AHP,” *Expert Syst. Appl.*, vol. 39, no. 1, pp. 61–67, Jan. 2012.

[87] Y. Tsukamoto, “An approach to fuzzy reasoning method,” in *Advances in fuzzy set theory and applications*, M. M. Gupta, R. K. Ragade, and R. R. Yager, Eds. Amsterdam: North-Holland Publishing Company, 1979, pp. 137–149.

[88] L. Ciani, G. Guidi, and G. Patrizi, “Condition-based Maintenance for Oil&Gas system basing on Failure Modes and Effects Analysis,” in *2019 IEEE 5th International forum on Research and Technology for Society and Industry (RTSI)*, 2019, pp. 85–90.

[89] K. O. Kim and M. J. Zuo, “General model for the risk priority number in failure mode and effects analysis,” *Reliab. Eng. Syst. Saf.*, vol. 169, no. September 2017, pp. 321–329, 2018.

[90] N. Sellappan and K. Palanikumar, “Modified Prioritization Methodology for Risk Priority Number in Failure Mode and Effects Analysis,” *Int. J. Appl. Sci. Technol.*, vol. 3, no. 4, pp. 27–36, 2013.

[91] R. Baillot and Y. Deshayes, *Reliability Investigation of LED Devices for Public Light Applications*. ISTE Press Ltd, Elsevier, 2017.

[92] S. M. Shrestha *et al.*, “Determination of dominant failure modes using FMECA on the field deployed c-Si modules under hot-dry desert climate,” *IEEE J. Photovoltaics*, vol. 5, no. 1, pp. 174–182, 2015.

[93] A. Mohammadi and M. Tavakolan, “Construction project risk assessment using combined fuzzy and FMEA,” *Proc. 2013 Jt. IFSA World Congr. NAFIPS Annu. Meet. IFSA/NAFIPS 2013*, pp. 232–237, 2013.

[94] H. C. Liu, L. Liu, and N. Liu, “Risk evaluation approaches in failure mode and effects analysis: A literature review,” *Expert Syst. Appl.*, vol. 40, no. 2, pp. 828–838, 2013.

[95] J. Braband, “Improving the risk priority number concept,” *J. Syst. Saf.*, vol. 39, no. 3, pp. 21–23, 2003.

[96] K.-H. Chang, Y.-C. Chang, and P.-T. Lai, “Applying the concept of exponential approach to enhance the assessment capability of FMEA,” *J. Intell. Manuf.*, vol. 25, no. 6, pp. 1413–1427, Dec. 2014.

[97] H. Akbarzade Khorshidi, I. Gunawan, and M. Y. Ibrahim, “Applying UGF Concept to Enhance the Assessment Capability of FMEA,” *Qual. Reliab. Eng. Int.*, vol. 32, no. 3, pp. 1085–1093, 2016.

[98] T.-L. Nguyen, M.-H. Shu, and B.-M. Hsu, “Extended FMEA for Sustainable Manufacturing: An Empirical Study in the Non-Woven Fabrics Industry,” *Sustainability*, vol. 8, no. 9, p. 939, Sep. 2016.

[99] G. Carmignani, "An integrated structural framework to cost-based FMECA: The priority-cost FMECA," *Reliab. Eng. Syst. Saf.*, vol. 94, no. 4, pp. 861–871, 2009.

[100] F. Rezaei, M. H. Yarmohammadian, A. Haghshenas, A. Fallah, and M. Ferdosi, "Revised risk priority number in failure mode and effects analysis model from the perspective of healthcare system," *Int. J. Prev. Med.*, vol. 9, no. February, 2018.

[101] Y. Tang, D. Zhou, and F. T. S. Chan, "AMWRPN: Ambiguity Measure Weighted Risk Priority Number Model for Failure Mode and Effects Analysis," *IEEE Access*, vol. 6, pp. 27103–27110, 2018.

[102] K. H. Chang, "Evaluate the orderings of risk for failure problems using a more general RPN methodology," *Microelectron. Reliab.*, vol. 49, no. 12, pp. 1586–1596, 2009.

[103] R. Sawhney, K. Subburaman, C. Sonntag, P. R. Venkateswara Rao, and C. Capizzi, "A modified FMEA approach to enhance reliability of lean systems," *Int. J. Qual. Reliab. Manag.*, vol. 27, no. 7, pp. 832–855, 2010.

[104] R. Y. Trianto, M. R. Pahlevi, and B. Z. Bardani, "FMECA development in PLN TRANS-JBTB," *Int. Conf. High Volt. Eng. Power Syst. ICHVEPS 2017 - Proceeding*, vol. 2017-Janua, pp. 567–570, 2017.

[105] J. M. Kuitche, R. Pan, and G. Tamizhmani, "Investigation of dominant failure mode(s) for field-aged crystalline silicon PV modules under desert climatic conditions," *IEEE J. Photovoltaics*, vol. 4, no. 3, pp. 814–826, 2014.

[106] M. Giardina and M. Morale, "Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology," *J. Loss Prev. Process Ind.*, vol. 35, pp. 35–45, 2015.

[107] L. He, T. Jin, N. Xiao, H.-Z. Huang, and Y. Li, "Multiple failure modes analysis and weighted risk priority number evaluation in FMEA," *Eng. Fail. Anal.*, vol. 18, no. 4, pp. 1162–1170, 2011.

[108] N. J. Lindsey, "An innovative Goddard Space Flight Center methodology for using FMECA as a risk assessment and communication tool," *Proc. - Annu. Reliab. Maintainab. Symp.*, vol. 2016-April, pp. 1–9, 2016.

[109] L. Hammadi, A. A. Ouahman, J. E. S. De Cursi, and A. Ibourk, "An approach based on FMECA methodology for a decision support tool for managing risk in Customs supply chain: A case study," *2015 Int. Conf. Logist. Informatics Serv. Sci. LISS 2015*, pp. 0–5, 2015.

[110] Y. Chen, L. Du, Y.-F. Li, H.-Z. Huang, and X. Li, "FMECA for aircraft electric system," in *2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering*, 2011, pp. 122–125.

[111] A. C. F. Guimarães, C. M. F. Lapa, and M. D. L. Moreira, "Fuzzy methodology applied to Probabilistic Safety Assessment for digital system in nuclear power plants," *Nucl. Eng. Des.*, vol. 241, no. 9, pp. 3967–3976, Sep. 2011.

[112] H. Yang and Z. Bai, "Risk evaluation of boiler tube using FMEA," *6th Int. Conf. Fuzzy Syst. Knowl. Discov. FSKD 2009*, vol. 7, no. x, pp. 81–85, 2009.

[113] Y.-S. Lee, H.-C. Kim, J.-M. Cha, and J.-O. Kim, "A new method for FMECA using expert system and fuzzy theory," in *2010 9th International Conference on Environment and Electrical Engineering*, 2010, no. 1, pp. 293–296.

[114] L. Gan, Y. Pang, Q. Liao, N.-C. Xiao, and H.-Z. Huang, “Fuzzy criticality assessment of FMECA for the SADA based on modified FWGM algorithm &amp; centroid deffuzzification,” in *2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering*, 2011, pp. 195–202.

[115] A. J. Sang, K. M. Tay, C. P. Lim, and S. Nahavandi, “Application of a genetic-fuzzy FMEA to rainfed lowland rice production in sarawak: Environmental, health, and safety perspectives,” *IEEE Access*, vol. 6, no. iii, pp. 74628–74647, 2018.

[116] V. R. Renjith, M. Jose kalathil, P. H. Kumar, and D. Madhavan, “Fuzzy FMECA (failure mode effect and criticality analysis) of LNG storage facility,” *J. Loss Prev. Process Ind.*, vol. 56, no. January, pp. 537–547, Nov. 2018.

[117] L. Liu, S. Ma, Z. Wang, and P. Li, “Use-related risk analysis for medical devices based on improved FMEA,” *Work*, vol. 41, no. SUPPL.1, pp. 5860–5865, 2012.

[118] M. Giardina, F. Castiglia, and E. Tomarchio, “Risk assessment of component failure modes and human errors using a new FMECA approach: Application in the safety analysis of HDR brachytherapy,” *J. Radiol. Prot.*, vol. 34, no. 4, pp. 891–914, 2014.

[119] T. R. Moss and J. Woodhouse, “Criticality analysis revisited,” *Qual. Reliab. Eng. Int.*, vol. 15, no. 2, pp. 117–121, 1999.

[120] A. Pillay and J. Wang, “Modified failure mode and effects analysis using approximate reasoning,” *Reliab. Eng. Syst. Saf.*, vol. 79, no. 1, pp. 69–85, Jan. 2003.

[121] H.-C. Liu, L. Liu, and Q.-L. Lin, “Fuzzy Failure Mode and Effects Analysis Using Fuzzy Evidential Reasoning and Belief Rule-Based Methodology,” *IEEE Trans. Reliab.*, vol. 62, no. 1, pp. 23–36, Mar. 2013.

[122] A. C. F. Guimarães and C. M. F. Lapa, “Fuzzy FMEA applied to PWR chemical and volume control system,” *Prog. Nucl. Energy*, vol. 44, no. 3, pp. 191–213, Jan. 2004.

[123] A. C. F. Guimarães and C. M. F. Lapa, “Hazard and operability study using approximate reasoning in light-water reactors passive systems,” *Nucl. Eng. Des.*, vol. 236, no. 12, pp. 1256–1263, Jun. 2006.

[124] A. C. F. Guimarães and C. M. Franklin Lapa, “Effects analysis fuzzy inference system in nuclear problems using approximate reasoning,” *Ann. Nucl. Energy*, vol. 31, no. 1, pp. 107–115, Jan. 2004.

[125] R. K. Sharma, D. Kumar, and P. Kumar, “Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling,” *Int. J. Qual. Reliab. Manag.*, vol. 22, no. 9, pp. 986–1004, 2005.

[126] K. Xu, L. . Tang, M. Xie, S. . Ho, and M. . Zhu, “Fuzzy assessment of FMEA for engine systems,” *Reliab. Eng. Syst. Saf.*, vol. 75, no. 1, pp. 17–29, Jan. 2002.

[127] T. L. Jee, K. M. Tay, and C. P. Lim, “A New Two-Stage Fuzzy Inference System-Based Approach to Prioritize Failures in Failure Mode and Effect Analysis,” *IEEE Trans. Reliab.*, vol. 64, no. 3, pp. 869–877, Sep. 2015.

[128] H. Gargama and S. K. Chaturvedi, “Criticality assessment models for failure mode effects and criticality analysis using fuzzy logic,” *IEEE Trans. Reliab.*, vol. 60, no. 1, pp. 102–110, 2011.

[129] G. A. Keskin and C. Özkan, “An alternative evaluation of FMEA: Fuzzy ART algorithm,” *Qual. Reliab. Eng. Int.*, vol. 25, no. 6, pp. 647–661, Oct. 2009.

[130] Z. Zhang and X. Chu, “Risk prioritization in failure mode and effects analysis under uncertainty,” *Expert Syst. Appl.*, vol. 38, no. 1, pp. 206–214, 2011.

[131] H. Zhang, Y. Dong, I. Palomares-Carrascosa, and H. Zhou, “Failure mode and effect analysis in a linguistic context: A consensus-based multiattribute group decision-making approach,” *IEEE Trans. Reliab.*, vol. 68, no. 2, pp. 566–582, 2019.

[132] C.-T. Chen, “Extensions of the TOPSIS for group decision-making under fuzzy environment,” *Fuzzy Sets Syst.*, vol. 114, no. 1, pp. 1–9, Aug. 2000.

[133] M. Braglia, M. Frosolini, and R. Montanari, “Fuzzy TOPSIS Approach for Failure Mode, Effects and Criticality Analysis,” *Qual. Reliab. Eng. Int.*, vol. 19, no. 5, pp. 425–443, 2003.

[134] M. Mangeli, A. Shahraki, and F. H. Saljooghi, “Improvement of risk assessment in the FMEA using nonlinear model, revised fuzzy TOPSIS, and support vector machine,” *Int. J. Ind. Ergon.*, vol. 69, no. December 2018, pp. 209–216, 2019.

[135] M. Braglia, “MAFMA: multi-attribute failure mode analysis,” *Int. J. Qual. Reliab. Manag.*, vol. 17, no. 9, pp. 1017–1033, Dec. 2000.

[136] J. Li, H. Fang, and W. Song, “Failure Mode and Effects Analysis Using Variable Precision Rough Set Theory and TODIM Method,” *IEEE Trans. Reliab.*, vol. 68, no. 4, pp. 1242–1256, Dec. 2019.

[137] Z. Wang, J.-M. Gao, R.-X. Wang, K. Chen, Z.-Y. Gao, and W. Zheng, “Failure Mode and Effects Analysis by Using the House of Reliability-Based Rough VIKOR Approach,” *IEEE Trans. Reliab.*, vol. 67, no. 1, pp. 230–248, Mar. 2018.

[138] H.-C. Liu, Z. Li, W. Song, and Q. Su, “Failure Mode and Effect Analysis Using Cloud Model Theory and PROMETHEE Method,” *IEEE Trans. Reliab.*, vol. 66, no. 4, pp. 1058–1072, Dec. 2017.

[139] H.-C. Liu, J.-X. You, P. Li, and Q. Su, “Failure Mode and Effect Analysis Under Uncertainty: An Integrated Multiple Criteria Decision Making Approach,” *IEEE Trans. Reliab.*, vol. 65, no. 3, pp. 1380–1392, Sep. 2016.

[140] J. Wu and Q. Cao, “Same families of geometric aggregation operators with intuitionistic trapezoidal fuzzy numbers,” *Appl. Math. Model.*, vol. 37, no. 1–2, pp. 318–327, Jan. 2013.

[141] G. JIANG, H. YUAN, P. LI, and P. LI, “A new approach to fuzzy dynamic fault tree analysis using the weakest n -dimensional t -norm arithmetic,” *Chinese J. Aeronaut.*, vol. 31, no. 7, pp. 1506–1514, Jul. 2018.

[142] F. Dinmohammadi, B. Alkali, M. Shafiee, C. Bérenguer, and A. Labib, “Risk Evaluation of Railway Rolling Stock Failures Using FMECA Technique: A Case Study of Passenger Door System,” *Urban Rail Transit*, vol. 2, no. 3–4, pp. 128–145, Dec. 2016.

[143] P. Liu, X. Cheng, Y. Qin, Y. Zhang, and Z. Xing, “Reliability analysis of metro door system based on fuzzy reasoning petri net,” *Lect. Notes Electr. Eng.*, vol. 288 LNEE, no. VOL. 2, pp. 283–291, 2014.

[144] J. Kim and H. Y. Jeong, “Evaluation of the adequacy of maintenance tasks using the failure consequences of railroad vehicles,” *Reliab. Eng. Syst. Saf.*, vol. 117, pp. 30–39, 2013.

[145] J. Carretero *et al.*, "Applying RCM in large scale systems: a case study with railway networks," *Reliab. Eng. Syst. Saf.*, vol. 82, no. 3, pp. 257–273, Dec. 2003.

[146] Y. Deng, Q. Li, and Y. Lu, "A research on subway physical vulnerability based on network theory and FMECA," *Saf. Sci.*, vol. 80, pp. 127–134, 2015.

[147] F. P. García Márquez, F. Schmid, and J. C. Collado, "A reliability centered approach to remote condition monitoring. A railway points case study," *Reliab. Eng. Syst. Saf.*, vol. 80, no. 1, pp. 33–40, 2003.

[148] Yu-Mei Niu, Yu-Zhu He, Jian-Hong Li, and Xiao-Jun Zhao, "The optimization of RPN criticality analysis method in FMECA," in *2009 International Conference on Apperceiving Computing and Intelligence Analysis*, 2009, pp. 166–170.

[149] International Electrotechnical Commision, "IEC 60812 Failure modes and effects analysis." 2018.

[150] Y. W. Kerk, K. M. Tay, and C. P. Lim, "An Analytical Interval Fuzzy Inference System for Risk Evaluation and Prioritization in Failure Mode and Effect Analysis," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1589–1600, Sep. 2017.

[151] A. Pandey, M. Singh, A. U. Sonawane, and P. S. Rawat, "FMEA Based Risk Assessment of Component Failure Modes in Industrial Radiography," *Int. J. Eng. Trends Technol.*, vol. 39, no. 4, pp. 216–225, Sep. 2016.

[152] S. Broggi *et al.*, "Application of failure mode and effects analysis (FMEA) to pretreatment phases in tomotherapy," *J. Appl. Clin. Med. Phys.*, vol. 14, no. 5, pp. 265–277, Sep. 2013.

[153] A. Jomde *et al.*, "Failure modes effects and criticality analysis of the linear compressor," *Mater. Today Proc.*, vol. 4, no. 9, pp. 10184–10188, 2017.

[154] Z. Bluvband, P. Grabov, and O. Nakar, "Expanded FMEA (EFMEA)," in *Annual Symposium Reliability and Maintainability, 2004 - RAMS*, 2004, pp. 31–36.

[155] Z. Bluvband and P. Grabov, "Failure analysis of FMEA," in *2009 Annual Reliability and Maintainability Symposium*, 2009, pp. 344–347.

[156] Youhu Zhao, Guicui Fu, Bo Wan, and Chun Pei, "An improved cost-based method of Risk Priority Number," in *Proceedings of the IEEE 2012 Prognostics and System Health Management Conference (PHM-2012 Beijing)*, 2012, pp. 1–4.

[157] J. B. Bowles, "The new SAE FMECA standard," pp. 48–53, 2002.

[158] S. Duicu and A.-E. Dumitrascu, "Researches concerning risk assessing using Pareto diagram for design process of technological processes," in *11th WSEAS International conference on Signal processing, computational geometry and artificial vision*, 2011, pp. 189–192.

[159] R. Kent, "Design quality management," *Qual. Manag. Plast. Process.*, pp. 227–262, 2016.

[160] K. O. Kim and M. J. Zuo, "Optimal allocation of reliability improvement target based on the failure risk and improvement cost," *Reliab. Eng. Syst. Saf.*, vol. 180, pp. 104–110, Dec. 2018.

[161] K. O. Kim, Y. Yang, and M. J. Zuo, "A new reliability allocation weight for reducing the occurrence of severe failure effects," *Reliab. Eng. Syst. Saf.*, vol. 117, pp. 81–88, Sep. 2013.

[162] L. Tanghong and X. Gang, "Test and Improvement of Ventilation Cooling System for High-

Speed Train," in *2010 International Conference on Optoelectronics and Image Processing*, 2010, vol. 2, pp. 493–497.

[163] C. F. Bonnett, *Practical Railway Engineering*, Second. IMPERIAL COLLEGE PRESS, 2005.

[164] American Society of Heating Refrigerating and Air-Conditioning Engineers, "Guideline for the Design and Application of Heating , Ventilation and Air Conditioning Equipment for Rail Passenger Vehicles." 2014.

[165] International Organization for Standardization, "Iso 14224- Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment." 2016.

[166] C. D. Griffith and S. Mahadevan, "Inclusion of fatigue effects in human reliability analysis," *Reliab. Eng. Syst. Saf.*, vol. 96, no. 11, pp. 1437–1447, Nov. 2011.

[167] A. Felice, F. & Petrillo, *Human factors and reliability engineering for safety and security in critical infrastructures: decision making, theory, and practice.* 2015.

[168] V. Di Pasquale, S. Miranda, R. Iannone, and S. Riemma, "A Simulator for Human Error Probability Analysis (SHERPA)," *Reliab. Eng. Syst. Saf.*, vol. 139, pp. 17–32, 2015.

[169] V. Di, R. Iannone, S. Miranda, and S. Riemm, "An Overview of Human Reliability Analysis Techniques in Manufacturing Operations," in *Operations Management*, vol. i, no. tourism, InTech, 2013, p. 13.

[170] Erik Hollnagel, *Cognitive Reliability and Error Analysis Method*, First. Elsevier, 1998.

[171] A. Birolini, *Reliability engineering - Theory and Practice*, 8th ed. Springer Berlin Heidelberg, 2017.

[172] S. Qiu *et al.*, "Evaluation of human error probabilities based on classical HRA models : an application to railway systems To cite this version : HAL Id : hal-01149780 Evaluation of human error probabilities based on classical HRA models : an application to railway system," 2015.

[173] J. Reason, "Human error: models and management," *BMJ*, vol. 320, no. 7237, pp. 768–770, Mar. 2000.

[174] J. Rasmussen, "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models," *IEEE Trans. Syst. Man. Cybern.*, vol. SMC-13, no. 3, pp. 257–266, May 1983.

[175] B. Kirwan, *A Guide to Practical Human Reliability Assessment.* Taylor & Francis, 1994.

[176] P. C. Cacciabue, "Modelling and simulation of human behaviour for safety analysis and control of complex systems," *Saf. Sci.*, vol. 28, no. 2, pp. 97–110, 1998.

[177] X. Zheng, M. L. Bolton, C. Daly, and E. Biltekoff, "The development of a next-generation human reliability analysis: Systems analysis for formal pharmaceutical human reliability (SAFPHR)," *Reliab. Eng. Syst. Saf.*, vol. 202, no. March, p. 106927, Oct. 2020.

[178] J. Park, W. Jung, and J. Kim, "Inter-relationships between performance shaping factors for human reliability analysis of nuclear power plants," *Nucl. Eng. Technol.*, vol. 52, no. 1, pp. 87–100, Jan. 2020.

[179] L. Wang, Y. Wang, Y. Chen, X. Pan, and W. Zhang, "Performance shaping factors

dependence assessment through moderating and mediating effect analysis," *Reliab. Eng. Syst. Saf.*, vol. 202, no. February 2019, p. 107034, Oct. 2020.

[180] P. Liu, Y. Qiu, J. Hu, J. Tong, J. Zhao, and Z. Li, "Expert judgments for performance shaping Factors' multiplier design in human reliability analysis," *Reliab. Eng. Syst. Saf.*, vol. 194, no. August 2017, p. 106343, Feb. 2020.

[181] S. Rangra, M. Sallak, W. Schon, and F. Vanderhaegen, "A Graphical Model Based on Performance Shaping Factors for Assessing Human Reliability," *IEEE Trans. Reliab.*, vol. 66, no. 4, pp. 1120–1143, Dec. 2017.

[182] D. Swain and H. E. Guttmann, "Handbook of reliability analysis with emphasis on nuclear plant applications," no. August, 1983.

[183] G. Hannaman, A. Spurgin, and Y. Lukic, *Human cognitive reliability model for PRA analysis.* Palo Alto, CA: Draft Report NUS-4531, EPRI Project RP2170-3. Electric Power and Research Institute, 1984.

[184] D. E. Embrey, P. Humphreys, E. A. Rosa, B. Kirwan, and K. Rea, *SLIM-MAUD: an approach to assessing human error probabilities using structured expert judgment. Volume I. Overview of SLIM-MAUD.* NUREG/CR-3518-Vol.1, 1984.

[185] J. C. Williams, "HEART- A proposed method for achieving high reliability in process operation by means of human factors engineering technology," in *Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society*, 1985, pp. 5/1-5/15.

[186] B. Kirwan, "The validation of three human reliability quantification techniques — THERP, HEART and JHEDI: Part 1 — technique descriptions and validation issues," *Appl. Ergon.*, vol. 27, no. 6, pp. 359–373, Dec. 1996.

[187] S. Abrishami, N. Khakzad, and S. M. Hosseini, "A data-based comparison of BN-HRA models in assessing human error probability: An offshore evacuation case study," *Reliab. Eng. Syst. Saf.*, vol. 202, no. November 2019, p. 107043, Oct. 2020.

[188] S. E. Cooper *et al.*, "A Technique for Human Error Analysis (ATHEANA): Technical Basis and Methodology Description," no. NUREG/CR--6350; BNL-NUREG--52467, 1996.

[189] NUREG/CR-6883, "The SPAR-H human reliability analysis method," *U.S. Nuclear Regulatory Commission.* U.S. Nuclear Regulatory Commission, 2005.

[190] B. Kirwan, H. Gibson, R. Kennedy, J. Edmunds, G. Cooksley, and I. Umbers, "Nuclear action reliability assessment (NARA): a data-based HRA tool," *Saf. Reliab.*, vol. 25, no. 2, pp. 38–45, 2005.

[191] P. Trucco and M. C. Leva, "A probabilistic cognitive simulator for HRA studies (PROCOS)," *Reliab. Eng. Syst. Saf.*, vol. 92, no. 8, pp. 1117–1130, 2007.

[192] P. H. Woods DD, Roth EM, "Cognitive Environment Simulation: An Artificial Intelligence System for Human Performance Assessment, technical report NUREG-CR-4862," vol. 1987. US Regulatory Commission, Washington DC.

[193] P. C. Cacciabue, F. Decortis, B. Drozdowicz, M. Masson, and J. P. Nordvik, "COSIMO: A Cognitive Simulation Model of Human Decision Making and Behavior in Accident Management of Complex Plants," *IEEE Trans. Syst. Man Cybern.*, vol. 22, no. 5, pp. 1058–

1074, 1992.

[194] K. Corker and B. Smith, “An architecture and model for cognitive engineering simulation analysis - Application to advanced aviation automation,” no. October, 1993.

[195] K. Sasou, K. Takano, S. Yoshimura, K. Haraoka, and M. Kitamura, “Modeling and simulation of operator team behavior in nuclear power plants,” *Adv. Hum. Factors/Ergonomics*, vol. 20, no. C, pp. 415–420, 1995.

[196] X. Zheng, M. L. Bolton, and C. Daly, “Extended SAFPHR (Systems Analysis for Formal Pharmaceutical Human Reliability): Two approaches based on extended CREAM and a comparative analysis,” *Saf. Sci.*, vol. 132, no. August, p. 104944, Dec. 2020.

[197] S. Abrishami, N. Khakzad, S. M. Hosseini, and P. van Gelder, “BN-SLIM: A Bayesian Network methodology for human reliability assessment based on Success Likelihood Index Method (SLIM),” *Reliab. Eng. Syst. Saf.*, vol. 193, no. September 2019, p. 106647, Jan. 2020.

[198] N. J. Ekanem, A. Mosleh, and S.-H. Shen, “Phoenix – A model-based Human Reliability Analysis methodology: Qualitative Analysis Procedure,” *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 301–315, Jan. 2016.

[199] M. Abílio Ramos, E. López Droguett, A. Mosleh, and M. Das Chagas Moura, “A human reliability analysis methodology for oil refineries and petrochemical plants operation: Phoenix-PRO qualitative framework,” *Reliab. Eng. Syst. Saf.*, vol. 193, no. September 2019, p. 106672, Jan. 2020.

[200] N. Vaez and F. Nourai, “RANDAP: An integrated framework for reliability analysis of detailed action plans of combined automatic-operator emergency response taking into account control room operator errors,” *J. Loss Prev. Process Ind.*, vol. 26, no. 6, pp. 1366–1379, Nov. 2013.

[201] M. M. Aliabadi, “Human error analysis in furnace start-up operation using HEART under intuitionistic fuzzy environment,” *J. Loss Prev. Process Ind.*, vol. 69, no. May 2020, p. 104372, Mar. 2021.

[202] M. Zhang, D. Zhang, H. Yao, and K. Zhang, “A probabilistic model of human error assessment for autonomous cargo ships focusing on human–autonomy collaboration,” *Saf. Sci.*, vol. 130, no. May, p. 104838, Oct. 2020.

[203] S. F. Greco, L. Podofillini, and V. N. Dang, “A Bayesian model to treat within-category and crew-to-crew variability in simulator data for Human Reliability Analysis,” *Reliab. Eng. Syst. Saf.*, vol. 206, p. 107309, Feb. 2021.

[204] K. Laumann and M. Rasmussen, “Suggested improvements to the definitions of Standardized Plant Analysis of Risk-Human Reliability Analysis (SPAR-H) performance shaping factors, their levels and multipliers and the nominal tasks,” *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 287–300, Jan. 2016.

[205] J. Liu *et al.*, “A study on assigning performance shaping factors of the SPAR-H method for adequacy human reliability analysis of nuclear power plants,” *Int. J. Ind. Ergon.*, vol. 81, no. September 2020, p. 103051, Jan. 2021.

[206] Z. Wang, S. Zeng, J. Guo, and H. Che, “A Bayesian network for reliability assessment of man-machine phased-mission system considering the phase dependencies of human cognitive error,” *Reliab. Eng. Syst. Saf.*, vol. 207, no. December 2020, p. 107385, Mar. 2021.

[207] D.-H. Ham and J. Park, "Use of a big data analysis technique for extracting HRA data from event investigation reports based on the Safety-II concept," *Reliab. Eng. Syst. Saf.*, vol. 194, no. September 2017, p. 106232, Feb. 2020.

[208] B. Dhillon, *Transportation Systems Reliability and Safety.* 2011.

[209] EN 50126-1, "Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process." CENELEC - European Committee for Electrotechnical Standardization, 2017.

[210] J. Liu, F. Schmid, W. Zheng, and J. Zhu, "Understanding railway operational accidents using network theory," *Reliab. Eng. Syst. Saf.*, vol. 189, no. November 2018, pp. 218–231, Sep. 2019.

[211] F. De Felice and A. Petrillo, *Human factors and reliability engineering for safety and security in critical infrastructures: decision making, theory, and practice.* Springer-Verlag, 2018.

[212] R. L. Boring, *Advances in Human Error, Reliability, Resilience, and Performance*, vol. 589. Cham: Springer International Publishing, 2018.

[213] W. H. Gibson, E. D. Megaw, M. S. Young, and E. Lowe, "A taxonomy of human communication errors and application to railway track maintenance," *Cogn. Technol. Work*, vol. 8, no. 1, pp. 57–66, 2006.

[214] M. Grozdanovic, "Usage of Human Reliability Quantification Methods," *Int. J. Occup. Saf. Ergon.*, vol. 11, no. 2, pp. 153–159, Jan. 2005.

[215] J. Wreathall, D. Bley, E. Roth, J. Multer, and T. Raslear, "Using an integrated process of data and modeling in HRA," *Reliab. Eng. Syst. Saf.*, vol. 83, no. 2, pp. 221–228, 2004.

[216] M. A. Gibson, W. H., Halliday, M.W., Sutton, L., Shelton, J. and Bond, "A Train driving simulator experiment to investigate driver fault diagnosis," in *People and Rail Systems-Human Factors at the Heart of the Railway*, J. R. Wilson, B. Norris, T. Clarke, and A. Mills, Eds. CRC Press, 2007.

[217] B. Kirwan, "Human error identification techniques for risk assessment of high risk systems - Part 1: Review and evaluation of techniques," *Appl. Ergon.*, vol. 29, no. 3, pp. 157–177, 1998.

[218] S. Reinach and A. Viale, "Application of a human error framework to conduct train accident/incident investigations," *Accid. Anal. Prev.*, vol. 38, no. 2, pp. 396–406, Mar. 2006.

[219] U.S. Department of Transportation, "A Comparative Risk Assessment of Remote Control Locomotive Operations versus Conventional Yard Switching Operations." 2006.

[220] F. Vanderhaegen, "A non-probabilistic prospective and retrospective human reliability analysis method — application to railway system," *Reliab. Eng. Syst. Saf.*, vol. 71, no. 1, pp. 1–13, Jan. 2001.

[221] P. C. Cacciabue, "Human error risk management methodology for safety audit of a large railway organisation," in *Applied Ergonomics*, 2005, vol. 36, no. 6 SPEC. ISS., pp. 709–718.

[222] R. Hamer, P. Waterson, and G. T. Jun, "Human factors and nuclear safety since 1970 – A critical review of the past, present and future," *Saf. Sci.*, vol. 133, no. August 2020, p. 105021, Jan. 2021.

[223] M. Porthin, M. Liinasuo, and T. Kling, "Effects of digitalization of nuclear power plant

control rooms on human reliability analysis – A review," *Reliab. Eng. Syst. Saf.*, vol. 194, no. October 2017, p. 106415, Feb. 2020.

[224] J. Tao, D. Qiu, F. Yang, and Z. Duan, "A bibliometric analysis of human reliability research," *J. Clean. Prod.*, vol. 260, p. 121041, Jul. 2020.

[225] R. Patriarca *et al.*, "Human reliability analysis: Exploring the intellectual structure of a research field," *Reliab. Eng. Syst. Saf.*, vol. 203, no. September 2019, p. 107102, Nov. 2020.

[226] L.-X. Hou, R. Liu, H.-C. Liu, and S. Jiang, "Two decades on human reliability analysis: A bibliometric analysis and literature review," *Ann. Nucl. Energy*, vol. 151, p. 107969, Feb. 2021.

[227] J. R. Wilson, "Fundamentals of systems ergonomics/human factors," *Appl. Ergon.*, vol. 45, no. 1, pp. 5–13, Jan. 2014.

[228] M. T. Baysari, A. S. McIntosh, and J. R. Wilson, "Understanding the human factors contribution to railway accidents and incidents in Australia," *Accid. Anal. Prev.*, vol. 40, no. 5, pp. 1750–1757, Sep. 2008.

[229] M. T. Baysari, C. Caponecchia, A. S. McIntosh, and J. R. Wilson, "Classification of errors contributing to rail incidents and accidents: A comparison of two human error identification techniques," *Saf. Sci.*, vol. 47, no. 7, pp. 948–957, Aug. 2009.

[230] E. S. Patterson, "Handoff strategies in settings with high consequences for failure: lessons for health care operations," *Int. J. Qual. Heal. Care*, vol. 16, no. 2, pp. 125–132, Apr. 2004.

[231] X. Gibert, V. M. Patel, and R. Chellappa, "Deep Multitask Learning for Railway Track Inspection," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 1, pp. 153–164, Jan. 2017.

[232] X. Liu, M. R. Saat, and C. P. L. Barkan, "Analysis of Causes of Major Train Derailment and Their Effect on Accident Rates," *Transp. Res. Rec. J. Transp. Res. Board*, vol. 2289, no. 1, pp. 154–163, Jan. 2012.

[233] P. M. Salmon, G. J. M. Read, N. A. Stanton, and M. G. Lenné, "The crash at Kerang: Investigating systemic and psychological factors leading to unintentional non-compliance at rail level crossings," *Accid. Anal. Prev.*, vol. 50, pp. 1278–1288, Jan. 2013.

[234] F. Belmonte, W. Schön, L. Heurley, and R. Capel, "Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway trafficsupervision," *Reliab. Eng. Syst. Saf.*, vol. 96, no. 2, pp. 237–249, Feb. 2011.

[235] E. M. Roth, J. Multer, and T. Raslear, "Shared Situation Awareness as a Contributor to High Reliability Performance in Railroad Operations," *Organ. Stud.*, vol. 27, no. 7, pp. 967–987, Jul. 2006.

[236] H. Gibson, "Railway Action Reliability Assessment user manual - A technique for the quantification of human error in the rail industry," pp. 1–96, 2012.

[237] S. Dindar, S. Kaewunruen, and M. An, "Bayesian network-based human error reliability assessment of derailments," *Reliab. Eng. Syst. Saf.*, vol. 197, no. January, p. 106825, May 2020.

[238] J.-L. Zhou, Y. Lei, and Y. Chen, "A hybrid HEART method to estimate human error probabilities in locomotive driving process," *Reliab. Eng. Syst. Saf.*, vol. 188, no. March, pp.

80–89, Aug. 2019.

[239] J.-L. Zhou and Y. Lei, “A slim integrated with empirical study and network analysis for human error assessment in the railway driving process,” *Reliab. Eng. Syst. Saf.*, vol. 204, no. July, p. 107148, Dec. 2020.

[240] M. Kyriakidis, A. Majumdar, and W. Y. Ochieng, “The human performance railway operational index—a novel approach to assess human performance for railway operations,” *Reliab. Eng. Syst. Saf.*, vol. 170, pp. 226–243, Feb. 2018.

[241] E. C. Wigglesworth, “A human factors commentary on innovations at railroad – highway grade crossings in Australia,” *J. Safety Res.*, vol. 32, pp. 309–321, 2001.

[242] J. Davey, A. Wallace, N. Stenson, and J. Freeman, “The experiences and perceptions of heavy vehicle drivers and train drivers of dangers at railway level crossings,” *Accid. Anal. Prev.*, vol. 40, no. 3, pp. 1217–1222, May 2008.

[243] G. S. Larue and C. Wullems, “Human Factors Evaluation of a Novel Australian Approach for Activating Railway Level Crossings,” *Procedia Manuf.*, vol. 3, no. Ahfe, pp. 3293–3300, 2015.

[244] S. Laapotti, “Comparison of fatal motor vehicle accidents at passive and active railway level crossings in Finland,” *IATSS Res.*, vol. 40, no. 1, pp. 1–6, Jul. 2016.

[245] A. Zaman, B. Ren, and X. Liu, “Artificial Intelligence-Aided Automated Detection of Railroad Trespassing,” *Transp. Res. Rec. J. Transp. Res. Board*, vol. 2673, no. 7, pp. 25–37, Jul. 2019.

[246] C. Chi, T. Chang, and C. Tsou, “In-depth investigation of escalator riding accidents in heavy capacity MRT stations,” *Accid. Anal. Prev.*, vol. 38, no. 4, pp. 662–670, Jul. 2006.

[247] A. Rjabovs and R. Palacin, “The influence of system design-related factors on the safety performance of metro drivers,” *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit*, vol. 231, no. 3, pp. 317–328, Mar. 2017.

[248] C. Poirier, S. Adelé, and J.-M. Burkhardt, “Individual accidents at the interface between platform, train and tracks (PT2I) in the subway: a literature review,” *Cogn. Technol. Work*, vol. 23, no. 2, pp. 203–224, May 2021.

[249] C. Lin, M. Rapik Saat, and C. P. Barkan, “Quantitative causal analysis of mainline passenger train accidents in the United States,” *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit*, vol. 234, no. 8, pp. 869–884, Sep. 2020.

[250] Z. Zhang, T. Turla, and X. Liu, “Analysis of human-factor-caused freight train accidents in the United States,” *J. Transp. Saf. Secur.*, vol. 0, no. 0, pp. 1–29, Dec. 2019.

[251] Z. Zhang and X. Liu, “Safety risk analysis of restricted-speed train accidents in the United States,” *J. Risk Res.*, vol. 23, no. 9, pp. 1158–1176, Sep. 2020.

[252] H.-L. Chang and L.-S. Ju, “Effect of consecutive driving on accident risk: A comparison between passenger and freight train driving,” *Accid. Anal. Prev.*, vol. 40, no. 6, pp. 1844–1849, Nov. 2008.

[253] J.-L. Zhou and Y. Lei, “Paths between latent and active errors: Analysis of 407 railway accidents/incidents’ causes in China,” *Saf. Sci.*, vol. 110, no. December 2017, pp. 47–58, Dec. 2018.

[254] N. Khademi, M. Babaei, J.-D. Schmöcker, and A. Fani, “Analysis of incident costs in a vulnerable sparse rail network – Description and Iran case study,” *Res. Transp. Econ.*, vol. 70, no. September, pp. 9–27, Oct. 2018.

[255] K. Klockner and Y. Toft, “Accident Modelling of Railway Safety Occurrences: The Safety and Failure Event Network (SAFE-Net) Method,” *Procedia Manuf.*, vol. 3, no. Ahfe, pp. 1734–1741, 2015.

[256] Z. Wang, G. Su, M. Skitmore, J. Chen, A. P. C. Chan, and B. Xia, “Human Error Risk Management Methodology for Rail Crack Incidents,” *Urban Rail Transit*, vol. 1, no. 4, pp. 257–265, Dec. 2015.

[257] A. Naweed, M. S. Young, and J. Aitken, “Caught between a rail and a hard place: a two-country meta-analysis of factors that impact Track Worker safety in Lookout-related rail incidents,” *Theor. Issues Ergon. Sci.*, vol. 20, no. 6, pp. 731–762, Nov. 2019.

[258] R. Lawton and N. J. Ward, “A systems analysis of the Ladbroke Grove rail crash,” *Accid. Anal. Prev.*, vol. 37, no. 2, pp. 235–244, Mar. 2005.

[259] M. Kyriakidis, S. Simanjuntak, S. Singh, and A. Majumdar, “The indirect costs assessment of railway incidents and their relationship to human error - The case of Signals Passed at Danger,” *J. Rail Transp. Plan. Manag.*, vol. 9, no. January, pp. 34–45, May 2019.

[260] X. Liu, T. Turla, and Z. Zhang, “Accident-Cause-Specific Risk Analysis of Rail Transport of Hazardous Materials,” *Transp. Res. Rec. J. Transp. Res. Board*, vol. 2672, no. 10, pp. 176–187, Dec. 2018.

[261] H. Ebrahimi, F. Sattari, L. Lefsrud, and R. Macciotta, “Analysis of train derailments and collisions to identify leading causes of loss incidents in rail transport of dangerous goods in Canada,” *J. Loss Prev. Process Ind.*, vol. 72, no. May, p. 104517, Sep. 2021.

[262] G. S. Braut, Ø. Solberg, and O. Njå, “Organizational effects of experience from accidents. Learning in the aftermath of the Tretten and Åsta train accidents,” *Transp. Res. Part A Policy Pract.*, vol. 69, pp. 354–366, Nov. 2014.

[263] C. J. Beale, “Recent railway industry accidents. Learning Points for the Process Industries,” *Trans. Inst. Chem. Eng. Part B*, vol. 80, no. January, pp. 25–32, 2002.

[264] Y. Niwa, “A proposal for a new accident analysis method and its application to a catastrophic railway accident in Japan,” *Cogn. Technol. Work*, vol. 11, no. 3, pp. 187–204, Sep. 2009.

[265] M. Ghazel and E.-M. El-Koursi, “Two-Half-Barrier Level Crossings Versus Four-Half-Barrier Level Crossings: A Comparative Risk Analysis Study,” *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 3, pp. 1123–1133, Jun. 2014.

[266] G. S. Larue, A. Rakotonirainy, and N. L. Haworth, “A simulator evaluation of effects of assistive technologies on driver cognitive load at railway-level crossings,” *J. Transp. Saf. Secur.*, vol. 8, no. sup1, pp. 56–69, Jun. 2016.

[267] F. Senesi, G. Ridolfi, and S. Buonincontri, “The application of the CE regulation 402/13 and the quantitative evaluation of risk to the Italian Railway ‘SSC’ (supporting system for the driver) control command system,” *Int. J. Saf. Secur. Eng.*, vol. 6, no. 2, pp. 394–405, Jun. 2016.

[268] T. Meyers, A. Stambouli, K. McClure, and D. Brod, “Risk Assessment of Positive Train Control by Using Simulation of Rare Events,” *Transp. Res. Rec. J. Transp. Res. Board*, vol.

2289, no. 1, pp. 34–41, Jan. 2012.

[269] X. Chen, A. Guan, X. Qiu, H. Huang, J. Liu, and H. Duan, “Data configurations in railway signalling engineering - an application of enterprise systems techniques,” *Enterp. Inf. Syst.*, vol. 7, no. 3, pp. 354–374, Aug. 2013.

[270] H. Song, T. Shen, and W. Wang, “Train-Centric Communication-Based Close Proximity Driving Train Movement Authority System,” *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 3, pp. 22–34, 2018.

[271] B. Roets, M. Verschelde, and J. Christiaens, “Multi-output efficiency and operational safety: An analysis of railway traffic control centre performance,” *Eur. J. Oper. Res.*, vol. 271, no. 1, pp. 224–237, Nov. 2018.

[272] R. Andreasson, A. A. Jansson, and J. Lindblom, “The coordination between train traffic controllers and train drivers: a distributed cognition perspective on railway,” *Cogn. Technol. Work*, vol. 21, no. 3, pp. 417–443, Aug. 2019.

[273] S. Lei *et al.*, “Cognitive Abilities Predict Safety Performance: A Study Examining High-Speed Railway Dispatchers,” *J. Adv. Transp.*, vol. 2021, pp. 1–10, Jun. 2021.

[274] S. Qiu, M. Sallak, W. Schon, and Z. Cherfi-Boulanger, “Modeling of ERTMS Level 2 as an SoS and Evaluation of its Dependability Parameters Using Statecharts,” *IEEE Syst. J.*, vol. 8, no. 4, pp. 1169–1181, Dec. 2014.

[275] M. Kyriakidis, A. Majumdar, and W. Y. Ochieng, “Data based framework to identify the most significant performance shaping factors in railway operations,” *Saf. Sci.*, vol. 78, pp. 60–76, Oct. 2015.

[276] M. Kyriakidis, V. Kant, S. Amir, and V. N. Dang, “Understanding human performance in sociotechnical systems – Steps towards a generic framework,” *Saf. Sci.*, vol. 107, pp. 202–215, Aug. 2018.

[277] B. Ryan, J. R. Wilson, S. Sharples, G. Morrisroe, and T. Clarke, “Developing a Rail Ergonomics Questionnaire (REQUEST),” *Appl. Ergon.*, vol. 40, no. 2, pp. 216–229, Mar. 2009.

[278] B. Ryan, J. R. Wilson, S. Sharples, and T. Clarke, “Attitudes and opinions of railway signallers and related staff, using the Rail Ergonomics Questionnaire (REQUEST),” *Appl. Ergon.*, vol. 40, no. 2, pp. 230–238, Mar. 2009.

[279] C. Krehl and N. Balfe, “Cognitive workload analysis in rail signalling environments,” *Cogn. Technol. Work*, vol. 16, no. 3, pp. 359–371, Aug. 2014.

[280] L. Pickup, J. R. Wilson, S. Sharpies, B. Norris, T. Clarke, and M. S. Young, “Fundamental examination of mental workload in the rail industry,” *Theor. Issues Ergon. Sci.*, vol. 6, no. 6, pp. 463–482, Nov. 2005.

[281] K. Tripathi and H. Borrion, “Safe, secure or punctual? A simulator study of train driver response to reports of explosives on a metro train,” *Secur. J.*, vol. 29, no. 1, pp. 87–105, Feb. 2016.

[282] N. Brandenburger, A. Naumann, and M. Jipp, “Task-induced fatigue when implementing high grades of railway automation,” *Cogn. Technol. Work*, vol. 23, no. 2, pp. 273–283, May 2021.

[283] T. G. Raslear, J. Gertler, and A. DiFiore, “Work schedules, sleep, fatigue, and accidents in the US railroad industry,” *Fatigue Biomed. Heal. Behav.*, vol. 1, no. 1–2, pp. 99–115, Apr. 2013.

[284] M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, “An enhanced SHERPA (E-SHERPA) method for human reliability analysis in railway engineering,” *Reliab. Eng. Syst. Saf.*, vol. 215, no. February, p. 107866, Nov. 2021.

[285] D. Lee *et al.*, “Sleeping, sleeping environments, and human errors in South Korean male train drivers,” *J. Occup. Health*, vol. 61, no. 5, pp. 358–367, Sep. 2019.

[286] H. J. Jeon *et al.*, “Sleep Quality, Posttraumatic Stress, Depression, and Human Errors in Train Drivers: A Population-Based Nationwide Study in South Korea,” *Sleep*, vol. 37, no. 12, pp. 1969–1975, Dec. 2014.

[287] S. Nayak, S. Tripathy, and A. Dash, “Role of non technical skill in human factor engineering: a crucial safety issue in Indian Railway,” *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, no. 5, pp. 1120–1136, Oct. 2018.

[288] C. Calabrese, B. Mejia, C. A. McInnis, M. France, E. Nadler, and T. G. Raslear, “Time of day effects on railroad roadway worker injury risk,” *J. Safety Res.*, vol. 61, pp. 53–64, Jun. 2017.

[289] R. J. Houghton, C. White, D. Golightly, and J. R. Wilson, “Span of control in supervision of rail track work,” *Cogn. Technol. Work*, vol. 18, no. 2, pp. 361–378, May 2016.

[290] D. Aleksić, M. Marković, M. Vasiljević, G. Stojić, N. Pavlović, and I. Tanackov, “Analysis of impact of meteorological conditions on human factors in estimating the risk of railway accidents,” *Transport*, vol. 33, no. 5, pp. 1–14, Sep. 2017.

[291] N. Balfe, S. Sharples, and J. R. Wilson, “Impact of automation: Measurement of performance, workload and behaviour in a complex control environment,” *Appl. Ergon.*, vol. 47, pp. 52–64, Mar. 2015.

[292] M. SHIGEMORI, T. INOUE, and M. SAWA, “Tasks for Estimating Human Error Tendency,” *Q. Rep. RTRI (railw. Tech. Res. Institute)*, vol. 47, no. 4, pp. 198–204, 2006.

[293] L. Ciani, G. Guidi, G. Patrizi, and D. Galar, “Improving Human Reliability Analysis for railway systems using fuzzy logic,” *IEEE Access*, pp. 1–1, 2021.

[294] M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, “Human error probability estimation for safety and diagnostic systems in railway engineering,” *Meas. Sensors*, vol. 18, p. 100105, Dec. 2021.

[295] C. Hassan, P. Balasubramaniam, A. Raman, N. Mahmood, F. Hung, and N. Sulaiman, “Inclusion of Human Errors Assessment in Failure Frequency Analysis-–A Case Study for the Transportation of Ammonia by Rail in Malaysia,” *Process Saf. Prog.*, vol. 28, no. 1, pp. 60–67, 2009.

[296] S. Singh and R. Kumar, “Evaluation of Human Error Probability of Disc Brake Unit Assembly and Wheel Set Maintenance of Railway Bogie,” *Procedia Manuf.*, vol. 3, no. Ahfe, pp. 3041–3048, 2015.

[297] W. Wang, X. Liu, and Y. Qin, “A modified HEART method with FANP for human error assessment in high-speed railway dispatching tasks,” *Int. J. Ind. Ergon.*, vol. 67, no. December, pp. 242–258, 2018.

[298] W. Wang, X. Liu, and Y. Qin, “A modified HEART method with FANP for human error assessment in high-speed railway dispatching tasks,” *Int. J. Ind. Ergon.*, vol. 67, pp. 242–258, Sep. 2018.

[299] F. Mahdi Rezaie, A. M. Fakoor Saghih, and N. Motahari Farimani, “A novel hybrid approach based on CREAM and fuzzy ANP to evaluate human resource reliability in the urban railway,” *J. Transp. Saf. Secur.*, vol. 0, no. 0, pp. 1–39, Apr. 2020.

[300] M. Marseguerra, E. Zio, and M. Librizzi, “Human reliability analysis by fuzzy ‘CREAM,’” *Risk Anal.*, vol. 27, no. 1, pp. 137–154, 2007.

[301] X. Chen, X. Liu, and Y. Qin, “An extended CREAM model based on analytic network process under the type-2 fuzzy environment for human reliability analysis in the high-speed train operation,” *Qual. Reliab. Eng. Int.*, vol. 37, no. 1, pp. 284–308, Feb. 2021.

[302] Y. Sun, Q. Zhang, Z. Yuan, Y. Gao, and S. Ding, “Quantitative Analysis of Human Error Probability in High-Speed Railway Dispatching Tasks,” *IEEE Access*, vol. 8, pp. 56253–56266, 2020.

[303] Lombardi, “THE MANAGEMENT OF UNCERTAINTY: MODEL FOR EVALUATION OF HUMAN ERROR PROBABILITY IN RAILWAY SYSTEM,” *Am. J. Appl. Sci.*, vol. 11, no. 3, pp. 381–390, Mar. 2014.

[304] D. A. Wiegmann and S. A. Shappell, *A Human Error Approach to Aviation Accident Analysis. The Human Factors Analysis and Classification System.* Routledge, 2003.

[305] C. Li, T. Tang, M. M. Chatzimichailidou, G. T. Jun, and P. Waterson, “A hybrid human and organisational analysis method for railway accidents based on STAMP-HFACS and human information processing,” *Appl. Ergon.*, vol. 79, no. September 2018, pp. 122–142, Sep. 2019.

[306] Q. Zhan, W. Zheng, and B. Zhao, “A hybrid human and organizational analysis method for railway accidents based on HFACS-Railway Accidents (HFACS-RAs),” *Saf. Sci.*, vol. 91, pp. 232–250, Jan. 2017.

[307] L. Punzet, S. Pignata, and J. Rose, “Error types and potential mitigation strategies in Signal Passed at Danger (SPAD) events in an Australian rail organisation,” *Saf. Sci.*, vol. 110, no. June 2017, pp. 89–99, Dec. 2018.

[308] R. Madigan, D. Golightly, and R. Madders, “Application of Human Factors Analysis and Classification System (HFACS) to UK rail safety of the line incidents,” *Accid. Anal. Prev.*, vol. 97, pp. 122–131, Dec. 2016.

[309] H. Gibson, “Railway Action Reliability Assessment user manual - A technique for the quantification of human error in the rail industry.” Rail Safety and Standards Board, pp. 1–96, 2012.

[310] C. Y. Lam and K. Tai, “Network topological approach to modeling accident causations and characteristics: Analysis of railway incidents in Japan,” *Reliab. Eng. Syst. Saf.*, vol. 193, no. September 2019, p. 106626, Jan. 2020.

[311] M. Konstandinidou, Z. Nivolianitou, C. Kiranoudis, and N. Markatos, “A fuzzy modeling application of CREAM methodology for human reliability analysis,” *Reliab. Eng. Syst. Saf.*, vol. 91, no. 6, pp. 706–716, 2006.

[312] A. Rotshtein, L. Pustylnik, and B. A. Polin, “Method of Fuzzy Perfectness in Human Reliability Analysis: Selection of Performance Conditions,” in *Advances in System Reliability Engineering*, Elsevier, 2019, pp. 209–226.

[313] Q. Zhou, Y. D. Wong, H. S. Loh, and K. F. Yuen, “A fuzzy and Bayesian network CREAM model for human reliability analysis – The case of tanker shipping,” *Saf. Sci.*, vol. 105, no. December 2017, pp. 149–157, 2018.

[314] P. cheng Li, G. hua Chen, L. cao Dai, and L. Zhang, “A fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks,” *Saf. Sci.*, vol. 50, no. 7, pp. 1569–1583, 2012.

[315] A. Maniram Kumar, S. Rajakarunakaran, and V. Arumuga Prabhu, “Application of Fuzzy HEART and expert elicitation for quantifying human error probabilities in LPG refuelling station,” *J. Loss Prev. Process Ind.*, vol. 48, pp. 186–198, 2017.

[316] P. Baraldi, L. Podofillini, L. Mkrtchyan, E. Zio, and V. N. Dang, “Comparing the treatment of uncertainty in Bayesian networks and fuzzy expert systems used for a human reliability analysis application,” *Reliab. Eng. Syst. Saf.*, vol. 138, pp. 176–193, 2015.

[317] G. J. Klir and B. Yuan, *Fuzzy sets and fuzzy logic: Theory and applications.* Prentice Hall PTR, 1995.

[318] “Fuzzy numbers and fuzzy arithmetic,” in *Fuzzy Mathematical Programming and Fuzzy Matrix Games*, Berlin/Heidelberg: Springer-Verlag, pp. 39–56.

[319] S. Rezvani and M. Molani, “Representation of trapezoidal fuzzy numbers with shape function,” *Ann. Fuzzy Math. Informatics*, vol. 8, no. 1, pp. 89–112, 2014.

[320] R. Hassanzadeh, I. Mahdavi, N. M. Amiri, and A. Tajdin, “An α-cut approach for fuzzy product and its use in computing solutions of fully fuzzy linear systems,” *Int. J. Math. Oper. Res.*, vol. 12, no. 2, p. 167, 2018.

[321] E. Siahlooei and S. A. Shahzadeh Fazeli, “An Application of Interval Arithmetic for Solving Fully Fuzzy Linear Systems with Trapezoidal Fuzzy Numbers,” *Adv. Fuzzy Syst.*, vol. 2018, pp. 1–10, Jul. 2018.

[322] T. Akther and S. U. Ahmad, “A Computational Method for fuzzy arithmetic operations,” *Daffodil Int. Univ. J. Sci. Technol.*, vol. 4, no. 1, pp. 18–22, 2009.

[323] W. A. Lodwick and E. A. Untiedt, “A comparison of interval analysis using constraint interval arithmetic and fuzzy interval analysis using gradual numbers,” in *NAFIPS 2008 - 2008 Annual Meeting of the North American Fuzzy Information Processing Society*, 2008, pp. 1–6.

[324] M. Rausand, A. Barros, and A. Høyland, *System reliability theory. Models, Statistical Methods, and Applications.*, Third. John Wiley & Sons, Inc., 2021.

[325] L. Ciani and G. Guidi, “Application and analysis of methods for the evaluation of failure rate distribution parameters for avionics components,” *Measurement*, vol. 139, pp. 258–269, Jun. 2019.

[326] R. G. Mair, K. D. Onos, and J. R. Hembrook, “Cognitive Activation by Central Thalamic Stimulation: The Yerkes-Dodson Law Revisited,” *Dose-Response*, vol. 9, no. 3, p. dose-response.1, Jul. 2011.

[327] P. G. Gwyer, “Applying the Yerkes-Dodson Law to Understanding Positive or Negative Emotions,” *Glob J Intellect Dev Disabil*, vol. 3, no. 2, pp. 2–4, 2017.

[328] R. M. Yerkes and J. D. Dodson, “The relation of strength of stimulus to rapidity of habit-formation,” *J. Comp. Neurol. Psychol.*, vol. 18, no. 5, pp. 459–482, Nov. 1908.

[329] B. Allotta, P. D’Adamio, M. Malvezzi, L. Pugi, A. Ridolfi, and G. Vettori, “A localization algorithm for railway vehicles,” in *2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings*, 2015, pp. 681–686.

[330] F. Cuppi, V. Vignali, C. Lantieri, L. Rapagnà, N. Dimola, and T. Galasso, “High density European Rail Traffic Management System (HD-ERTMS) for urban railway nodes: The case study of Rome,” *J. Rail Transp. Plan. Manag.*, vol. 17, p. 100232, Mar. 2021.

Annex A

This annex includes the proof of the Weibull parameters assessment for the calculation of equation (6.4).

Considering the bound of possible HEP values given by the RARA method for each GTT as follow:

$$\mathrm{HEP}_{nominal}=\left[HEP_{\mathrm{n},min};HEP_{\mathrm{n},max}\right] \tag{A.1}$$

Thus, k is set to have the minimum of the curve at t=1 h.

$$\mathrm{HEP}_{nominal}(\mathrm{t})|_{t=1h}=HEP_{\mathrm{n},min} \tag{A.2}$$

Introducing the nominal HEP in eq. (4) into (22):

$$1-k\cdot e^{-\alpha\cdot(1-t)^{\beta}}\Big|_{t=1h}=HEP_{\mathrm{n},min} \tag{A.3}$$

Therefore, for each one of the GTT, the k parameter is given by:

$$\mathrm{k}=1-\mathrm{HEP}_{\mathrm{n,\ min}} \tag{A.4}$$

The parameter α is set considering that the maximum human error probability is reached at the end of the shift (t_{max}).

$$\mathrm{HEP}_{nominal}(\mathrm{t})|_{t=t_{max}}=HEP_{\mathrm{n},max} \tag{A.5}$$

Introducing the nominal HEP in eq. (4) into (25):

$$1-k\cdot e^{-\alpha\cdot(t-1)^{\beta}}\Big|_{t=t_{max}}=HEP_{\mathrm{n},max} \tag{A.6}$$

$$1-k\cdot e^{-\alpha\cdot(t_{max}-1)^{\beta}}=HEP_{\mathrm{n},max} \tag{A.7}$$

$$e^{-\alpha\cdot(t_{max}-1)^{\beta}}=\frac{1-HEP_{n,max}}{k} \tag{A.8}$$

$$-\alpha\cdot(t_{max}-1)^{\beta}=\ln\left(\frac{1-HEP_{n,max}}{k}\right) \tag{A.9}$$

$$\alpha=-\frac{\ln\left(\frac{1-HEP_{n,max}}{k}\right)}{(t_{max}-1)^{\beta}} \tag{A.10}$$

$$\alpha=\frac{\ln\left(\frac{k}{1-HEP_{n,max}}\right)}{(t_{max}-1)^{\beta}} \tag{A.11}$$

List of Original Publication

The research activity of the author has led to several publications in international journals and conferences. These are summarized below.

Bibliometric Indices

The author's bibliometric indices are the following:
H-index = 5,
total number of citations = 104 by 64 documents
source: SCOPUS database on March 16, 2022

International Journals

1. L. Ciani, G. Guidi, “Application and analysis of methods for the evaluation of failure rate distribution parameters for avionics components”, **Measurement**, vol. 139, pp. 258-269, 2019.
2. L. Ciani, G. Guidi, and G. Patrizi, “A Critical Comparison of Alternative Risk Priority Numbers in Failure Modes, Effects, and Criticality Analysis,” **IEEE Access**, vol. 7, pp. 92398–92409, 2019.
3. M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, “Maintainability improvement using allocation methods for railway systems,” **ACTA IMEKO**, vol. 9, no. 1, pp. 10–17, 2020.
4. L. Ciani, A. Bartolini, G. Guidi, and G. Patrizi, “A hybrid tree sensor network for a condition monitoring system to optimise maintenance policy,” **ACTA IMEKO**, vol. 9, no. 1, pp. 3–9, 2020.
5. V. Pazzi et al., “Analysis of the Influence of the GPS Errors Occurred While Collecting Electrode Coordinates on the Electrical Resistivity of Tumuli,” **Sensors**, vol. 20, no. 10, p. 2966, May 2020.

6. L. Ciani, M. Catelani, A. Bartolini, G. Guidi, and G. Patrizi, “Influence of Raised Ambient Temperature on a Sensor Node Using Step-Stress Test,” **IEEE Trans. Instrum. Meas.**, vol. 69, no. 12, pp. 9549–9556, Dec. 2020.

7. L. Ciani et al., “Comparing the Effects of GPS Error on Different Electrical Resistivity Tomography Arrays for Archeological Investigations,” **IEEE Trans. Instrum. Meas.**, vol. 70, Article No. 1001612, 2021.

8. L. Ciani, G. Guidi, G. Patrizi, and D. Galar, “Condition-Based Maintenance of HVAC on a High-Speed Train for Fault Detection,” **Electronics**, vol. 10, no. 12, p. 1418, Jun. 2021.

9. M. Catelani, L. Ciani, D. Galar, G. Guidi, S. Matucci, and G. Patrizi, “FMECA Assessment for Railway Safety-Critical Systems Investigating a New Risk Threshold Method,” **IEEE Access**, vol. 9, pp. 86243–86253, 2021.

10. M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, “An enhanced SHERPA (E-SHERPA) method for human reliability analysis in railway engineering,” **Reliab. Eng. Syst. Saf.**, vol. 215, no. February, Article No. 107866, Nov. 2021.

11. L. Ciani, M. Catelani, A. Bartolini, G. Guidi, and G. Patrizi, “Design optimisation of a wireless sensor node using a temperature-based test plan,” **ACTA IMEKO**, vol. 10, no. 2, pp. 37–45, 2021.

12. M. Catelani, L. Ciani, G. Guidi, G. Patrizi, and D. Galar, “Estimate the useful life for a heating, ventilation, and air conditioning system on a high-speed train using failure models,” **ACTA IMEKO**, vol. 10, no. 3, pp. 100–107, 2021.

13. L. Ciani, G. Guidi, G. Patrizi, and D. Galar, “Improving Human Reliability Analysis for Railway Systems Using Fuzzy Logic,” **IEEE Access**, vol. 9, pp. 128648–128662, 2021.

14. L. Ciani, G. Guidi, and G. Patrizi, “Fuzzy-based approach to solve classical RPN drawbacks for railway signaling systems,” **IEEE Intelligent Transportation System Magazine**, Article in Press, 2021.

15. M. Catelani, L. Ciani, A. Bartolini, C. Del Rio, G. Guidi, G. Patrizi, "Reliability analysis of wireless sensor network for smart farming applications", **Sensors**, vol. 21, no. 22, Article number 7683, 2021.

16. L. Ciani, G. Guidi and G. Patrizi, “Human reliability in railway engineering: Literature review and bibliometric analysis of the last two decades”, Safety Science, Article in Press, 2022.

International Conferences and Workshops

1. M. Catelani, L. Ciani, G. Guidi, and M. Venzi, “Parameter estimation methods for failure rate distributions,” in **14th IMEKO TC10 Workshop on Technical Diagnostics 2016: New Perspectives in Measurements, Tools and Techniques for Systems Reliability, Maintainability and Safety**, pp. 441-445, 2016.

2. L. Ciani, G. Guidi, G. Patrizi, and M. Venzi, “System Maintainability Improvement using Allocation Procedures,” in **2018 IEEE International Systems Engineering Symposium (ISSE)**, Oct. 2018.

3. L. Ciani, A. Bartolini, G. Guidi, and G. Patrizi, “Condition Monitoring of Wind Farm based on Wireless Mesh Network,” in **16th IMEKO TC10 Conference**: “Testing, Diagnostics & Inspection as a comprehensive value chain for Quality & Safety,” 2019, pp. 39–44.

4. V. Pazzi et al., “ERT investigation of tumuli: does the errors in locating electrodes influence the resistivity?,” in **2019 IMEKO TC-4 International Conference on Metrology for Archaeology and Cultural Heritage**, 2019, pp. 527–532.

5. M. Catelani, L. Ciani, A. Bartolini, G. Guidi, and G. Patrizi, “Standby Redundancy for Reliability Improvement of Wireless Sensor Network,” in **2019 IEEE 5th International forum on Research and Technology for Society and Industry (RTSI)**, Sep. 2019, pp. 364–369.

6. L. Ciani, G. Guidi, and G. Patrizi, “Condition-based Maintenance for Oil&Gas system basing on Failure Modes and Effects Analysis,” in **2019 IEEE 5th International forum on Research and Technology for Society and Industry (RTSI)**, Sep. 2019, pp. 85–90.

7. L. Ciani, M. Catelani, A. Bartolini, G. Guidi, and G. Patrizi, “Electrical characterization of a monitoring system for precision farming under temperature stress,” in **24th IMEKO TC4 International Symposium and 22nd International Workshop on ADC and DAC Modelling and Testing**, 2020, pp. 270–275.

8. V. Pazzi et al., “Evaluation of the GPS errors influence on the resistivity in ERT investigation of funeral mounds,” in **EGU General Assembly**, 2020

9. M. Catelani, L. Ciani, A. Bartolini, G. Guidi, and G. Patrizi, “Characterization of a low-cost and low-power environmental monitoring system,” in **2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)**, May 2020, pp. 1–6.

10. M. Catelani, L. Ciani, G. Guidi, and D. Galar, “A Practical Solution for HVAC Life Estimation Using Failure Models,” **17th IMEKO TC 10 and EUROLAB Virtual Conference “Global Trends in Testing, Diagnostics & Inspection for 2030”,** 2020.

11. L. Ciani, G. Guidi, and D. Galar, "Reliability evaluation of an HVAC ventilation system with FTA and RBD analysis," **6th IEEE international symposium on systems engineering (ISSE)**, Oct. 2020.
12. M. Catelani et al., "Effects of inaccurate electrode positioning in subsurface resistivity measurements for archeological purposes," in **2021 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)**, May 2021.
13. M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, "Accelerated Testing and Reliability estimation of electronic boards for automotive applications," in **2021 IEEE International Workshop on Metrology for Automotive (MetroAutomotive)**, Jul. 2021, pp. 199–204.
14. L. Ciani et al., "Effect of Pulses Distribution in a Buck Converter Controlled with Pulse Skipping Modulation," in **2021 IEEE 15th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG)**, Jul. 2021, pp. 1–6.
15. M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, "Human error probability estimation for safety and diagnostic systems in railway engineering," **Meas. Sensors, Proc. Of the IMEKO XXIII World congress (IMEKO2021)**, Vol. 18, p. 100105, Dec. 2021.
16. M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, "Reliability Analysis of Diagnostic System for Condition Monitoring of Industrial Plant", **2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI)**, September 6-9, 2021
17. M. Catelani, L. Ciani, G. Guidi, and G. Patrizi, "Reliability Allocation: an iterative approach for complex systems", **2021 IEEE International Symposium on Systems Engineering (ISSE)**, September 2021

National Journals

1. M. Catelani, L. Ciani, G. Guidi, G. Patrizi, "Introduzione alla logica Fuzzy nell'analisi FMECA", **Tutto_Misure**, anno XXII, N. 01, 2020.
2. M. Catelani, L. Ciani, G. Guidi, G. Patrizi, "Applicazione della logica Fuzzy all'analisi FMECA", **Tutto_Misure**, anno XXII, N. 02, 2020.

National Conferences

1. M. Catelani, L. Ciani, G. Guidi, “Valutazione di affidabilità di un sistema di ventilazione HVAC tramite analisi RBD”, Atti del **XXXVI Congresso nazionale di misure elettriche ed elettroniche GMEE**, 12-14 Settembre 2019, Perugia, Italia.

2. M. Catelani, L. Ciani, A. Bartolini, G. Guidi, G. Patrizi, “Analisi in temperatura di un nodo sensore mediante test stress a gradino”, Atti del **XXXVII Congresso nazionale di misure elettriche ed elettroniche GMEE**, 10-12 Settembre 2020.

3. M. Catelani et al., “Effetti dell’errato posizionamento degli elettrodi nelle misure di resistività del terreno per la ricerca di tumuli etruschi”, Atti del **XXXVII Congresso nazionale di misure elettriche ed elettroniche GMEE**, 10-12 Settembre 2020.

4. M. Catelani et al. “Influenza della qualità dei dati di tomografia elettrica sui risultati d’inversione della resistività per applicazioni archeologiche”, Atti del **XXXVIII Congresso nazionale di misure elettriche ed elettroniche GMEE**, 16-18 Settembre 2021.