Springer Series in Reliability Engineering

Fabio De Felice
Antonella Petrillo *Editors*

Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures

Decision Making, Theory, and Practice

Springer

Springer Series in Reliability Engineering

Series editor
Hoang Pham
Piscataway, New Jersey, USA

More information about this series at http://www.springer.com/series/6917

Fabio De Felice • Antonella Petrillo
Editors

Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures

Decision Making, Theory, and Practice

Springer

Editors
Fabio De Felice
Department of Civil and Mechanical Engineering
University of Cassino and Southern Lazio
Cassino (FR), Italy

Antonella Petrillo
Department of Engineering
University of Napoli "Parthenope"
Napoli (NA), Italy

ISSN 1614-7839 ISSN 2196-999X (electronic)
Springer Series in Reliability Engineering
ISBN 978-3-319-62318-4 ISBN 978-3-319-62319-1 (eBook)
https://doi.org/10.1007/978-3-319-62319-1

Library of Congress Control Number: 2017951128

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Accidents continue to be the major concern in "*critical infrastructures*," and human factors have been proved to be the prime causes of accidents. Clearly, human dynamics are a challenging management function to guarantee reliability, safety, and cost reduction in critical infrastructures.

In this context, concepts of human error and reliability are integrated and complementary to each other. Based on our experience, we believe that both of them are vital to ensure a proper incident and accidental scenario management. In this book, we decided to focus on *human behavior* in order to recognize its potential involvement in system failure.

The book collects a high-quality selection of contemporary research and case studies on the complexity resulting from human/reliability management in industrial plants and critical infrastructures.

Thus, the book intends to analyze globally the problem regarding the human and reliability management to reduce human errors as much as possible and to ensure safety and security in critical infrastructures.

Intentionally, the book focuses more on applications rather than theoretical aspects as it aims to be an useful tool in disaster management.

The book is composed of nine chapters. Chapter "The importance of human Error and reliability management in critical conditions and infrastructures" aims to introduce the importance of the topic presenting various disasters that have occurred in critical infrastructures related to human errors or lack of reliability of systems. Chapter "An overview on human error analysis and reliability assessment" tries to respond to these questions: *What is HRA*? and What are the main features of the most well-known HRA methods? Chapter "Mathematical models for reliability allocation and optimization for complex systems" analyzes several reliability allocation techniques present in the literature. Starting from well-known methodologies, two reliability allocation methods have been proposed and validated. Chapter "Integrated engineering approach to safety, reliability, risk management and human factors" presents an integrated framework for analyzing engineering systems, operational procedures, and the human factors based on the application of

systems theory. An application example assessing safety, reliability, risk, and human factor issues related to a complex task of nondestructive inspection of piping segments of a primary circuit of an NPP shows the benefits of using the proposed integrated approach. Chapter "A fuzzy modeling application for human reliability analysis in the process industry" proposes a fuzzy modeling application for human reliability analysis in the process industry. Chapter "Prevention of human factors and Reliability analysis in operating of sipping device on IPR-R1 TRIGA reactor, a study case" describes the application of the "*what-if*" technique for assessing risk and reliability in sipping test operations, including an analysis to identify human error and equipment failure modes. Chapter "Human factors challenges in disaster management scenario" presents a hybrid model for human error probability analysis to investigate and to monitor the human factors in industrial plant through KPI indicators. Chapter "Use of Bayesian network for Human Reliability Modelling: possible benefits and an example of application" reports an action research project applied to the relationship of task and cognitive workload support on one of the most important aspects of an airport: ground handling. Finally, Chapter "A methodology to support decision making and effective Human Reliability methods in Aviation Safety" describes a methodology aimed at practical and straightforward implementations of risk assessment processes and able to tackle real problems. The application process might be used as guideline for the analysis of critical activities resulting from retrospective and prospective assessments of operational environments.

The book is enriched by figures, examples, and case studies.

The main benefit of the book is to look at case studies and the important areas of human and reliability management. The book is a timely publication and will be a valuable source of reference for those with responsibility for disaster and emergency planning according to the principles of reliability and human management.

We hope our readers will enjoy the book and will find it both interesting and useful.

As Editors of this book, we very much thank the authors accepting to contribute with their invaluable research and for their efforts, time, and precious works. Our special thanks to *Dr. Anthony Doyle*, the Executive Editor, and *Mr. Ravi Vengadachalam*, the Project coordinator, for their precious support and their team for this opportunity.

Napoli, Italy
April 2017

Fabio De Felice
Antonella Petrillo

Contents

The Importance of Human Error and Reliability Management in Critical Conditions and Infrastructures

Antonella Petrillo and Federico Zomparelli

Abstract Protection and safeguarding of critical infrastructures (such us chemical industry, oil & gas industry, nuclear industry, etc.) is an important subject of study in the contemporary society. The study of risks associated to critical infrastructure required models of good practice to investigate the complexity of processes in case of accidents. The risk management can be viewed in two ways: *human error* and *system reliability*. In other words in terms of human error it is essential to ensure the operator performance to manage a complex system or an unexpected situation. While in terms of system reliability it is essential to ensure that a system is at least as reliable as the system it is replacing. The present chapter aims to analyze the main disasters occurred in critical infrastructures related to human errors or lack of reliability of systems.

Keywords Human error • Reliability • Disaster • Critical infrastructures • Statistic analysis

1 Introduction

Over the past years, technological developments have led to a decrease of accidents due to technical failures through the use of redundancy and protection (Holla 2011). However, the "*human factor*" contributes significantly in accident dynamics, both statistically and in terms of severity of consequences. In fact, estimates agree that the errors committed by man are causes over 60% of accidents and for the remaining part the causes are due to technical deficiencies (Holla 2016).

The industrial accidents became a dangerous phenomenon as the enormous impact on the health of workers and on the economy in general.

A. Petrillo (✉)
University of Napoli "Parthenope", Naples, Italy
e-mail: antonella.petrillo@uniparthenope.it

F. Zomparelli
University of Cassino and Southern Lazio, Cassino, Italy
e-mail: f.zomparelli@unicas.it

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_1

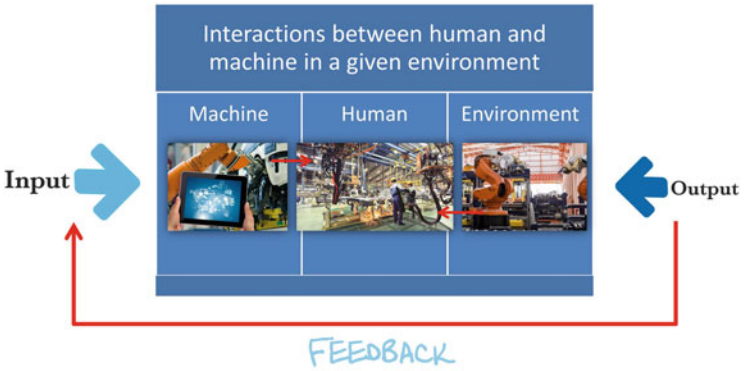


Fig. 1 Interactions between human and machine in a given environment (author's elaboration)

Major accidents in industrial establishments have negative consequences at internal and external level as stated by Suffo and Nebot (2016). A debate is taking place among academic researchers and risk management experts, about how best to protect critical infrastructures (Schulman et al. 2004).

The safety and the right management of industrial plants is the result of the interaction of a wide array of factors (Jenkins et al. 2010). The origin of industrial accidents is to be found in environmental, organisational and human factors. In particular, it is not possible to separate the human from the technology factors. High reliability has become a process that is achieved across organisations.

Figure 1 shows the interaction between humans and machines, both elements are indispensable.

Both of them are subject to errors. It is meaningful to identify relationships between them (Zhou et al. 2017). During a disaster may occur certain conditions under which humans are more likely to make errors (e.g. lack of time, stress, overload, etc.). Human error can be linked to various features of people and the operating environment (De Felice et al. 2016). In other words, human errors are a natural part of human behavior (Hovanec 2017).

Human error analysis is a priority to avoid disaster and to increase human performance as well as to engineer design of systems (Burke et al. 2002). In fact, thousands of deaths occur each year due to accidents in critical infrastructures.

The industry started to investigate the influence of various disasters over time and to perform meaningful analyses relative to understanding the risk and the role humans play in those analyses (Spurgin 2010). Of course, in each analysis, it is important to understand what influences could play a part in the possibility of an accident.

The rest of this chapter traces the general principles of national and international legislation in field of critical infrastructures. Moreover, a statistical analysis of disaster in the world is presented and Main historical disasters occurred in the world are described. Finally, conclusions and considerations are analyzed.

2 Foundations of National and International Legislation

The protection of critical infrastructure is considered a principal objective in any country. All Governments, normally defines studies and plan precautionary measures to reduce the risk. The first who have developed a Critical Infrastructure Protection System was the United States of America in 1996, but also the European Union has developed a research activities.

During risk analysis it is necessary to analyze the possible causes of accidents: machine failure, human error and natural disasters. Critical infrastructure management requires the innovative approaches to develop effective emergency procedures. In this section, the main European and Italian legislature relating to critical infrastructure is analyzed and a mapping of the Italian critical systems is realized (Bigley and Roberts 2001).

Legislation on industrial safety was born due to the numerous industrial accidents. Safety practices have been developed from regulating agencies (e.g., Occupational Safety and Health Administration OSHA) and many lessons have been learned from previous industrial accidents (Wallace 2016).

In particular the Seveso disaster in Italy, but also other disasters in European countries, have pushed the legislators to regulate safety in industrial plants. The first European directive is **1982/501/EC** "**Seveso**". The Seveso Directive aims at the prevention of major accidents involving dangerous substances.

The continuous evolution of industrial plants has led to the development of a new Directive **1996/82 /EC** "**Seveso II**" on the control of major-accident hazards involving dangerous substances. The third Directive **2012/18/EU** "**Seveso III**" modifies the regulations relating to industrial risks. Legislation applies to all establishments where there are dangerous substances.

The Directive covers establishments where dangerous substances may be present. Furthermore, defines hazardous substances: *toxic substances*; *flammable substances*; *explosive substances*; *oxidising substances*; and *substances dangerous for the environment*.

Depending on the amount of dangerous substances present, establishments are categorised in lower and upper tier establishments, the latter are subject to more stringent requirements.

Another important directive is the European Directive **2008/114/EC** on *the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* defines the identification of European critical infrastructures. The criteria that considers the Directive are:

- Loss of human lives;
- Economic effects (disruption);
- Public effect (psychological impacts).

The directive takes into account the aspect of the impact assessment and through a Plan–Do–Check–Act (PDCA) cycle develops continuous improvement actions.

The ECI (European Critical Infrastructures) on the basis of Directive 114/08 defines two areas classified as critical infrastructure: transport and energy.

The Ministry of environment annually updates the map of critical industries on the Italian territory. Sectors that fall in this analysis are:

- chemical and petrochemical plants;
- gas deposits;
- oil refining;
- oil deposits;
- deposits drugs;
- chemical deposits;
- production/deposit explosives;
- distillation;
- power plants;
- steel plants;
- treatment plants.

There are many infrastructure with significant risk in the Italian territory.

Figure 2 shows Italian infrastructures distribution (year 2013).

Figure 3 describes Italian critical infrastructure classified by sectors.

Table 1 shows the number (year 2015) of critical plants with significant risk on the Italian territory. It is possible to note that most of them are located in North Italy (Piemonte, Lombardia and Emilia Romagna).

While, Fig. 4 shows the distribution of Nuclear power plants in Europe. Map highlights that most of them are in France and in Germany.

3 Statistical Analysis of Disaster in the World

Disasters are destructions affecting communities. Represent the primary issues to public health. The emergency destabilizes the social system. The disaster is an event, concentrated in time and space, from which a company suffers serious damage. Disasters are classified as:

– *Natural disaster* is a sudden and severe disruption of nature that causes destruction in communities. Hydrogeological disasters, earthquakes, the volcanic eruptions, etc.
– *The man-made disasters* are produced by human activity, including include those technological or industrial accidents, buildings collapse, transport accidents, but also from fire disasters, terrorist attacks, wars, terrorism and bioterrorism.

In the last decades database have been developed in different countries to record emergency situations. Table 2 shows a list of the major available databases.

In Europe a well-known data base is the *Major Accident Reporting System* (MARS and later renamed eMARS) that was first established by the EU's Seveso

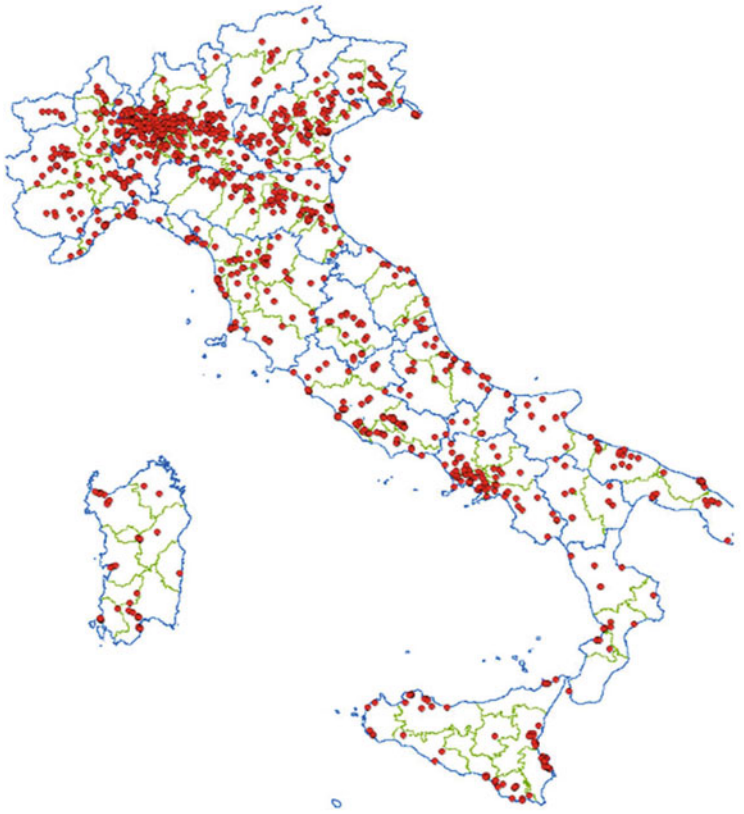


Fig. 2 Distribution of critical plants (source ISPRA http://www.isprambiente.gov.it/it)

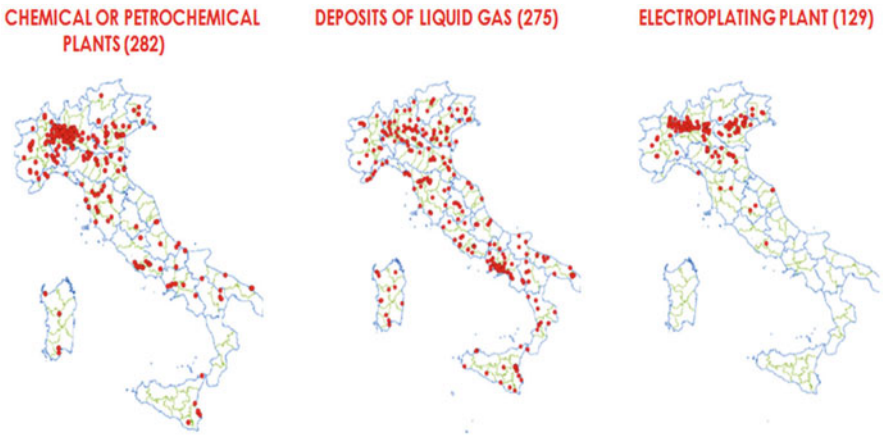


Fig. 3 Distribution of critical plants classified for sectors (source ISPRA—http://www.isprambiente.gov.it/it)

Table 1 Industrial plant with significant risk—2015

District	Industrial plant	%
Abruzzo	26	2.4
Basilicata	9	0.8
Calabria	17	1.6
Campania	70	6.4
Emilia Romagna	92	8.4
Friuli Venezia Giulia	30	2.7
Lazio	63	5.7
Liguria	32	2.9
Lombardia	285	26.0
Marche	16	1.5
Molise	8	0.7
Piemonte	102	9.3
Puglia	33	3.0
Sardegna	45	4.1
Sicilia	67	6.1
Toscana	59	5.4
Trentino Alto Adige	15	1.4
Umbria	17	1.6
Valle D'Aosta	6	0.5
Veneto	104	9.5
Tot. Italy	1096	100.0

Directive 82/501/EEC in 1982 and has remained in place with subsequent revisions to the **Seveso Directive** in effect today.

The purpose of the eMARS is to facilitate the exchange of lessons learned from accidents and near misses involving dangerous substances in order to improve chemical accident prevention and mitigation of potential consequences. MARS contains reports of chemical accidents and near misses provided to the Major Accident and Hazards Bureau (MAHB) of the European Commission's Joint Research Centre from EU, OECD and UNECE countries (under the TEIA Convention).

Reporting an event into eMARS is compulsory for EU Member States. For non-EU OECD and UNECE countries reporting accidents to the eMARS database is voluntary.

Table 3 describes year, number of events and type of event for chemical and petrochemical plants.

Data show that most of the incidents occurred in 2011 and in 2012. The main cause of the accident is due to release of toxic substances (48%).

More in detail, Fig. 5 shows a 10-year overview for petrochemical sector according to the classification type of events that has happened in European union and are recorded in eMARS database.

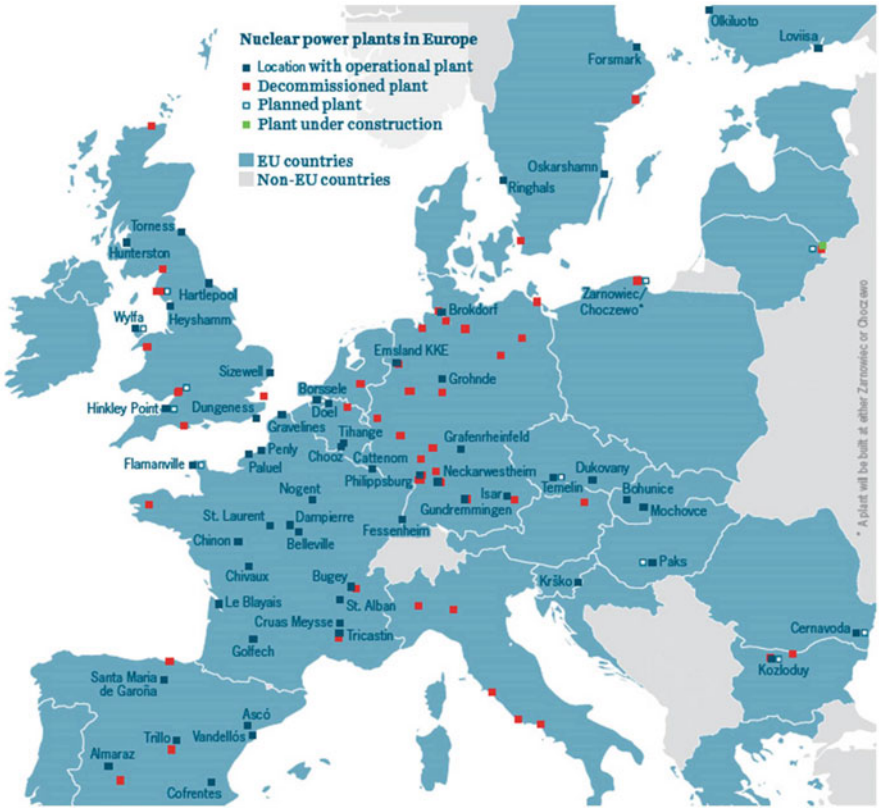


Fig. 4 Nuclear power plants in Europe (source www.wingas.com)

Another most important and significant source useful to monitor the emergency events is the database EM-DAT (http://www.emdat.be/). The database is a potential tool to investigate industrial accidents and disaster events worldwide.

From EM-DAT database it is possible to analyze the trend of disaster occurred in the world. Figure 6 shows the number of industrial disaster per Continent and per Europe. It is evident that most of them occurred over the last 20 years.

While, Fig. 7 shows the total number of industrial accident in the world. Figure 5 highlights that 2004 was the most critical year because 81 disasters occurred.

Figure 8 highlights the number of total deaths per Continent.

By analyzing the trend it is evident that 2002 caused many victims in the world (12.44,000).

Table 2 International database—emergency

Data base	Acronym	Agency	Scope
Major Hazard Incident Data Service	MHIDAS	HSE AEA Technology (UK)	International
Environmental Incident Database Service	EnvIDAS	HSE AEA Technology (UK)	International
OECD Database of Industrial Accidents	OECD	World Health Organization (WHO)	International
Major Accident Reporting System	MARS	European Commission (MAHB)	Europe union
Emergency Response Notification System	ERNS	US Environmental Protection Agency (EPA)	USA
Acute Hazardous Events Data Base	AHE	US EPA	USA
Australian System for Hazardous Materials Incident Reporting	ASHMIR	National Occupation al Health & Safety Commission	Australia
Awareness and preparedness for emergencies at Local Level	APELL	United nations Environment Programme (UNEP)	International
United Nations Economic Commission for Europe	UN/ECE	United Nations Economic Commission for Europe	Europe union
Database for accidents with Hazardous Materials	FACTS	Institute of Environmental and Emergency Technology	Netherland
Accidental release information program	ARIP	Environmental Protection Agency (EPA)	USA
Chemical Incident Reports Center	CIRC	Chemical Safety and Hazard Investigation Board	USA
Incident Reporting Information System	IRIS	National Response Center (NRC)	USA
Process Safety Incident Database	PSID	Center for Chemical Process Safety of the AIChe	USA
Analysis Research and Information Accidents	ARIA	French Ministry of Ecology, Sustainable Development and Energy	France
Emergency Events Database (EM-DAT)	EM-DAT	Centre for Research on the Epidemiology of Disasters—CRED	Belgium

4 Main Historical Disasters Occurred in the World

In recent years several accidents in critical systems have occurred. Among the major disasters occur worldwide in industrial plant we would like to mention some of them.

One of the memorable disaster was at the **London Beer Flood**, an incident that occurred in 1814 in London (Fig. 9). A large tank containing half a million liters of beer broke. Beer was sparse on the street causing damage and deaths. The accident is due to the lack of maintenance of the barrels for a human error. The accident caused nine deaths (Leyland 2014).

Table 3 Incident statistical eMARS 2010–2016 for chemical installation and petrochemical plant (source https://emars.jrc.ec.europa.eu/)

Year	n° events	Industry type	Event type
2016	0	/	/
2015	1	Petrochemical plant	Release of toxic substances
2014	2	Chemical installation	Fire
		Petrochemical plant	Fire
2013	7	Chemical installation	Release of toxic substances
		Chemical installation	Fire
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Fire
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Fire
		Chemical installation	Explosion
2012	12	Chemical installation	Explosion
		Chemical installation	Explosion
		Chemical installation	Release of toxic substances
		Chemical installation	Explosion
		Chemical installation	Release of toxic substances
		Chemical installation	Release of toxic substances
		Chemical installation	Release of toxic substances
		Chemical installation	Fire
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Fire
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Fire
2011	12	Chemical installation	Explosion
		Chemical installation	Release of toxic substances
		Chemical installation	Release of toxic substances
		Chemical installation	Fire
		Chemical installation	Explosion
		Chemical installation	Release of toxic substances
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Explosion
		Chemical installation	Release of toxic substances
		Chemical installation	Release of toxic substances
		Chemical installation	Release of toxic substances
2010	11	Chemical installation	Explosion and fire
		Chemical installation	Explosion and fire
		Chemical installation	Release of toxic substances
		Chemical installation	Explosion
		Petrochemical plant	Fire
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Explosion
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Release of toxic substances
		Petrochemical plant	Bursting of a high-pressure steam pipe
		Petrochemical plant	Fire

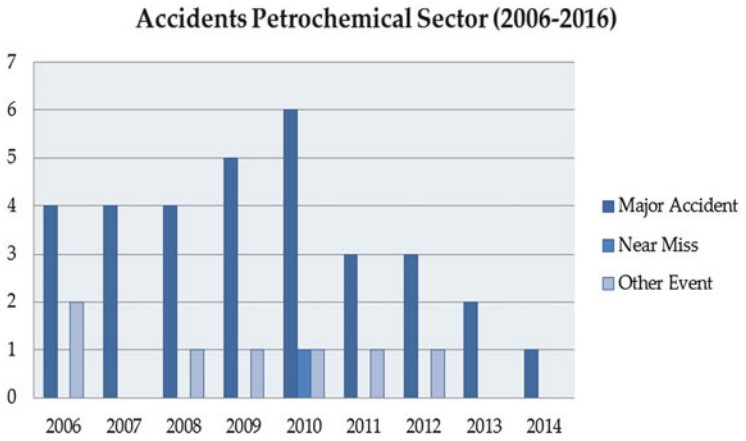


Fig. 5 Events types in eMARS 2006–2016 (source https://emars.jrc.ec.europa.eu/)

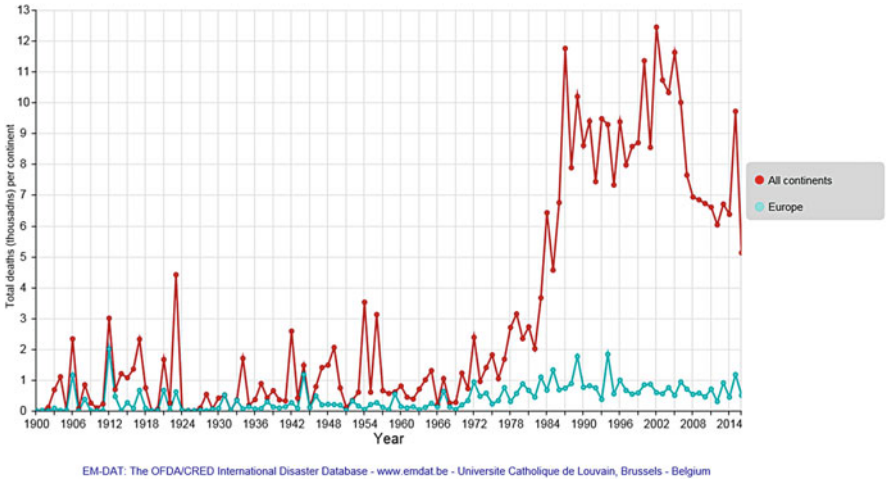


Fig. 6 Number of industrial disaster per Continent and in Europe from 1900 to 2016 (source http://emdat.be/)

The **Seveso disaster** occurred in 1976. Chemical company generated a toxic cloud of dioxin. Probably the cause of accident was human error (Fig. 10). Toxic cloud struck several countries. There were no deaths, but 240 people became ill with clorane a disease of the skin due to the toxic cloud. Flora and fauna was severely affected (Bertazzi 1991).

The **Bhopal disast**er occurred in India in 1984 (Fig. 11), due to the escape of 40 tons of toxic gas. This incident is the most serious chemical disaster in history (Eckerman 2005). The cause of accident is human error, which led to the deaths of some 15,000 people. About 4000 people were disabled due to the incident.

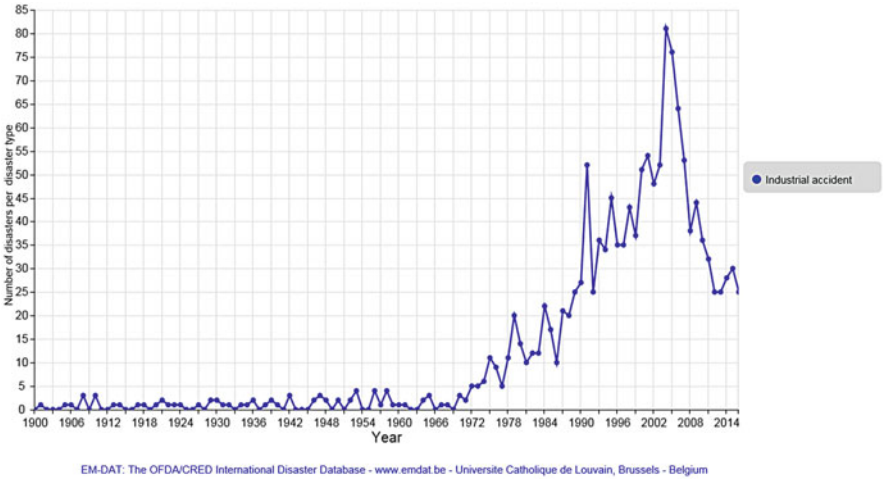


Fig. 7 Number of industrial accident in the world from 1900 to 2016 (source http://emdat.be/)

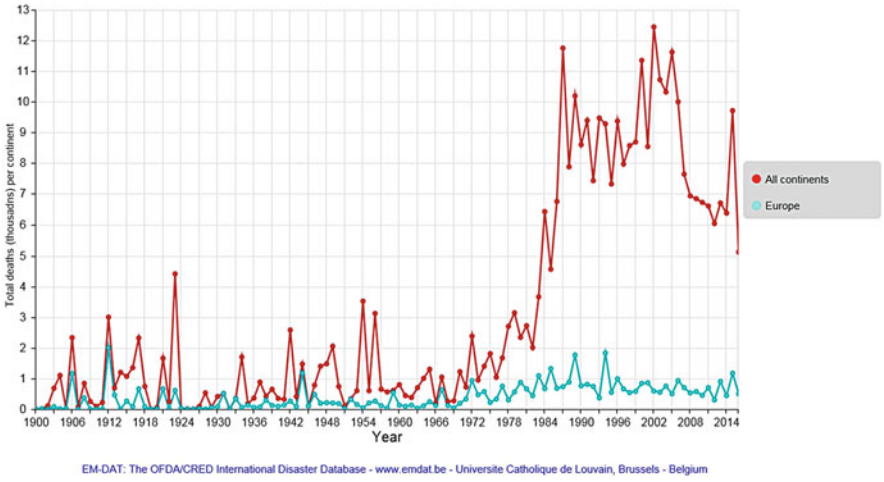


Fig. 8 Total deaths per Continent from 1900 to 2016 (source http://emdat.be/)

Chernobyl disaster was the worst accident at a nuclear plant (Fig. 12). The disaster occurred in 1986 in Ukraine. Causes of the accident are related to system design. During a test the reactor temperature increased and the pipes exploded. This has produced an explosion, and a huge fire (Wheatley et al. 2017).

Radioactive cloud expanded throughout Europe and it arrived up in North America. 336,000 people living near the plant were evacuated.

Some of data disaster:

- 31 dead during the incident;
- 6000 cases of thyroid cancer (Fig. 8);

Fig. 9 Street after the accident

Fig. 10 ICMESA company

- 500,000 workers involved;
- 1.8 million hectares of land contaminated ;
- 336,000 people evacuated.

Fig. 11 Chemical plant

Fig. 12 Chernobyl disaster

Buncefield disaster (2005), is an explosion in a fuel depot, which caused the most severe fire in England after the war (Fig. 13). 43 people were injured. More than 150 operators were involved in rescue operations (Bond 2006).

Fig. 13 Disaster of Buncefield

The **Tallmansville disaster** (2006) is an explosion which has rocked wells and tunnels in the Sago mine, tapping 13 miners of whom 12 have died due to carbon monoxide. 15 people were dead. Rescue teams had to proceed with caution, continually testing for hazards such as water seeps, explosive gas concentrations, and unsafe roof conditions (Dao 2006).

The accident at the aluminum factory in **Ajka** (Hungary) occurred in 2010. A vast pool of sludge broke, flooding the neighboring countries with industrial sludge. The cause of the accident is caused due to human error. The chemical components contained in the sludge exterminate all life in the rivers (Enserink 2010).

Data emerging from this disaster are:

- 8 deaths;
- 90 people hospitalized for chemical burns;
- 40 km^2 area affected by the flood.

Fukushima disaster in 2011 is related to an explosion in a nuclear reactor (Fig. 14) because of a tsunami (Brumfiel 2012). After the explosion radioactive substances are leaking. The accident caused a natural disaster, with the contamination of water. The maintenance costs are around one billion dollars and 170,000 people were evacuated from their homes (Echavarri et al. 2013).

The **Qingdao disaster** (2013), is an incident occurred while several workers were trying to repair a leak in the pipes owned by Sinopec, the largest Chinese oil company (Fig. 15). 52 people were dead and 166 people were injured. Rescue operations were difficult even because of the heavy rain. After explosion, 18,000 people were evacuated from Qingdao (Zhang et al. 2015).

Fig. 14 Nuclear plant after the accident

Savar disaster (2013) is a building collapsed (Fig. 16). The structure housed several textile factories in Bangladesh, who built clothes for western companies. 233 people were dead and 700 people were injured. Rescuers immediately had saved 2500 people but there were many missing. Many hours were needed to extinguish the flames (Alamgir et al. 2014).

A review of accident scenarios showed that they were more likely to occur, and the consequences are significant. It is evident that as much information is possible to obtain as better is possible to manage an accident scenario. It could be useful to keep in mind some precepts that can help to analyse an accident. The most important precepts are: (1) Ensure adequate training of the plant personnel; (2) Design features of control rooms; (3) Define role and responsibility and (4) Analyze possible "environment" under which the accident can take place.

Definitively, a proper accident management must to use as much information from the accident related to the influences that could condition the responses of the personnel and of the systems.

In fact, for instance, the Chernobyl Accident was caused by the necessity to conduct an experiment within a fixed time, leading to high stress in the operators and behaviour.

Fig. 15 Disaster of Qingdao

Fig. 16 Disaster of Savar

5 Conclusions

Accidents continue to be the major concern in the industry, and human factors have been proved to be the prime causes to accidents. Clearly, human dynamics in reliability and maintainability are a challenging management function to guarantee reliability, safety and costs reduction in industrial plants. Prevention represents one of the basic pillars of preventing the crisis phenomena in the current society. In this chapter we have examined the importance of human error and reliability management in critical conditions and infrastructures through the analysis of foundations of National and international legislation. Furthermore, main historical disaster were analyzed.

References

Alamgir M, Parvin R, Haque Khan MA (2014) Tragedy in Savar: management of victims in Enam Medical College Hospital. J Enam Med Coll 4(1):31–35
Bertazzi PA (1991) Long-term effects of chemical disasters. Lessons and results from Seveso. Sci Total Environ 106(1–2):5–20
Bigley GA, Roberts KH (2001) The incident command system: high-reliability organizing for complex and volatile task environments. Acad Manag J 44(6):1281–1299
Bond S (2006) Questions still unanswered in Buncefield probe. Edie Daily. Oct 2009
Brumfiel G (2012) PRINT—FUKUSHIMA. Nature 485(7399):423–424
Burke MJ, Sarpy SA, Tesluk PE, Smith-Crowe K (2002) General safety performance: a test of a grounded theoretical model. Pers Psychol 55:429–457
Dao J (2006) 12 miners found alive 41 hours after explosion. nytimes.com. Accessed 27 May 2016
De Felice F, Petrillo A, Zomparelli F (2016) A hybrid model for human error probability analysis. IFAC-PapersOnLine 49(12):1673–1678
Echavarri L et al (2013) The Fukushima Daiichi nuclear power plant accident, 2013. Nuclear Energy Agency No.7161
Eckerman I (2005) The Bhopal Saga—causes and consequences of the world's largest industrial disaster. Universities Press, India
Enserink M (2010) After red mud flood, scientists try to halt wave of fear and rumors. Science 330 (6003):432–433
Holla K (2011) Risk assessment in accident prevention considering uncertainty and human factor influence. In: Tsvetkov P (ed) Nuclear power—control, reliability and human factors. InTech. doi: 10.5772/17228
Holla K (2016) Major industrial accidents prevention in European union and in Slovak Republic context. Int J Environ Sci 1:19–27
Hovanec M (2017) Digital factory as a prerequisite for successful application in the area of ergonomics and human factor. Theor Issues in Ergon Sci 18(1):35–45
Jenkins DP, Salmon PM, Stanton NA, Walker GH (2010) A new approach for designing cognitive artefacts to support disaster management. Ergonomics 53(5):617–635
Leyland S (2014) The great beer flood of London. In: A curious guide to London. Random House. ISBN 978-0-593-07323-0
Schulman P, Roenn E, van Eetennnn M, de Bruijnennnn M (2004) High reliability and the management of critical infrastructures. J Conting Crisis Manag 12(1):14–28
Spurgin AJ (2010) Human reliability assessment: theory and practice. Taylor and Francis Group, New York
Suffo M, Nebot E (2016) Proximity as an integral factor in the evaluation of the territorial risk under the European Seveso Directive: application in Andalusia (South Spain). Process Saf Environ Prot 99:137–148
Wallace JC (2016) Creating a safety conscious organization and workforce. Organ Dyn 45:305–312
Wheatley S, Sovacool B, Sornette D (2017) Of disasters and dragon kings: a statistical analysis of nuclear power incidents and accidents. Risk Anal 37(1):99–115
Zhang Z, Zhang X, Xu Z, Yao H, Li G, Liu X (2015) Emergency countermeasures against marine disasters in Qingdao City on the basis of scenario analysis. Nat Hazard 75(Suppl 2):233–255
Zhou T, Wu C, Zhang J, Zhang D (2017) Incorporating CREAM and MCS into fault tree analysis of LNG carrier spill accidents. Saf Sci 96:183–191

Antonella Petrillo, degree in Mechanical Engineering, PhD at the University of Cassino and Southern Lazio. Now Professor at University of Naples "Parthenope" (Department of Engineering) where she conducts research activities on Multi-criteria decision analysis (MCDA), Industrial Plant, Disaster Management, Logistic and Safety.

Federico Zomparelli, degree in Management Engineering at University of Cassino and Southern Lazio. Now, he is a PhD student in Mechanical Engineering at the University of Cassino and Southern Lazio. His research activity is focused on MCDA, lean management, risk analysis and industrial plant optimization.

An Overview on Human Error Analysis and Reliability Assessment

Fabio De Felice and Antonella Petrillo

Abstract There is a continuous debate about the proper role of man and machine in complex operational frameworks. Formal human analyses and risk management techniques are becoming more important part to manage the relationship between human factors and accident analyses. There are different types of Human Reliability Analysis (HRA) models. HRA methods differ in their characteristics but a common feature in all methods is the definition of the human error probability (HEP). The aim of this chapter is not to cover all of the possible HRA approaches and above not from a mathematical point of view but conceptual one. In fact, no one approach can answer all of the separate issues that can arise in human reliability. The utility of a particular approach is a function of a number of components, not just the absolute value of a method. Expert judgment is an integral part of HRA to capture information about human actions. Definitively, the aim of this chapter is twofold. It tries to respond to these questions: *What is HRA?* and *What are the main features of the most well-known HRA methods?*

Keywords HRA • HEP • Performance shaping factors • Methods • Errors

1 Introduction

The Human Reliability Analysis (HRA) was born 50 years old in nuclear field, where a human error can generate an accidents with serious consequences (French et al. 2011). Over the past years, technological innovations developments decrease accidents due to technical failures. However, it is impossible to talk about reliability of a system without consider the failure rate of all its components. One of those components is "*man*", whose rate of failure/error goes to change the rate of

F. De Felice (✉)
University of Cassino and Southern Lazio, Cassino, Italy
e-mail: defelice@unicas.it

A. Petrillo
University of Napoli "Parthenope", Napoli, Italy
e-mail: antonella.petrillo@uniparthenope.it

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_2

breakdowns of components with which it can interact (De Felice et al. 2012). The vast majority of current catastrophes arises by a combination of many small events, system faults and human errors that would be irrelevant individually, but when they are combined can lead emergency situations. For this reason, wrong and inappropriate human actions create safety problems. Human factor contributes in dynamic accidents. Errors committed by man are cause of 60–70% of accidents (Hollnagel 1993). Accidents are the most obvious human errors in industrial systems, but minor faults can seriously reduce operation performance in terms of productivity and efficiency (Kirwan 1994). Human reliability analysis consider an interdisciplinary fields: reliability personnel, engineers, human factors specialists and psychologists. There is not a method in literature can be considered the best, because each one has advantages and disadvantages. The standard definition of HRA is the probability that a person will perform according to the requirements of task for a specified period of time and not perform any extraneous activity that can degrade the system. The recommended practice for conducting HRA is based upon the IEEE Standard 1082, "*IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Systems*" (1997). Figure 1 shows the human reliability assessment process according to IEEE STS 1082.

In response to ever changing market needs, there was a diffusion of technologically advanced plants that can provide flexibility and timeliness in production (Watson 1985). The use of those advanced technologies, beside managerial advantages, has led to reliability issues specifically intended as the probability that a system fulfill assigned mission. To this reliability concept are closely related risk and workers safety that may be directly and indirectly affected by processes. It has been observed that system failures due to human intervention are not negligible; in particular, some sources report that human error is cause of failure systems with, in many cases, disastrous consequences. Fortunately, in recent years, technological advances have shifted human intervention from a direct commitment to simple manual control of automatic process of machines.

Over the years several methodologies for human reliability analysis have been made. This development has led researchers to analyze accurately information to order to understand what could be the best approach for HRA. Developed methodologies can be distinguished into **three macro-categories:** *first, second and third generation methods* (Adhikari et al. 2008).

First generation methods include 35–40 methods for human reliability, many of which are variations on a single method. Theoretical basis which relates most of first-generation methods are:

- error classification method according to the concept "omission-commission";
- definition of "performance shaping factors" (PFS);
- cognitive model: skill-based, rule-based, knowledge-based.

First generation approaches tend to be atomistic in nature; they encourage the evaluator to break a task into component parts and then consider the potential impact of modifying factors such as time pressure, equipment design and stress. These methods focus on the skill and rule base level of human action and are often

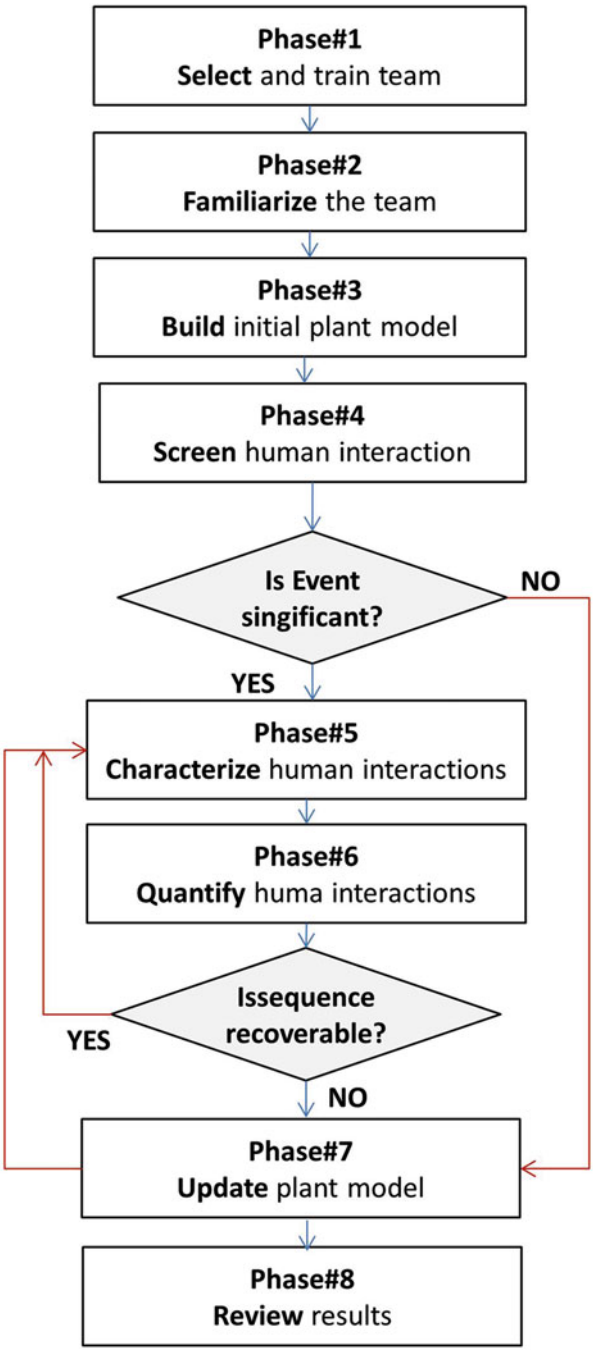


Fig. 1 Human reliability assessment process (IEEE STS 1082 1997)

criticised for failing to consider such things as the impact of context, organisational factors and errors of commission. Despite these criticisms they are useful and many are in regular use for quantitative risk assessments (Bell and Holroyd 2009).

Second generation methods, term coined by Dougherty (1990) try to overcome limitations of traditional methods, in particular:

- provide guidance on possible and probable decision paths followed by operator, using mental processes models provided by cognitive psychology;
- extend errors description beyond usual binary classification (omission-commission), recognizing importance of so-called "cognitive errors";
- consider dynamic aspects of human-machine interaction and can be used as basis for simulators development of operator performance.

In recent years, the limitations and shortcomings of the second generation methods have led to development *emerging third generation* methodologies, that we will categorize not chronologically but considering their characteristics and applicability.

Much of the discussion about methods and effects is in the context of a nuclear plant; however, many of the methods apply to other industries.

2 HRA: First Generation Methods

First generation methods have been developed to help risk evaluators predict and quantify the human error (Hollnagel 2000). First generation encourage the evaluator to break a task into component parts and then consider the potential impact of modifying factors such as time pressure, equipment design and stress (De Felice et al. 2013). First generation methods focus on skill and rule base level of human action and are often criticised for failing to consider such things as impact of context, organisational factors and errors of commission. Despite these criticisms they are useful and many are in regular use for quantitative risk assessments. First generation techniques work on the basis of the simple dichotomy of "*fits*/*doesn't* fit" in the matching of error situation in context with related error identification and quantification and second generation techniques are more theory based in their assessment and quantification of errors. HRA techniques have been utilised in a range of industries including healthcare, engineering, nuclear, transportation and business sector.

In the following paragraphs the main methods have been analyzed.

2.1 Operator Action Tree (OAT)

Operator Action Tree (OAT) was developed by John Wreathall in early 1980s (Wreatall 1982). The OAT approach to HRA is based on the premise that the

response to an event can be described as consisting of three stages: observing or noting the event; diagnosing or thinking about it; responding to it. OAT identifies three types of purely *cognitive errors*:

- failure to perceive that there was an accident;
- failure to diagnose nature of incident and identify actions required to remedy it;
- error in temporal evaluation of correct behavior implementation.

OAT methodology considers the probability of failure in diagnosing an event, i.e., the classical case of response or non-response.

Estimation of failure probability is closely related to the nominal interval of time required to make a decision when an anomaly is detected. This interval can be written formally by Eq. (1):

$$T = t_1 - t_2 - t_3 \tag{1}$$

where:

- T represents required time to make decision;
- t1 represents interval time between the beginning of incident and the end of actions that are related;
- t2 represents time between start of incident and planning of mind intervention;
- t3 represents required time to implement what is planned (t_2).

Because of this, OAT cannot be said to provide an adequate treatment of human erroneous actions. However, it differs from the majority of first generation methodology for HRA by maintaining a distinction among three phases of response: observation, diagnosis and response. This amounts to a simple process model and acknowledges that response is based on a development that includes various activities by operator (Senders et al. 1985). It allows for mis-interpretation by the operator at various key stages in the execution of a task. There are two significant aspects. The first is the limited time which the operator has to carry out the task. The OAT method has a time failure (or non-response) probability relationship. The second is that the operator can take various decision paths and the assessor can determine whether they are key or not. All paths but one lead to failure then they can be grouped together. However if for example failure to diagnose the event correctly could lead to inappropriate action (as evidence indicates has happened since operators often do not follow standard procedures) then the OAT representation should reflect this. Although the OAT representation shown does not show recovery action, it may be appropriate also to allow for this key extension of the tree. The OAT representation potentially is capable of modelling human performance reliability with high levels of problem solving requirement.

2.2 Technique for Human Error Rate Prediction (THERP)

Technique for Human Error Rate Prediction (THERP) began already in 1961. It was developed in the Sandia Laboratories for the US Nuclear Regulatory Commission (Hollnagel 2005). This is a first generation methodology which means that its procedures follow the way conventional reliability analysis models a machine. THERP is probably the best known of first-generation HRA methods. The aim of this methodology is to calculate the probability of successful performance of necessary activities for realization of a task. THERP involves performing a task analysis to provide a description of performance characteristics of human tasks being analysed. Results are represented graphically in an HRA event tree, which is a formal representation of required actions sequence (Kirwan 1996). THERP relies on a large human reliability database containing HEPs (Human Error Probabilities) which is based upon both plant data and expert judgments. This technique was the first approach in HRA to come into broad use and is still widely used in a range of applications even beyond its original nuclear setting. The THERP approach is based on the results of a task analysis, which breaks a task into a number of subtasks.

The basic tool is an event tree for the analysis of human reliability as shown in Fig. 2.

Each node is relative to one of the prefigured actions, the sequence of which is represented from top to bottom. Each node has two branches: the branch to the left marked with the lowercase letter indicates success, the branch to the right marked with uppercase letter indicates the failure (each action is identified by letters in alphabetical order, with the exception of capital letters S and F, used to indicate success and bankruptcy respectively).

Once the qualitative part and the event tree is completed, the quantification consists in associating a nominal human error probability with each tree node.

The main work on THERP was done during 1970s, resulting in the so-called THERP handbook "*Handbook of Human Reliability Analysis with Emphasis on*

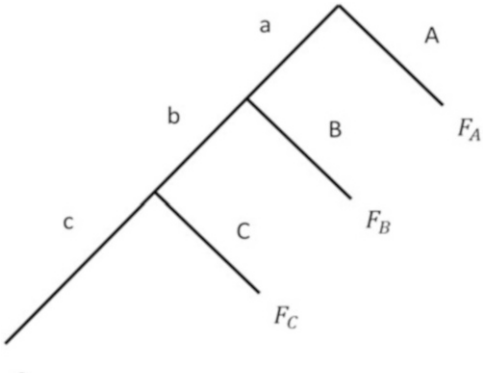


Fig. 2 Example of HRA event tree

Nuclear Power Plant Applications" (Swain and Guttman 1983) that provides also a large number of nominal probability values, grouped into 27 tables.

The methodology consists of the following six steps:

- Define the system failures of interest. These failures include functions of the system in which human error has a greater likelihood of influencing the probability of a fault, and those which are of interest to the risk assessor;
- Identify, list and analyze related human operations performed and their relationship to system tasks and function of interest. This stage of process necessitates a comprehensive task and human error analysis;
- Task analysis lists and sequences the discrete elements and information required by task operators. For each step of task, possible occurring errors which may transpire are considered by analyst and precisely defined. An event tree visually displays all events which occur within a system. The event tree thus shows a number of different paths each of which has an associated end state or consequence;
- Estimate relevant human error probabilities; Estimate the effects of human error on the system failure events. With the completion of the HRA the human contribution to failure can then be assessed in comparison with the results of the overall reliability analysis;
- Recommend changes to the system and recalculate the system failure probabilities. Once the human factor contribution is known, sensitivity analysis can be used to identify how certain risks may be improved in the reduction of HEPs. Error recovery paths may be incorporated into the event tree as this will aid the assessor when considering the possible approaches by which the identified errors can be reduced. Review consequences of proposed changes with respect to availability, reliability and cost-benefit. THERP is probably the best known of first-generation HRA methods. This methodology in complete than other because describes both how events should be modelled and how they should be quantified. Dominance of HRA event tree, however, means that classification scheme and model necessarily remain limited, since event tree can only account for binary choices (success-failure);
- Final feature of THERP is the use of performance shaping factors to complement task analysis. The use of this technique to account for non-specific influences is found in most first-generation HRA methods. The separate use of performance shaping factor is relevant for an evaluation of operator model, since it suggests that the model by itself is context independent.

2.3 Success Likelihood Index Method (SLIM)

Success Likelihood Index Method (SLIM) is a technique used in the field of human reliability Assessment (HRA), for evaluate the human error probability occurring throughout the completion of a specific task (Embrey et al. 1984). From such analyses measures can then be taken to reduce the likelihood of errors occurring

within a system and therefore lead to an improvement in the overall levels of safety. There exist three primary reasons for conducting an HRA:

– error identification;
– error quantification;
– error reduction.

As there exist a number of techniques used for such purposes, they can be split into one of two classifications: first generation techniques and second generation techniques. SLIM is a decision-analytic approach to HRA which uses expert judgement to quantify performance shaping factors (PSFs). PSFs concern the individuals, environment or task, which have the potential to either positively or negatively affect performance e.g. available task time. Such factors are used to derive a Success Likelihood Index (SLI), a form of preference index, which is calibrated against existing data to derive a final human error probability (HEP). The PSF's which require to be considered are chosen by experts and are namely those factors which are regarded as most significant in relation to the context in question. The technique consists of two modules: MAUD (multi-attribute utility decomposition) which scales the relative success likelihood in performing a range of tasks, given the PSFs probable to affect human performance; and SARAH (Systematic Approach to the Reliability Assessment of Humans) which calibrates these success scores with tasks with known HEP values.

From expert judgment and derived values for SLI indices, human error probability conversions (HEPs) are performed by using logarithmic relationships at constant coefficients, as shown in the following Eq. (2):

$$\log(HEP) = a \cdot SLI + b \tag{2}$$

Where a and b are constants; a and b are calculated from the SLIs of two tasks where the HEP has already been established.

2.4 *Systematic Human Action Reliability Procedure (SHARP)*

SHARP methodology can be employed by the analyst as guidance to make assessments of human reliability, suitable for use in a PSA. Different techniques can be used within the SHARP framework. Innovation can be employed when current techniques are deemed insufficient for adequately addressing the case under study. The model is developed in different steps (Hannaman and Spurgin 1984):

– Step#1: Definition to ensure that all human interactions are adequately considered in the study;
– Step#2:Screening to identify the human interactions that are significant to the operation and safety of the plant;

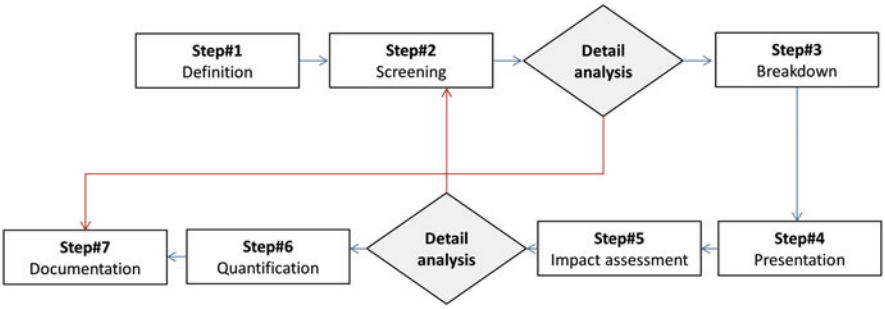


Fig. 3 Flowchart representing the SHARP procedure

- Step#3: Breakdown to develop a detailed description of important human interactions by defining the key influence factors necessary to complete the modelling. Human interaction modelling consists of a representation, impact assessments and quantification;
- Step#4: Representation to select and apply techniques for modelling important human interactions in the logic structures. Such methods help to identify additional significant human actions that might impact system logic trees;
- Step#5: Impact assessment to explore impact of significant human actions identified in the preceding step on the system logic trees;
- Step#6: Quantification to apply appropriate data or other quantification methods to assign probabilities for various interactions examined, determine sensitivities and establish uncertainty ranges;
- Step#7: documentation to include all necessart information for getting a traceable, understandable and reproducible assessment.

Each of the steps outlined above provides input (input) values, rules, and returning outputs.

Figure 3 shows a Flowchart representing the SHARP procedure.

2.5 Empirical Technique to Estimate Operator's Error (TESEO)

Empirical technique to estimate operator's error (TESEO) was developed in 1980 (Bello and Columbari 1980). The methodology is relatively straightforward and is easy to use but is also limited; it is useful for quick overview HRA assessments as opposed to those which are highly detailed and in-depth. Within the field of HRA, there is a lack of theoretical foundation of the technique as is widely acknowledged throughout. This technique is used in HRA to evaluate human error probability occurring throughout the completion of a specific task. From such analyses measures can then be taken to reduce likelihood of errors occurring within a system and therefore lead to an improvement in overall levels of safety. TESEO method

determines human error probability (HEP) through the product of five factors, each featuring an aspect of system as shown in Eq. (3).

$$HEP = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \cdot K_5 \tag{3}$$

Where:

- **K1**: type of task to be executed;
- **K2**: time available to the operator to complete the task;
- **K3**: operator's level of experience/characteristics;
- **K4**: operator's state of mind;
- **K5**: prevalent environmental and ergonomic conditions.

The five factors represent quantified PSFs in different situations (see Table 1).

TESEO technique is typically quick and straightforward in comparison to other HRA tools, not only in producing a final result, but also in sensitivity analysis e.g. it is useful in identifying the effects improvements in human factors will have on the overall human reliability of a task. It is widely applicable to various control room designs or with procedures with varying characteristics (Humphreys 1995).

2.6 Human Cognitive Reliability (HCR)

HCR is a cognitive modeling approach to HRA developed in 1984 (Hannaman et al. 1984). The method uses Rasmussen's idea of rule-based, skill-based, and knowledge-based decision making to determine likelihood of failing a given task (Rasmussen 1983), as well as considering the PSFs of operator experience, stress and interface quality. The database underpinning this methodology was originally developed through the use of nuclear power-plant simulations due to a requirement for a method by which nuclear operating reliability could be quantified. The basis for HCR approach is actually a normalized time-reliability curve, where shape is determined by dominant cognitive process associated with task being performed. HCR method can be described as having the following step:

- Identify actions that must be analyzed by HRA using task analysis method;
- Classify types of cognitive processing required by actions;
- Determine median response time of a crew to perform required tasks;
- Adjust median response time to account for performance influencing factors. This is done by means of the PSF coefficients K_1 (operator experience), K_2 (stress level) and K_3 (quality of operator/plant interface) given in the literature and using the following formula, Eq. (4):

$$T(1/2) = T^*(1/2)(1 + K_1)(1 + K_2)(1 + K_3) \tag{4}$$

Table 1 Flowchart representing the SHARP procedure

Factor	Description	Detail		Value
K1	Activity's typological factor	Sample, routine		0.001
		Requiring attention, routine		0.01
		Not routine		0.1
K2	Time available	Routine activities	>20 s	0.5
			>10 s	1
			>2 s	10
		Non-routine activities	>60 s	0.1
			>45 s	0.3
			>30 s	1
			>3 s	10
K3	Operator's qualities	Carefully selected, expert, well trained		0.5
		Average knowledge and training		1
		Little knowledge, poorly trained		3
K4	State of anxiety	Situation of grave emergency		3
		Situation of potential emergency		2
		Normal situation		1
K5	Environmental ergonomic factor	Excellent microclimate, excellent interface with plant		0.7
		Good microclimate, good interface with plant		1
		Discrete microclimate, discrete interface with plant		3
		Discrete microclimate, poor interface with plant		7
		Worse microclimate, poor interface with plant		11

K coefficients are experimentally calculated; values obtained for these coefficients and the criteria for their choice are shown in the Table 2.

HCR is probably the first-generation HRA approach that most explicitly refers to a cognitive model. Since it was developed, the treatment of human erroneous actions in HCR remains on the same level as in many other first-generation methods, i.e., a basic distinction between success and failure and in this case also no-response. The three modes of decision-making, knowledge-based, skill-based and rule-based are all modelled (see Fig. 4). In contrast, some disadvantages are: the rules for judging Knowledge-based, Skill-based and Rule-based behavior are not exhaustive. Assigning the wrong behavior to a task can mean differences of up to two orders of magnitude in the HEP.

The method is very sensitive to changes in the estimate of the median time. Therefore, this estimate must be very accurate, otherwise the estimation in the HEP will suffer as a consequence; as the HCR correlation was originally developed for use within the nuclear industry, it is not immediately applicable to situations out-with this domain.

Table 2 PSFs and corresponding correction factors in HCR

i	PSF	Description	Detail	K_i
1	Training	Advanced	Qualified personnel with more than 5 years of experience	−0.22
		Good	Qualified personnel with more than 6 months of experience	0.00
		Initial	Personale qualificato con meno di 6 mesi di esperienza	0.44
2	State of stress	Situation of grave emergency	Great stress; Emergency with staff under pressure	0.44
		Heavy workload And/or potential emergency	Average situation; High potential workload required	0.28
		Normal situation	Staff is committed to making small adjustments and interventions	0.00
		Low stress	Staff must face a sudden emergency	0.28
3	Quality of the plant	Excellent	Advanced tools are available to assist staff in emergencies	−0.22
		Good	Information is well organized and integrated	0.00
		Sufficient	Staff must integrate the information	0.44
		Poor	Information not sufficient	0.78
		Very poor	Information poor	0.92

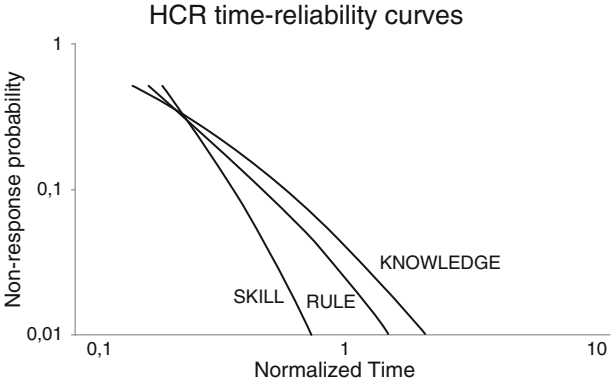


Fig. 4 Non-response probability according to HCR model

2.7 Human Error Assessment and Reduction Technique (HEART)

HEART technique is based on the ergonomics literature, and it uses a set of basic error probabilities modified by the assessor by structured PSFs considerations. HEART is one of the most popular techniques currently used in the United Kingdom (Kirwan 1996).

Table 3 Generic task

N°	Generic task	Limitations of unreliability (%)	k (t=1)	k (t=8)	α	β
1	Totally unfamiliar	0.35–0.97	0.65	0.03	0.1661	1.5
2	System recovery	0.14–0.42	0.86	0.58	0.0213	1.5
3	Complex task requiring high level of comprehension and skill	0.12–0.28	0.88	0.72	0.0108	1.5
4	Fairly simple task performed rapidly or given scant attention	0.06–0.13	0.94	0.87	0.0042	1.5
5	Routin, highly practised	0.007–0.045	0.993	0.955	0.0021	1.5
6	Restoring a system by following the procedures of controls	0.008–0.007	0.992	0.993	−5.44E-05	1.5
7	Completely familiar, well designed, highly practised, routine task	0.00008–0.009	0.9999	0.991	0.00005	1.5
8	Respond correctly to system command even when there is an augmented or automated supervisory system	0.00000–0.0009	1	0.9991	4.86E-05	1.5

The key quantification elements of the HEART process are:

- Classify task into one of the generic categories;
- Assign a nominal HEP to the task;
- Determine which error producing conditions may affect task reliability;
- Determine the assessed proportion of affect for each task reliability;
- Calculate the task HEP.

HEART uses eight general categories to classify operator tasks, but only six have been chosen for the proposed model. The categories shown in Table 3 can represent a wide range of work activities from simple to more complex ones, from ones with a very high error rates to those more reliable, thanks to the presence of automatic systems of supervision.

This range of activities allows the module to apply the model to very different working environments without any kind of restrictions. For each category, it is calculated the performance of human reliability function (HR) and the probability of human error (HEP), based on Weibull distribution. Table 4 summarizes HRA methodologies.

3 HRA: Second Generation Methods

The development of "second generation" tools began in the 1990s with the aim to improve HRA approaches. Benefits of second generation over first generation approaches is yet to be established. They have also yet to be empirically validated

Table 4 First generation HRA methodologies

Method	Advantages	Disadvantages	Application
OAT	Simple, flexible and reliable	It neglects the differences between the activities	Nuclear
SHARP	It contains safety guidelines		Man-machine system
TESEO	Simple application	Empirical approach limitations	Nuclear—Chemical
SLIM	Flexible, solid and it use a calculator	Subjective judgments	Nuclear—Chemical
HCR	Simple application	It neglects perception error	Nuclear
THERP	Using procedures. Applicable in several sectors	It ignores cognitive errors	Nuclear
HEART	It considers the different activities	It does not consider the environment	Nuclear—Chemical

(Di Pasquale et al. 2013). The second generation methods, try to overcome limitations of traditional methods, in particular:

- **to provide** guidance on possible and probable decision paths followed by operator, using mental processes models provided by cognitive psychology;
- **to extend** errors description beyond usual binary classification (omission-commission), recognizing importance of so-called "cognitive errors";
- **to consider** dynamic aspects of human-machine interaction and can be used as basis for simulators development of operator performance.
- **to estimate** and analyze cognitive reliability, is required a suitable model of human information processing.

The most popular cognitive models are based on the following theories:

- S.O.R. paradigm (stimulus-organism-response): argues that response is a function of stimulus and organism, thus a stimulus acts on organism which in turn generates a response;
- man as a mechanism of information processing: according to this vision, mental processes are strictly specified procedures and mental states are defined by causal relations with other sensory inputs and mental states. It is a recent theory that sees man as an information processing system (IPS);
- cognitive viewpoint: in this theory, cognition is seen as active rather than reactive; in addition, cognitive activity is defined in a cyclical mode rather than sequential mode.

3.1 A Technique for Human Error Analysis (ATHEANA)

ATHEANA is both a retrospective and prospective HRA methodology developed by the US nuclear industry regulatory commission in 2000 (Barriere et al. 2000). It was developed in the hope that certain types of human behavior in nuclear plants

and industries, which use similar processes, could be represented in a way in which they could be more easily understood. It seeks to provide a robust psychological framework to evaluate and identify PSFs—including organizational/environmental factors—which have driven incidents involving human factors, primarily with intention of suggesting process improvement. Essentially it is a method which represents complex accident reports within a standardized structure, which may be easier to understand and communicate.

After a series of studies of plant's incidents, it was observed that incidents occurred in a context where the combination of plant state, performance shaping factors and dependencies led, almost inevitably, to a human error. Hence the main underlying principle of ATHEANA is that error forcing conditions (EFCs) are described for non-nominal situations.

The basic steps of the ATHEANA methodology are (Forester et al. 2004):

- Define and interpret under consideration issue;
- Detail required scope of analysis;
- Describe the base case scenario for a given initiating event, including norm of operations within environment, considering actions and procedures;
- Define human failure events (HFEs) and/or unsafe actions (UAs) which may affect task in question;
- Identify potential vulnerabilities in operators' knowledge base;
- Search for deviations from base case scenario for which UAs are likely;
- Identify and evaluate complicating factors and links to PSFs;
- Evaluate recovery potential;
- Quantify HFE probability;
- Incorporate results into the PRA (Probabilistic Risk Assessment).

The most significant advantage of ATHEANA is that it provides a much richer and more holistic understanding of the context concerning the human factors known to be the cause of incident, as compared with most first generation methods. Compared to many other HRA quantification methods, ATHEANA allows for the consideration of a much wider range of performance shaping factors and also does not require that these be treated as independent. This is important as the method seeks to identify any interactions which affect the weighting of the factors of their influence on a situation. In contrast some criticisms are: the method is cumbersome and requires a large team, the method is not described in sufficient detail that one could be sure that different teams would produce the same results (Forester et al. 1998).

Figure 5 summarizes ATHEANA methodology.

The most significant advantage of ATHEANA is that it provides a much richer and more holistic understanding of context concerning the Human Factors known to be cause of the incident, as compared with most first generation methods.

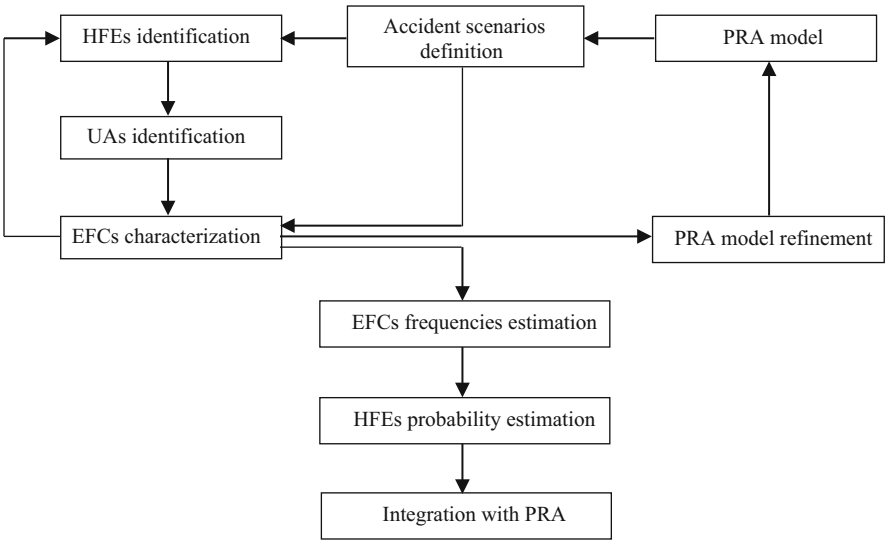


Fig. 5 Flow-chart of ATHEANA methodology application

3.2 Cognitive Reliability and Error Analysis Method (CREAM)

CREAM methodology is a technique used in HRA for the purposes of evaluating human error probability occurring throughout completion of a specific task (Hollnagel 1998). The identified cognitive model for CREAM methodology is called "CoCoM" (contextual control model). The "CoCoM" model is based on the four cognitive function definition:

- observation;
- interpretation;
- planning;
- execution.

CREAM divides the error events into observational errors (phenotypes) and non-observational errors. Phenotypes, which are known as error modes, are the errors that have the external manifestations. Errors, which cannot be observed, are errors that do not have the external appearance and they occur during the human thinking process. CREAM considers that phenotypes are the consequence of non-observational errors by certain transformation of cause to effect, while the latter is considered as the ultimate causes which lead to human errors. CREAM method defines nine correction factors CFPs:

1. adequacy of organization;
2. working conditions;
3. adequacy of MMI and operational support;

4. availability of procedures/plans;
5. number of simultaneous goals;
6. available time;
7. time of day;
8. adequacy of training;
9. preparation and crew collation quality.

There are several levels of each factor to reflect its effect to human performance. In order to reflect the scenario effects on human cognitive behaviors, CREAM method defines four cognitive control modes, which are:

– scrambled;
– opportunistic;
– tactical;
– strategic.

The procedure to assess the error probability is to add to the nine CPC levels that contribute positively (Σ improved) and those who contribute negatively (Σ reduced), getting a pair of values that are inserted in Fig. 1 to locate one of the four categories of control mode:

1. *Scrambled*: unpredictable situation, operator does not have control (error probability range 1E10-1 $<$ p $<$ 1E0);
2. *Opportunistic*: limiting actions, lack of knowledge and staff competence (error probability range 1E-2 $<$ p $<$ 0.5E0);
3. *Tactical*: planned actions, operator knows the rules and procedures of the system (error probability range 1E-3 $<$ p $<$ 1E-1);
4. *Strategic*: operator has a long time to plan its work (error probability range 0.5E-5 $<$ p $<$ 1E-2).

3.3 Task Analysis for Error Identification (TAFEI)

The task analysis for error identification (TAFEI) has been development in 1991 (Baber and Stanton 2002). The basic stages are to produce a description of the user's interaction with the product in terms of a state-space diagram. The sequence of states represented to be necessary and sufficient to achieving a specific goal. This means that one might develop a series of such diagrams if one wanted to examine a range of interactions with the product, e.g., as a form of scenario analysis. The main reason for specifying a user goal is to avoid the combinatorial explosion associated with state-based descriptions of dialogue, i.e., to eliminate the problem of attempting to capture every single state in a product's use, and to force the focus on the user's purposeful interaction with the product. The main phases of TAPEI procedure are:

– Defining User Goal and Task Sequences
– Developing State-Space Diagrams

– mapping task sequences onto state-space diagrams
– constructing error matrices
– Validating

3.4 Standardised Plant Analysis Risk–Human Reliability Analysis Method (SPAR-H)

The standardised plant analysis risk–human reliability analysis method (SPAR-H) has been development in 1999 (NUREG/CR-6883 2005). The main goal of the method is to assess cognitive human process of failure such as detection, understanding, decision and action.

The basic SPAR-H framework includes the following steps:

– decomposes probability into contributions from diagnosis failures and action failures;
– accounts for the context associated with human failure events (HFEs) by using performance-shaping factors (PSFs), and dependency assignment to adjust a base-case human-error probability (HEP);
– uses pre-defined base-case HEPs and PSFs, together with guidance on how to assign the appropriate value of the PSF;
– employs a beta distribution for uncertainty analysis;
– uses designated worksheets to ensure analyst consistency.

The SPAR-H method assigns human activity to one of two general task categories: action or diagnosis. Examples of action tasks include operating equipment, performing line-ups, starting pumps, conducting calibration or testing, and other activities performed during the course of following plant procedures or work orders. Diagnosis tasks consist of reliance on knowledge and experience to understand existing conditions, planning and prioritizing activities, and determining appropriate courses of action. Base error rates for the two task types associated with the SPAR-H method were calibrated against other HRA methods. The calibration revealed that the SPAR-H human error rates fall within the range of rates predicted by other HRA methods. A number of HRA methods do not have an explicit human performance model. The SPAR-H method is built on an explicit information-processing model of human performance derived from the behavioral sciences literature that was then interpreted in light of activities at NPPs. In 1999, further research identified eight PSFs capable of influencing human performance. These PSFs are accounted for the SPAR-H quantification process. These factors include:

1. Available time;
2. Stress and stressors;
3. Experience and training;
4. Complexity;

5. Ergonomics (& HMI);
6. Procedures;
7. Fitness for duty;
8. Work processes.

While many contemporary methods address PSFs in some form, SPAR-H method is one of the few that addresses the potential beneficial influence of these factors. That is, positive influences of PSFs can operate in some instances to reduce nominal failure rates (Gertman et al. 2005).

4 HRA: Third Generation Methods (A Simulation Approach)

In the face of any unresolved debate over first and second generation HRA a third generation of HRA is developed. There are more interesting and more important developments in HRA on the horizon, and it is time to augment first and second generation HRA methods. First and second generation HRA methods do and will continue to play a role in classifying and quantifying human performance. First and second generation methods should continue to be implemented wherever needed. Second generation methods should continue to be researched and improved to ensure an efficient, accurate, and complete capture of human performance. What sets this form of HRA apart is that it provides a dynamic basis for HRA modeling and quantification. First and second generation methods, by any definition, have featured largely static task analyses of operating events as the underlying basis of performance modeling. These methods have also relied on performance estimations mapped to similar previous performance derived through empirical data or expert opinion. Simulation-based HRA differs from its antecedents in that it is a dynamic modeling system that reproduces human decisions and actions as the basis for its performance estimation. Simulation based HRA may utilize a frequentist approach for calculating HEPs, in which varieties of human behaviors are modeled across a series of monte carlo style replications, thus producing an error rate over a denominator of repeated trials. Simulation based HRA may also augment previous HRA methods by dynamically computing PSF levels to arrive at HEPs for any given point in time (Boring 2007).

4.1 Simulator for Human Error Probability Analysis (SHERPA)

The purpose of each HRA method must be to assess human behaviour and to quantify error probability, in order to reduce and prevent possible conditions of

human error probability, and to reduce and prevent possible conditions of human error in a working context.

The Simulator for Human Error Probability Analysis (SHERPA) model provides a theoretical framework that exploits the advantages of the simulation tools and the traditional HRA methods. It has been developed by Di Pasquale et al. (2015). The model tries to predict the human error probability, for a given scenario, in every kind of industrial system or other type of working environment. Three HRA elements converge into the model:

- Task classification in one of the generic tasks proposed by the HEART model;
- Performance shaping factors analysis of SPAR-H methods;
- Dynamic implementation using computer simulation.

The aspiration for the simulator for human error probability analysis (SHERPA) model is not that it be a new HRA method in the long list of existing ones, but that it provides a theoretical framework that addresses the problem of human reliability in a different way from most HRA methods. Human reliability is estimated here as function of the performed task, performance shaping factors and also time worked, with the purpose of considering how reliability depends on the task and on working context, as well as on the time that operators have already spent at their work. Moreover, contextual factors of the second generation method (SPAR-H) allow careful evaluation of the working environment in order to identify the most negative factors. The model is able to provide for the following functions:

1. estimating human reliability, as function of time, of work environment conditions, of physical and mental employee condition and of rest breaks distribution during the shift;
2. assessing the effects due to different human reliability levels, through evaluation of processes, activities or tasks performed more or less correctly;
3. assessing the impact of context on human reliability, via performance shaping factors.

4.2 Probabilistic Cognitive Simulator (PROCOS)

A probabilistic cognitive simulator for HRA studies (PROCOS) has been developed by Trucco and Leva in 2007 (Trucco and Leva 2007). The simulator aims to analyse both error prevention and error recovery. It is based on "semi-static approach" and it aims to study how the PSFs influence the operator cognitive process and human error probability. The simulation model requires: (1) a preventive risk analysis; (2) a cognitive model of the operator and (3) a taxonomy of the possible error type. The simulation model comprised two cognitive flow charts, reproducing the behaviour of a process industry operator. The simulator does not perform a time-dependent simulation process.

5 Conclusions

After examining some of human reliability analysis techniques, it is necessary to highlight the uncertainties that still exist when choosing this type of approach to the human factor. The use of principles and methods for components reliability shows, in fact, the estimate of probability of human error on the same level of the fault. In addition these methods, prefers basic psychological models, remain anchored to the inner phase of cognitive process, do not show the link with the external conditions. Considering influences that environment has on human performance, we must give appropriate weight to those that are also considered latent system errors. These flaws of system remain latent for a certain period of time, but in connection with other etiological factors can give rise to an incident in which man is the last link in a random errors chain and deficiencies relating the context in which it operates. Therefore it would be desirable, for a correct dimensioning of prevention system, apply techniques for human reliability analysis in an integrated way to design work environments and the widespread sharing, from part of the whole organization, of the values of safety.

References

Adhikari S, Bayley C, Bedford T, Busby JS, Cliffe A, Devgun G, Eid M, French S, Keshvala R, Pollard S, Soane E, Tracy D, Wu S (2008) Human reliability analysis: a review and critique. Manchester Business School, Manchester

Baber C, Stanton NA (2002) Task analysis for error identification: theory, method and validation. Theor Issues in Ergon Sci 3(2):212–227

Barriere M, Bley D, Cooper S, Forester J, Kolaczkowski A, Luckas W, Parry G, Ramey-Smith A, Thompson C, Whitehead D, Wreathall J (2000) NUREG-1624: technical basis and implementation guidelines for a technique for human event analysis (ATHEANA). US Nuclear Regulatory Commission

Bell J, Holroyd J (2009) Review of human reliability assessment method. Health and Safety Laboratory, Buxton

Bello GC, Columbari C (1980) The human factors in risk analyses of process plants: the control room operator model, TESEO. Reliab Eng 1:3–14

Boring RL (2007) Dynamic human reliability analysis: benefits and challenges of simulating human performance. Risk Reliab Soc Saf 2:1043–1049

De Felice F, Petrillo A, Carlomusto A, Ramondo A (2012) Human reliability analysis: a review of the state of the art. IRACST–Int J Res Manag Technol (IJRMT) 2(1)

De Felice F, Petrillo A, Carlomusto A, Romano U (2013) Modelling application for cognitive reliability and error analysis method. Int J Eng Technol 5(5):4450–4464

Di Pasquale V, Iannone R, Miranda S, Riemma S (2013) An overview of human reliability analysis techniques in manufacturing operations. In: Schiraldi M (ed) Operations management. InTech

Di Pasquale V, Miranda S, Iannone R, Riemma S (2015) A simulator for human error probability analysis (SHERPA). Reliab Eng Syst Saf 139:17–32

Dougherty E (1990) Human reliability analysis—where shouldst thou turn? Reliab Eng Syst Saf 29(3):283–299

Embrey DE, Humphreys P, Rosa EA, Kirwan B, Rea KS (1984) An approach to assessing human error probabilities using structured expert judgement (NUREG/CR-3518). US Nuclear Regulatory Commission, Washington, DC
Forester J, Bley D, Cooper S, Lois E, Siu N, Kolaczkowski A, Wreathall J (2004) Expert elicitation approach for performing ATHEANA quantification. Reliab Eng Syst Saf 83(2):207–220
Forester J, Ramey-Smith A, Bley D, Kolaczkowski A, Cooper S, Wreathall J, (1998) SAND--98-1928C: discussion of comments from a peer review of a technique for human event analysis (ATHEANA). Sandia Laboratory
French S, Bedford T, Pollard SJT, Soane E (2011) Human reliability analysis: a critique and review for managers. Saf Sci 49(6):753–763
Gertman D, Blackman H, Marble J, Byers J, Smith C (2005) The SPAR-H human reliability analysis method. US Nuclear Regulatory Commission
Hannaman GW, Spurgin AJ (1984) Systematic human action reliability procedure (SHARP) (No. EPRI-NP-3583). NUS Corporation, San Diego, CA
Hannaman GW, Spurgin AJ, Lukic YD (1984) Human cognitive reliability model for PRA analysis. Draft Report NUS-4531, EPRI Project RP2170-3. Electric Power and Research Institute, Palo Alto, CA
Hollnagel E (1993) Human reliability analysis: context and control. Academic Press, London
Hollnagel E (1998) Cognitive reliability and error analysis method: CREAM. Elsevier Science, Oxford
Hollnagel E (2000) Looking for errors of omission and commission or the hunting of the Snark revisited. Reliab Eng Syst Saf 68:135–145
Hollnagel E (2005) Human reliability assessment in context. Nucl Eng Technol 37(2):159–166
Humphreys PC (1995) Human reliability assessor's guide. Human Factors in Reliability Group, SRD Association
IEEE (1997) Guide for incorporating human action reliability analysis for nuclear power generating systems. IEEE, New York
Kirwan B (1994) Practical guide to human reliability assessment. Taylor and Francis, CRC Press, London
Kirwan B (1996) The validation of three human reliability quantification techniques—THERP, HEART, JHEDI: Part I—technique descriptions and validation issues. Appl Ergon 27 (6):359–373
Rasmussen J (1983) Skills, rules, knowledge; signals, signs and symbols and other distinctions in human performance models. IEEE Trans Syst Man Cybern SMC-13(3):257–266
Senders JW, Moray N, Smiley A (1985) Modeling operator cognitive interactions in nuclear power plant safety evaluation. Report prepared for the Atomic Energy Control Board. Ottawa, Canada
Swain AD, Guttman HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUAREG CR-1278.NRC, Washington, DC
The SPAR-H human reliability analysis method (2005) NUREG/CR-6883, INL/EXT-05-00509. Idaho National Laboratory, US Nuclear Regulatory Commission, Washington, DC
Trucco P, Leva MC (2007) A probabilistic cognitive simulator for HRA studies (PROCOS). Reliab Eng Syst Saf 92(8):1117–1130
Watson IA (1985) Review of human factors in reliability and risk assessment. The assessment and control of major hazards. pp 323–337
Wreatall J (1982) Operator action trees. An approach to quantifying operator error probability during accident sequences, NUS-4159. NUS Corporation, San Diego, CA

Fabio De Felice, PhD in Mechanical Engineering. Professor at the University of Cassino and Southern Lazio, board member of several international organizations. The scientific activity developed through studies and researches on problems concerning industrial plant engineering. Such activity ranges over all fields from improvement of quality in productive processes to the simulation of industrial plants, from support multi-criteria techniques to decisions (Analytic Hierarchy Process, Analytic Network Process), to RAMS Analysis and Human Reliability Analysis.

Antonella Petrillo, degree in Mechanical Engineering, PhD at the University of Cassino and Southern Lazio. Now Professor at University of Naples "Parthenope" (Department of Engineering) where she conducts research activities on Multi-criteria decision analysis (MCDA), Industrial Plant, Disaster Management, Logistic and Safety.

Mathematical Models for Reliability Allocation and Optimization for Complex Systems

Domenico Falcone, Alessandro Silvestri, Gianpaolo Di Bona, and Antonio Forcina

Abstract RAMS is an acronym for Reliability, Availability, Maintainability and Safety. These four properties concern the application of important methodologies for designing and managing complex technical systems. The present chapter analyses several reliability allocation techniques present in literature. Starting from well-known methodologies, two reliability allocation methods has been proposed and validated: Integrated Factors Method (I.F.M.) and Critical Flow Method (C.F.M.). We focus on the most important conventional methods to discuss their limitations to motivate the current research.

The proposed methods supply a logic for the analysis of prototype complex systems during the pre-design phase, even if it presents general characteristics that allow this logic to be extended to different design phases. In particular, the proposed CFM method can resolve the shortcomings of the conventional methods with a new reliability approach useful to series-parallel configurations in order to obtain important cost savings. In fact, the results show that the most conventional reliability allocation methods have one fundamental problem: in general, they are designed for complex system with series-configurations (preliminary phase design) but not for series-parallel configurations. The result is an increase of reliability allocated to units (series configuration) in order to guarantee the reliability target system (extremely low failure rate).

Keywords Reliability • Allocation methods • Integrated Factors Method • Critical Flow Method

D. Falcone • A. Silvestri • G. Di Bona (✉) • A. Forcina
University of Cassino and Southern Lazio, Cassino, Italy
e-mail: falcone@unicas.it; silvestr@unicas.it; dibona@unicas.it; antonio.forcina@uniparthenope.it

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_3

1 Introduction

The reliability of a complex system depends on the system chronological age and its work conditions. During the design phase, the evaluation of the reliability of the system is an important matter. The problem involves selection of components, redundancy strategies, cost reduction etc. The question is how to meet a reliability goal for the system, adequate to its mission.

In order to improve system reliability, designers may introduce in a system different technologies in series and parallel (series–parallel systems), and the use of redundancies could often help to reach the goal, even if costs increase.

In literature, there are two main possible approaches. The first type of analysis leads to the system's reliability target starting from data of units through a fault tree analysis ('bottom-up' approach). Reliability data of components could be only partially available, particularly in the case of innovative systems. The second type of analysis starts from similar systems and defines the target of each unit by applying allocation techniques ('top-down' approach). Also, in this case, reliability data of similar systems might not be available, and the choice of the most appropriate technique could be tricky. Both above usual approaches show advantages and disadvantages, even if the allocation methods allow reducing costs with the minimum reliability requirement for multiple components within a system that will yield the goal reliability value for the whole system. This then becomes a reliability allocation problem at the component level. The system's cost is then minimized by solving for an optimum component reliability, which satisfies the system's reliability goal requirement.

In the chapter the main literature allocation methods are showed, and some case studies are presented. Many of them use weights for the factors involved in reliability allocation.

2 Reliability Allocation Process and Literature Methods Overview

The allocation process is an iterative logic, based on the validation and the comparison of the allocated data with the reliability data supplied by construction companies or databanks (Fig. 1).

The above scheme proposes the following steps:

1. System definition (unit identification);
2. Reliability Block Diagram construction (logical connections among units);
3. Preliminary Hazard Analysis management (Top Event definition);
4. Definition of reachable reliability targets, through FTA, starting from data supplied by construction companies or presented in literature (success probability evaluation);

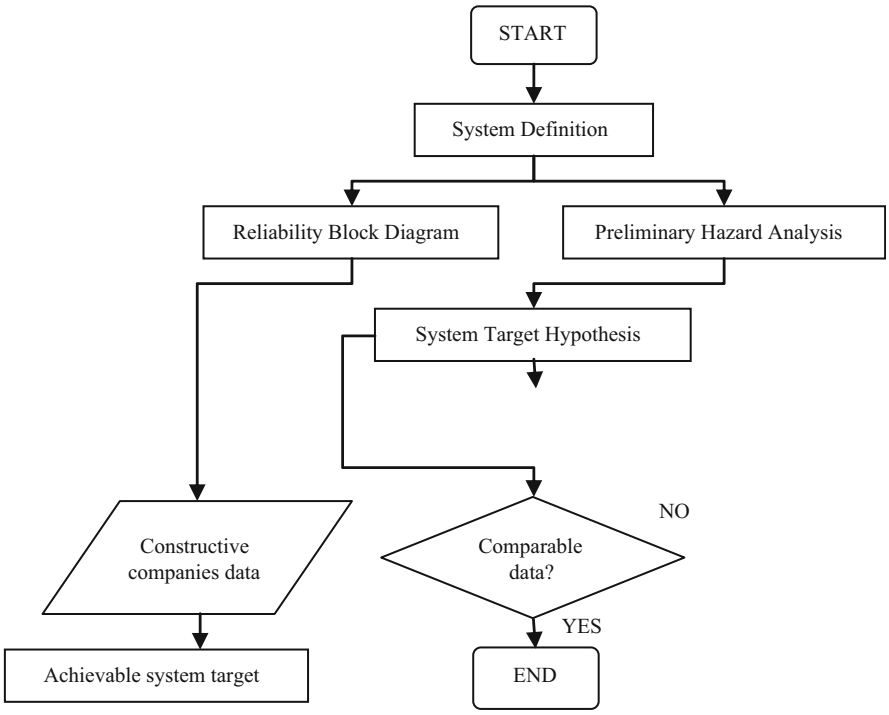


Fig. 1 General logical scheme for allocation

5. Reliability allocation to each unit (choice of the proper methodology);
6. Allocated data comparison with reachable data (obtained by reliability proofs);
7. Procedure interaction (difference reduction between the allocated data and the reachable ones.

A reliability allocation methodology starts by defining all or some of the following elements:

1. system and troubles (fundamental and not influential units, failures);
2. system reliability parameters (system reliability target);
3. feasibility of the system reliability target (comparison with similar systems);
4. unit technology (mean fault rate);
5. relation between the unit fault and the system fault (series, modified, redundant, multi-modal systems);
6. unit importance (relation between the system failure and the unit failure);
7. modal design adequacy (relation between the mission success probability and the modal efficiency);
8. operation cycles (operation time).

The system must be clearly defined, considering fundamental units and ignoring the not influential ones; every failure condition must be noticed. The starting point,

in the allocation model application, is the system reliability target, definable directly or through the following factors:

- *System Efficiency $S^*(T)$:* probability that the system will satisfy a fixed operative request, working for t hours, under fixed conditions;
- *System Reliability $R^*(T)$:* probability that the system will do perfectly the designed functions for t hours, under fixed conditions;
- *System Design Adequacy D_S:* probability that the execution of the expected designed functions will realise the mission success;
- *Operational Readiness P_{OR}:* probability that in every moment the system will be working correctly or be able to act, under fixed conditions;

$$S^*(T) = R^*(T) \cdot D_S \cdot P_{OR} \tag{1}$$

The feasibility of the global reliability target is verified through the comparison with systems of similar complexity, previously studied.

The factor of importance is initially valued intuitively and then defined through the ratio:

$$E_j = failures\ n^\circ\ caused\ by\ unit_j\ faults / unit_j\ faults\ n^\circ \tag{2}$$

Therefore, it is possible to affirm:

- the component allocated reliability increases with the reduction of the technology, the operative time, and the increase of the importance;
- the units with the same importance, operative time and technology, must have the same allocated reliability.

The mathematics treatment of allocation is strongly simplified if the following hypotheses are made:

- the units must be chosen by independent fault probabilities;
- the unit state must be described by binary terms: on/off.

In literature, there is not a universal technique (Barbarino 1990), suitable for reliability allocation of every system and every design phase.

Different methodologies can be used jointly; it is often possible to use more techniques in the different phases of a complex system plan. The allocation starts from the initial plan step, when few data about components are available. In this phase it is better to consider the sub-systems in a series configuration (the breakdown of any unit causes the mission failure) and to adopt one of the allocation methodologies for such systems such as *Base method* (Balaban and Jeffers 1999) and *Boyd method* (Boyd 1992). Then, when more data are available (number of components and their interconnections), it is possible to use other methodologies (Jarrell 2003) such as *Agree method* (Advisory Group of Reliability of Electronic Equipment (AGREE) 1957), *Cost method, Karmiol method,* (Karmiol 1965) *weighted factors sum, Bracha method* (Bracha 1964) and *FOO method* (United

States Department of Defense 1988) that allow to perform the allocation of reliability parameters using different factors (the system criticality and technology, the mission time, etc.).

In the following sections the main allocation methods are described and analyzed.

2.1 Base Method

The Base method considers the units of the investigated system in series, the breakdown of any unit causes the mission failure, moreover this method considers the fault rates as constant and independent.

In the Base Method the allocation of the requirements of reliability of a complex system components requires the solution of the following fundamental equation:

$$f(R_1, R_2 \ldots \cdot R_N) \geq R(t) \tag{3}$$

Rj: reliability allocated on the j-th unit, with j = 1...N;
R*: target goal of the system;
f(...): functional relationship between the reliability of the units and the system.

The method requires some basic assumptions: first, the rate of failure of each component is constant, the failures of any units are independent and the breaking of any units causes the failure of the mission.

With these assumptions we have that:

$$[R_1(t) \cdot R_2(t) \cdot \ldots \cdot R_N(t)] = R^*(t) \tag{4}$$

R(t): unit_j reliability for t operative hours;
R*(t): system reliability for t operative hours.

The above equation, remembering the analytical reliability definition, becomes (under the established hypotheses):

$$e^{-\lambda St} = e^{-\lambda 1t} \cdot e^{-\lambda 2t} \cdot \ldots \cdot e^{-\lambda Nt} \tag{5}$$

λ_j: unit_j fault rate;
λ_S: system fault rate.

This method is called Base Method because it does not consider factors such as the importance and functional differences between individual units. It also does not assess the actual feasibility of the requirements of the target system and fails to take into account any redundancy. Indeed, it is a methodology that can be applied only to systems in series, for which all elements have the same impact on the failure of the mission.

2.2 Boyd Method

The Boyd Method (Boyd 1992) represents an integration between two other methods, the EQUAL method and the ARINC one for systems in series.

The Equal method allocates the unit$_i$ fault rate (λ_{ai}), dividing the system fault rate (λ_{rS}) by the total number of subsystems (N):

$$\lambda_{ai} = \lambda_{rS}/N \tag{6}$$

The Arinc method, instead, allocates the fault rate starting from an initial value (λ_{pi} *and* λ_{pS}), obtained through data-banks or opportune hypotheses:

$$\lambda_{ai} = \lambda_{rS} \cdot \lambda_{pi}/\lambda_{pS} \tag{7}$$

The Boyd method, starting from the above techniques, proposes the following allocation formula:

$$\lambda_{ai} = M \cdot K \cdot \lambda_{rS} \cdot 1/N + (1 - K) \cdot \lambda_{rS} \cdot \lambda_{pi}/\lambda_{pS} \tag{8}$$

K: values between 0 (ARINC) and 1 (Equal);

The Boyd method mediates the two techniques just described from the following assumptions: the subsystems are in series, subsystems work for the same period of time during which the system operates; rates of failure are constants.

The method requires a preliminary knowledge of the values of failure rates of components. This condition makes the procedure not particularly flexible and not suitable for all types of systems.

2.3 Agree Method

The Agree method (Advisory Group on Reliability of Electronic Equipment), was born in the electronic field and emphasizes on the relations between unit faults and system faults, assuming the fault rates of the units in series as independent.

The single unit complexity is expressed in terms of modules (1 module, ½ module, etc.); every module presents a factor of importance *E,* which expresses the probability that the system mission failure takes place in presence of unit break down.

(i.e.: $E = 1$: probability = 100%; $E = 0$: probability = 0%). The fault rate allocated to the unit$_j$, starting from the hypothesis of a same fault rate for each module, is given by:

$$\lambda_i^{\circ} = \frac{n_j[-\ln R(t)]}{NE_j t_j} \tag{9}$$

n_j: unit$_j$ number of modules;
N: system total number of modules;
E_j: unit$_j$ factor of importance;
t_j: unit$_j$ number of operative hours ($0 < t_j < T$, where T is the system number of total operative hours).

The defined fault rate increases with the unit number of modules, decreases with the factor of importance.

2.4 Cost Method

Some methods propose a reliability allocation based on economic considerations. Considering the relation:

$$R^* = R_1^{\circ} \cdot R_2^{\circ} \cdot \ldots \cdot R_N^{\circ} \tag{10}$$

R_j°: reliability allocated to the unit$_j$;
R^*: system reliability target.

The method foresees the research of the minimum cost function, using Lagrange multipliers (complex analytical treatment):

$$C(R^*) = C\left(R_1^{\circ}\right) + C\left(R_2^{\circ}\right) + \ldots + C\left(R_N^{\circ}\right) \tag{11}$$

$C(R^*)$: cost needed to obtain the system reliability target;
$C(R_j^{\circ})$: cost needed to obtain the unit$_j$ reliability target.

2.5 Karmiol Method: Factors Product

This method considers the influence of different factors:

- *Complexity (Cx):* considers the number of functions for each sub-system (more complexity, less reliability);
- *State of Art-Technology (A):* considers the engineering progress for each sub-system;
- *Operative profile (O):* considers the mission time and the operative severity for each subsystem;
- *Criticality (Cr):* considers the influence of the sub-system on the system mission success (greater criticality, greater allocated reliability).

The values of the above factors are between 1 and 10, increasing for *Cx, A, O*, decreasing for *Cr* (greater criticality: Cr = 1; minor criticality: Cr = 10).

The product of the four factors represents the *effect factor* (*n*) for each sub-system:

$$n = Cx \cdot A \cdot O \cdot Cr \tag{12}$$

The value of the allocated reliability for the sub-system$_k$, derives from the expression below, where R is the reliability target of the system composed by m subsystems:

$$R_k = R^A x\, R^B \tag{13}$$
$$A = (n_1 + n_2 + \ldots + n_m)/(2\, x\, N\, x\, n_k)$$
$$B = F_k/[2\, x\, (F_1 + F_2 + \ldots + F_m)]$$
$$N = \Sigma_{i=1,\ldots,m}(n_1 + n_2 + \ldots + n_m)/n_i$$

n_k: effect factor for the subsystem$_k$; F$_k$: functions (operations) number for the subsystem$_k$.

This method, for the allocation of fault rates too, explained for series systems, could be easily extended to redundant systems.

2.6 Karmiol Method: Weighted Factors Sum

This method uses several factors, similarly to the previous method, [complexity (*Cx*), state of art-technology (*A*), operative profile (*O*), criticality (*Cr*)]. These factors are summed up to obtain the total weight factor for each sub-system working in series. The method starts from the allocation of unreliability, then of reliability and fault rates. The total weight factors, calculated for each sub-system$_i$ (T_i), are added to obtain the system total weight factor (T_S):

$$T_i = Cx_i + A_i + O_i + Cr_i \;\Rightarrow\; T_S = \Sigma_i T_i \tag{14}$$

We fix the system unreliability, then we can allocate the unreliability (and then the reliability and the fault rate) to each sub-system, through the relative weight factor:

$$W_i = T_i/T_S. \tag{15}$$

2.7 Bracha Method

The method requires the determination of the following four weight factors:

- *State of Art-Technology (A):* considers the level of the engineering progress for each sub-system;
- *Complexity (C):* considers the sub-system number of parts and the assembly difficulty:

$$C = 1 - Exp\left[-K_b + \left(0,6\left(K_p\right)\right]\right. \tag{16}$$

K_b: ratio between the number of components of the considered subsystem and of whole system;
K_p: ratio between the number of redundant components of the considered subsystem and of whole system.

- *Environmental conditions (E):* considers the operative severity for each subsystem:

$$E = 1 - 1/f \tag{17}$$

f: external stress (0: min stress; 100: max stress)

- *Operation time (T):* considers the operation time for each subsystem:

$$T = T_m/T_u \tag{18}$$

T_m: system mission total time;
T_u: subsystem operative time.

Then, it is possible to calculate the I_i index and the W_i weight factor, for the sub-level$_i$ (n: number of sub-levels in series):

$$I_i = A_i \cdot (C_i + E_i + T_i); \quad W_i = I_i/\Sigma_{j=1,\ldots,n} I_j \tag{19}$$

The reliability allocation for each sub-system ($R_i(t)$), starting from the system reliability target ($R_S(t)$), is defined by the following expression:

$$R_i(t) = [R_S(t)]^{Wi} \tag{20}$$

2.8 Feasibility of Objectives (FOO) Method

This method included in Mil-Hdbk-338B is based on Eq. (21) after considering four factors:

- A_{i1} : state of art-technology of unit i
- A_{i2} : intricacy of unit i
- A_{i3} : operating time of unit i
- A_{i4} : environmental condition

An expert judgment evaluates each factor using a 10-point numerical scale and the final allocation is given by (Table 1):

$$w_i = \frac{(A_{i1}A_{i2}A_{i3}A_{i4})}{\sum_{i=1}^{k}[A_{i1}A_{i2}A_{i3}A_{i4}]} \quad i = 1, \ldots, k \tag{21}$$

In order to overcome some limits of literature methods, two innovative methods and their applications are described in the following paragraphs.

Table 1 Principal advantages and disadvantages of the analysed methods

Method	Advantages	Disadvantages
Base	– Application simplicity – Objectivity	– Only applicable to systems in series – Only applicable in the initial phases – Fault rate knowledge of similar systems
Boyd (EQUAL and ARINC)	– Versatility	– Only applicable to systems in series – Only applicable in the initial phases
AGREE	– Good detail	– Only applicable to systems in series – Applicable in advanced phase – Partial subjectivity of the analyst
Cost	– Economic guide lines	– Complex or approximated analytical treatment
Karmiol – Factors product	– Very good detail – Applicable to innovative systems – Applicable in every phase	– Subjectivity of the analyst
Karmiol – Factors sum	– Very good detail – Applicable to innovative systems	– Only applicable to systems in series – Subjectivity of the analyst
Bracha	– Exact analytical treatment	– Not easy determination of stress factors – Component criticality not considered
FOO	– Applicable to innovative systems – Applicable in every phase	– Only applicable to systems in series

3 Integrated Factors Method

The Integrated Factors Method (Falcone et al. 2004) has been thought-out for complex systems during the pre-design phase. Subsequently, some changes have been introduced into this method, in order to permit its application to different design phases, when more detailed information about components is known. The new methodology was initially developed for systems in series configuration prototype systems (the "series" hypothesis is in favour of safety, in fact the failure of the mission happens when one unit breaks down). Studying in detail the different allocation methods, we realized that it was necessary to use opportune factors of influence.

The use of these factors enables to discriminate among the different units of the system. Initially, we have supposed the same technological level for the units and the same operative severity. We have chosen the following factors and relative indexes:

- *Criticality index (C):* ratio between the number of sub-system functions that cause an undesirable event if not realised, and the total number of system functions;
- *Complexity index (K):* referring to the technological and constructive structure; possible values are: 0.10 for simple system; 0.20–0.90 for not very complex system; 1.00 for complex ones;
- *Functionality index (F):* ratio between the total number of unit functions, and the total number of system functions;
- *Effectiveness index (O):* referring to the unit operative time; possible values are: 1.00 for the whole mission time; 0.67 for continuous and long times; 0.33 for instantaneous times.

The target severity is directly proportional to the *C* index increase but not to the other increases.

The evaluation of the above indexes, thanks to an Expert Judgement's help, enables to calculate a new index (that we called) the *Global Index* (*IG),* for the allocation of the unreliability of the system, (and, consequently, of its reliability). This index is defined through the relation:

$$IG_i = \frac{K_i F_i S_i}{C_i} \rightarrow IG\%_i = IG_i / (\Sigma_{i=1,\ldots,n} IG_i) \tag{22}$$

$IG\%_i$: percentage global index relative to the sub-system$_i$;
IG_i: global index relative to the sub-system$_i$;
n: number of units.

Then, in a dynamical approach, we have not changed the *C* and *F* indexes (but their evaluation, in an advanced phase comes from a functional-FMECA analysis and from complete component data); instead we have passed from a quality definition for the *K* and *O* indexes to a quantity definition:

– *Complexity index (K):* ratio between the number of parts of the unit and the number of parts of the whole system;
– *Effectiveness index (O):* ratio between the time of effectiveness of the unit and the mission total time.

In order to apply the new method to more complex systems, characterized by components with different technology, we have introduced new parameters that improve the *Global Index (IG).*

The equation that describes this the new index is:

$$IG_i = \frac{K_i F_i S_i O_i M_i}{C_i E_i} \tag{23}$$

In particular we introduced:

– *Technology index (S).* We assumed S = 0.5 for traditional components and S = 1: innovative components).
– *Electronic Functionality index (E).* We introduce this index in order to discriminate between electronic systems and mechanical ones, characterized by the same complexity. We assumed E = 1 for completely electronic system and E = 0.1 for completely mechanical system).

At last, we have introduced an increase (M) for the Effectiveness index (O), caused by a greater operative severity. The *Global Index* (IG) becomes:

We noted that in the new Eq. (23) of Global Index at the numerator there are those factors whose growth cause an unreliability increase, at the denominator those factors that cause a reduction. Then it is possible to allocate the system unreliability target *(U(t))* to the unit$_i$ *($U_i(t)$):*

$$U_i(t) = U(t) \cdot IG\%_i \tag{24}$$

The proposed method wants to integrate the advantages of the previously analysed techniques.

In particular the IFM method uses a great number of factors in order to consent the method to be applied to a wide variety of systems. The chosen standard input *data is the unreliability. The cheapness of the method is the simplicity of the analytical treatment.*

The main characteristics are:

– index values are between 0 and 1 (modular structure and dynamism);
– it is possible to eliminate not influential aspects putting the relative index equal to 1;
– it is possible to introduce, if necessary, other indexes, to consider other allocation characteristics.

All in all, our method is able to adapt the available methodologies to the different design phases, that is the fundamental requisite of RAMS analysis.

3.1 Integrated Factors Method Application

The "Integrated Factors Method", has been applied to a production sub-system, aiming at the realization of sintered products. In particular, the considered sub-system makes it possible to carry out the drying of dusts.

The subsystem has been decomposed in functional blocks through the application of a Product Tree Analysis (P.T.A.) and a Reliability Block Diagram (R.B.D.).

Subsequently, to quantify the factors of allocation, a Failure Mode and Effect Analysis (F.M.E.A.) has been implemented.

We fix as target the factor of unreliability of the subsystem, deduced by the scientific literature.

In the following we analyse the Production Process and the Sintering Products.

The metallurgy of the powders is a particular technology, suitable for producing finished metal or metal ceramic pieces, starting from powders mixed through pressing and sintering operations.

Generally, the process takes place in controlled atmosphere and consists of an opportune keeping of the powders at such temperatures as to cause the conglomeration of all the mass, without reaching the fusion of the material.

The starting materials are metal carbides, usually tungsten carbide and cobalt powders.

The methods for the preparation of the metal powders can be divided into two groups:

- *mechanical processes:* processing at machine tools, crushing, grinding and gritting;
- *chemical processes:* thermal decomposition, condensation, reduction, precipitation and replacement.

Before being compacted, the powders are mixed in spherical mills, by adding right quantities of solid lubricant (paraffin) and a solvent of the lubricant (isopropyl alcohol).

Alcohol helps the uniform distribution of the mass of the powders, forming a fluid mixture.

After the removal of the solvent, the paraffin covers the particles of powder and helps their union and compacting on the following phase of pressing or extrusion.

The retrieval of the solvent used takes place through the drying of the mixture, carried out through the heating of the mixture with warm water. The operation is effected under vacuum.

The following process of the pressing of the mixture can be of two types:

- mechanical: production of pieces in a finished shape and of small-medium size;
- hydraulic: production of box-shaped pieces and of medium-big size.

The extrusion process enables, as well as the hydraulic pressing, to obtain box-shaped and very long pieces.

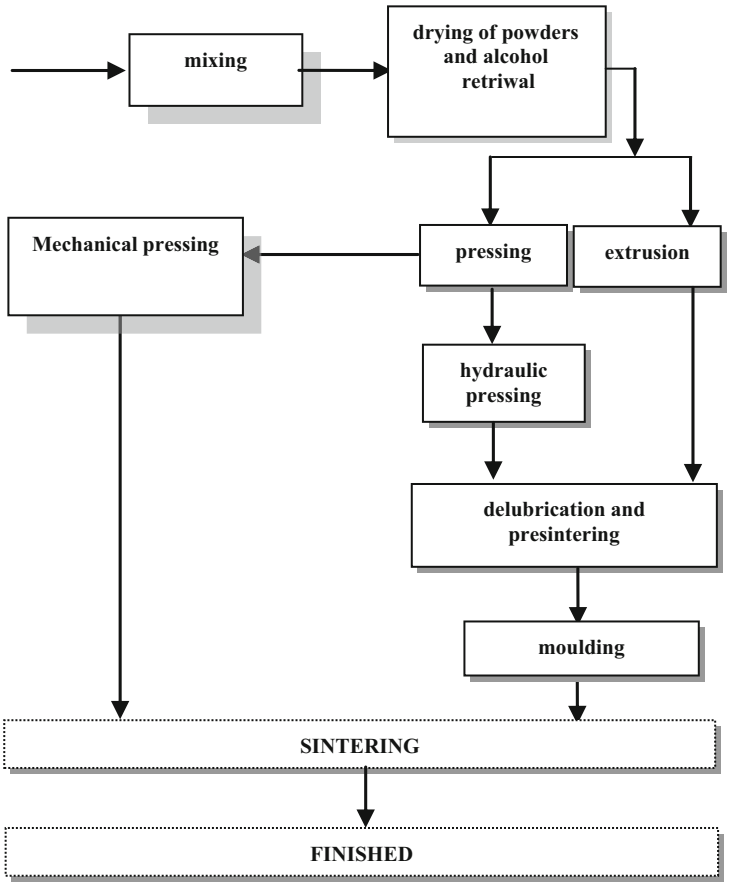


Fig. 2 Functional diagram of the productive cycle

The products obtained are then delubricated and presintered, in order to give suitable capacities of mechanical resistance for the following moulding process.

The product, obtained through working by tool machines, is sent to the sintering phase.

The cycle is carried out in induction or resistance furnaces and aims at changing the powder mixtures into a solid body (Fig. 2).

The fundamental parameters of such a process are:

- time;
- temperature;
- shape and sizes of the particles;
- surface state of the particles;
- degree of compacting.

For every type of powder there are some practical limits, within which it is possible to make time and temperature changes.

Too low temperature values would cause too long and not economic times; on the contrary, high temperatures would help the rising of vaporisation phenomena, gas solubility as well as mixture fusion. In general, when the temperature and the duration increase, even if remaining within the safety range, they aim at increasing the density, the resistance at traction and extension of the compacted product.

3.2 Functional Analysis of the Production Process

The allocation methodology (I.F.M) has been applied to the powder drying section, since it represents an important part within the production cycle. In fact, the lacking or partial retrieval of the lubricant would cause a difficult deposit of the paraffin on the powder particles, with consequent problems of the compacting of the powders in the next phase of pressing. The retrieval of the isopropyl alcohol is effected through a piston pump for the vacuum. The lack of physical redundancies causes probable breakdowns or malfunctions of the sub-system analysed, and it might involve considerable inefficiency as to costs and quality of the process. The piston pump for the vacuum, which needs the maximum reliability, shows the following mechanical characteristics:

- motor power: 3 kW;
- capacity: 100 m^3/h;
- turns per minute: 250;
- vacuum: 5.30 mbar;
- total weight: 380 kg.

The electric engine starts the rotation of the fly-wheel, which, through the camshaft, operates the connecting rod, the piston, the distributing rod and the slide valve. During its run, while the piston inhales the gases of the cylinder from the slits, it discharges the gases previously inhaled, during the reverse run, through the valves. The pump works in an intermittent way for about 20/22 h a day. During the remaining hours of inaction, it is then possible to carry out operations of ordinary maintenance. The lubrication of the sub-system is obtained through a pumping group formed by two pumps: a piston one and a gearing one.

The allocation of the reliable criticalities to the units of the sub-system required a preliminary study, whose main steps were:

- Product tree definition;
- Reliability Block Diagram definition (R.B.D.);
- Preliminary Hazard Analysis;
- Functional Analysis;
- Functional-FMECA.

The RBD has allowed to divide the vacuum pump into six functional units, as follows (see Fig. 3).

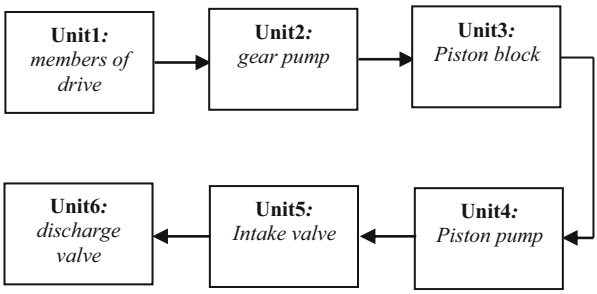


Fig. 3 Reliability block diagram

The Preliminary Hazard Analysis has enabled, besides, to determine two probable undesired events, for which we must fix some target hypotheses:

– loss of the functionality of the system (critical event);
– loss of the functionality of the system and of human lives (catastrophic event).

The functional blocks described have been the subject of a next functional analysis and FMEA. The FMEA is a technique of support to the critical examination of the system, during all the phases of its life cycle. The information supplied enables to determine the priorities for the process control and for the inspections, established during the construction and installation. These functional modules made it possible to estimate the factors characterizing the I.F.M. method, in order to allocate the reliability criticalities of the system. As regards the documents, it turned out that it was advantageous to realize the FMEA using modules drawn up specially for the system under examination, and prepared according to the purposes pursued. The information required by the module, subdivided into columns, was:

1. Number of identification of the element of the system taken into consideration;
2. Denomination of the element;
3. Function carried out by the element;
4. Ways and causes of failure;
5. Way of working of the element;
6. Effects of failure (local, superior, final);
7. Methods of pointing out of failure;
8. Compensatory measures foreseen;
9. Classes of gravity (critical and catastrophic).

3.3 Reliability Allocation Values

The reliability allocation has been done by the application of the "Integrated Factors Method", first version. So we have stressed the versatile and modulate structure of I.F.M. method. The S (technology index) and E (electronic functionality index) parameters of allocation are not discriminating for the components examined. In fact, all the plunger pump units are completely electromechanical

(E = 0.1) and off-the-shell type (S = 0.5 traditional components). *For each RBD unit, we have estimated the necessary indexes for the allocation by the application of a Functional Analysis-FMECA and an Expert Judgement's help. Starting from the evaluation of the indexes:*

- Complexity K;
- Critically C;
- Functionally F;
- Effectiveness O;

we have calculated:

- the value of the Global index (IG) relative to the sub-systems for each top event (Critical and Catastrophic Event);
- the value of the percentage global index (IG%) for each unit;
- the unreliability allocated values U_i;
- the consequent reliability allocated values R_i,

The results obtained for the critical event are shown in Table 2.

The I.F.M allocation results, in terms of IG%, are the following (Figs. 4, 5 and 6)

Then, we have allocated the unreliability target $U_s = 3.00 \times 10^{-1}$.

Since the reliability values R_i are: $R_i = (1-U_i)$, it is possible to obtain the reliability allocated values for each units analysed:

Starting from an analysis of the results obtained, it is possible to notice:

- the proposed method is able to carry out a very particularized allocation, selecting among the different units of the system;
- the method is able to allocate the greater U_s value to the units that have a high Complexity K and Functionality F value indexes (for instance, transmission parts).

Table 2 Allocation factors values (Allocated unreliability $U_s = 0.15$)

	Critical event target allocation					
I.F.M. factors	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5	Unit 6
c_1: n° of critical functions	*18*	*12*	*6*	*5*	*6*	*5*
c_2: n° of unit functions	*30*	*14*	*10*	*15*	*18*	*8*
C = (c_1/c_2)	0.60	0.86	0.60	0.33	0.33	0.63
f_1: n° of unit functions	*30*	*14*	*10*	*15*	*18*	*8*
f: n° of plunger pump	*95*	*95*	*95*	*95*	*95*	*95*
F = (f_1/f)	0.32	0.15	0.11	0.16	0.19	0.08
O(E.J.)	1	0.67	1	0.67	0.67	0.67
K (E.J.)	0.9	0.8	0.5	0.8	0.4	0.4
IG	**0.47**	**0.09**	**0.09**	**0.25**	**0.15**	**0.04**
IG%	**43.22**	**8.41**	**8.00**	**23.17**	**13.90**	**3.29**
U_s target	**3.00×10^{-1}** *(data banks)*					
U_i (%)	**12.97**	**2.52**	**2.40**	**6.95**	**4.17**	**0.99**
R_i (%)	**87.03**	**97.48**	**97.60**	**93.05**	**95.83**	**99.01**

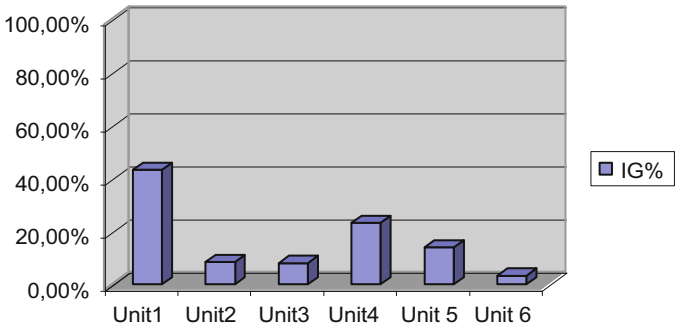


Fig. 4 Percentage global index IG%

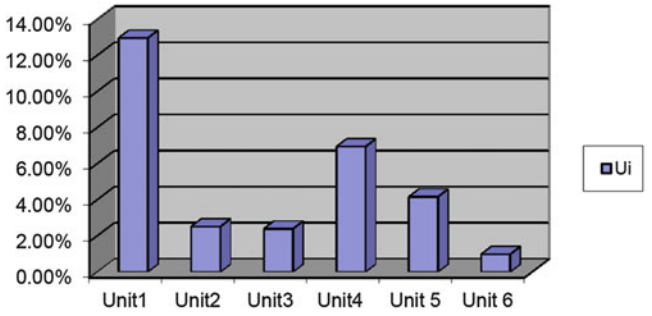


Fig. 5 Unreliability allocated values

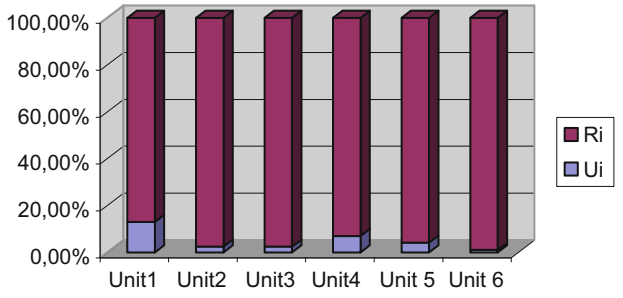


Fig. 6 Comparison between R_i and U_i parameters

In short, the method proposed shows the following advantages:

- it is not necessary to know reliability data of similar units, so we can apply the method to innovative systems too;
- it reduced subjectivity through an exact quali-quantity definition of K,O indexes;
- it is possible to introduce or eliminate factors, adapting the method to the system and to the project phase;
- simple analytical treatment.

Table 3 Reliability databanks

R_i Databanks						
	Unit 1 (FTA)	Unit 2	Unit 3	Unit 4	Unit 5	Unit 6
$R_{i\ (\%)}$	88.20	95.58	96.50	94.80	96.54	94.25

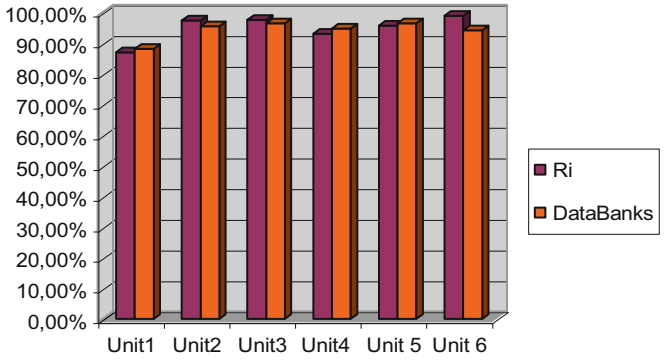


Fig. 7 Comparison between R_i and databanks parameters

3.4 Results Comparison

Subsequently, we have compared the I.F.M. results with the reliability data, obtained from databanks supplied by building firms or obtained through FTA (Table 3).

It is possible to notice that:

- the allocated reliability values are comparable to the supplied reliability ones;
- the units performance are respected (Fig. 7).

These considerations enable to legitimate the new method and its applicability to complex systems, like plunger pump.

4 Critical Flows Method

The new allocation methodology developed has been called Critical Flows Method (Di Bona et al. 2016). This new reliability allocation method wants to be a methodology "ad hoc" for the system examined, but it can also be extended to any complex system (series and parallel).

The starting point was the analysis only of significant units, according to experience. This is an indispensable indication to explain the so-called "buffer effect" (parallel configuration). The choice to limit the analysis to a very low

number of elements, depending on the particular Top Event, has led to less dispersed results, creating a scale of criticality and identifying priorities and hierarchies.

The previous analysis of the other methods, showed the need to use appropriate factors of influence to discriminate among the different system units (series and/or parallel configurations). The factors chosen were as follows:

Criticality—Index A_1 It permits to estimate the effects on a Top Event caused by a total or partial failure of a single unit. The method will involve higher reliability to less critical systems. It varies between 0 (∞ units in parallel configuration) for a low criticality of the unit and 1 (series configuration) for absolutely critical items. The criticality index is evaluated through the following ratio:

$$A_1 = \frac{1}{n} \tag{25}$$

Where "**n**" is the number of "*buffer elements*" (parallel configuration) that can oppose a risk implementation. For example, two units in series n = 1 (no buffer elements) and $A_1 = 1$, three units in parallel n = 3 (buffer elements) $A_1 = 0.33$.

State of the Art-Technology—Index A_2 It is the technological level of a unit. The method will involve higher reliability to most technologically advanced elements. It varies between 0 (ideally) for old design elements and 1 for newly developed units.

Complexity—Index A_3 It evaluates the complexity of the units, in terms of structure, assembly and interactions. The method will tend to associate higher reliability to less complex elements. We introduced three different levels of subsystem complexity, with three numerical values associated (Table 4).

Running Time—Index A_4 It values the operating time of a unit in comparison with the total time of the mission. The method will tend to involve higher reliability to units working for a lower average time. It is defined as the ratio between the average operation time of single element and the average time of the mission. For each unit the index T is given by the following ratio:

$$T = \frac{T_u}{T_s} \tag{26}$$

Operation Profile—Index A_5 It is representative of operating conditions, in terms of working stress. The method will associate more reliability to those elements working in less difficult environmental conditions. We introduced three different

Table 4 Subsystem complexity values

Value	Subsystem
0.33	No complex subsystem
0.66	Normal complexity
1	Complex subsystem

Table 5 Values for severity of environmental conditions

Value	Subsystem
0.33	Easy operative conditions
0.66	Normal operative conditions
1	Difficult operative conditions

levels for severity of environmental conditions, with three different numerical values associated (Table 5):

After the above evaluations, thanks to an Expert Judgement, it's possible to determine the Global Index (GI) for the reliability allocation of the system, defined as follows:

$$GI_i = \left(A_{i1}A_{i2}{A_{i3}}^{-1}A_{i4}A_{i5}\right) \quad i = 1, \ldots.., k \tag{27}$$

where GI_i is the Global Index of the specific unit of the system.

This method involves now calculating the GI weight of each unit, according to the following formulation:

$$w_i = \frac{GI_i}{\sum_{j=1}^{n} GI_j} = \frac{\left(A_{i1}A_{i2}{A_{i3}}^{-1}A_{i4}A_{i5}\right)}{\sum_{i=1}^{k}\left(A_{i1}A_{i2}{A_{i3}}^{-1}A_{i4}A_{i5}\right)} \quad i = 1, \ldots.., k \tag{28}$$

Where w_i is the global weight of the i-th unit, compared to the indexes of other units and k is the number of analyzed units. After the evaluation of the global index for each unit, it is possible to allocate the system reliability target using Eq. (6): $R_i(t) = R(t)^{W_i}$

4.1 Critical Flows Method Application

The Critical Flows method has been applied to a cooling system, representing a fundamental subsystem of the toroidal system for thermonuclear fusion.

In order to obtain the energy production through controlled thermonuclear fusion, it is necessary to heat a plasma of deuterium–tritium up to very high temperatures (about 10^8 °C), keeping the hot plasma confined in a magnetic field, able to force particles to follow spiral trajectories, away from the container walls (*magnetic confinement*).

In magnetic confinement fusion hot plasma is enclosed inside a vacuum chamber.

We have studied two different magnetic configurations:

- Mirror configuration;
- Toroidal symmetry configuration.

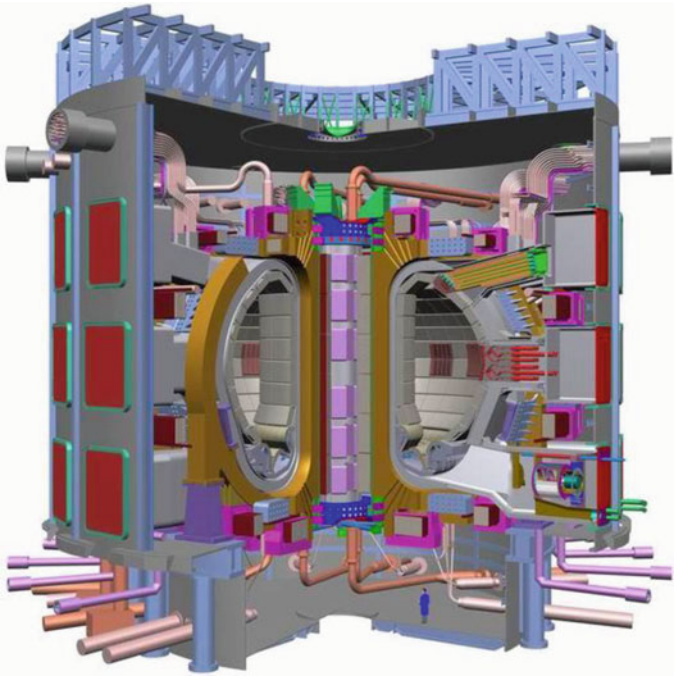


Fig. 8 Toroidal machine

Today, the most used configuration is the toroidal one (Fig. 8). In this case, the toroidal magnetic field is produced by copper coils positioned around a cavity in the centre.

The generation of a high magnetic field inside the chamber is due to a current of 37.8 kA for a period of about 1.5 s. Therefore, it is necessary to cool the vacuum chamber and coils through a closed circuit of liquid nitrogen, characterized by (Fig. 9):

- Three storage tanks of liquid nitrogen, total capacity of 90,000 l, pressure of 2.5 bar;
- Two cryogenic pumps, lubricated by the same liquid nitrogen, delivery of about 30 m^3/h;
- Two evaporators;
- Tanks, valves and typical accessories.

The nitrogen pipes reach the cryostat, the main component of the plant, containing the toroidal system, covered by a polymeric material. Inside the cryostat, pressure is bigger than outside (20 mm H_2O), in order to avoid the possibility of entry of atmospheric air, in case of sealing problems at the equatorial doors. In fact, the air humidity freezes and forms dangerous layers of ice (work temperature of −190 °C).

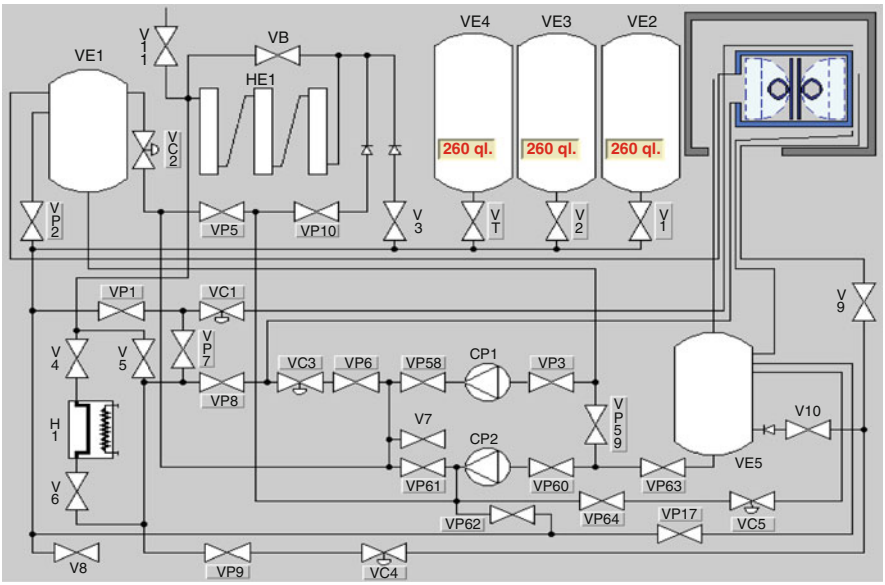


Fig. 9 Cooling system

The mission of the cooling system is to guarantee correct environmental operating conditions of the toroidal machine. Initially, the copper coils are cooled up to a temperature of −190 °C, needed to have specific values of resistivity and consequently high currents (37.8 kA), required to produce the magnetic fields necessary for plasma confinement.

Through a Reliability Block Diagram (RBD), we have divided the whole system into functional blocks in series, in order to realize the reliability analysis (Karmiol, Bracha and FOO Methods). The identified units are:

- Unit 1. Manual valves.
- Unit 2. Safety valves.
- Unit 3. Restraint valves.
- Unit 4. On-off valves.
- Unit 5. Solenoid valves.
- Unit 6. Breaking discs.
- Unit 7. Pressure valves.
- Unit 8. Self-regulation valves.
- Unit 9. Pressure-regulation valves.
- Unit 10. Level valves.
- Unit 11. Cryostat.
- Unit 12. Liquid nitrogen tanks.
- Unit 13. Separation tank.
- Unit 14. Collection tank.
- Unit 15. Main evaporators.

Table 6 Preliminary hazard analysis

Top event	Minor	Marginal	Critical	Catastrophic
Frequent				
Probable				
Occasional	CoolingCycle interruption (1) Nitrogen outflow (2)	Low pressure in cryostat		
Rare				Damage in cryostat
Improbable				

Table 7 Reliability target values (*Life Circle = 25years*)

Top event	Accepted faults/ mission	λ faults/ mission	λ faults/ year (2mission/ year)	Reliability target (%)	Allocated unreliability (%)
T.E.1: Catastrophic	1/500	0.002	0.004	90.48	9.52
T.E.2: Marginal	1/250	0.004	0.008	81.87	18.13
T.E.3: Minor (1)	1/250	0.004	0.008	81.87	18.13
T.E.4: Minor (2)	1/250	0.004	0.008	81.87	18.13

– Unit 16. Secondary evaporators.
– Unit 17. Heater.
– Unit 18. Cryogenic pumps.
– Unit 19. Compressed air system.
– Unit 20. Measure modules.

In the next phase, we have defined Top Events through (Table 6) a Preliminary Hazard Analysis (PHA).

For each top event, we have fixed a reliability target value, relating to the knowledge of the system and to planned or expected goals (Table 7).

4.2 Reliability Allocation Using Literature Methods

Before applying the CFM, allocation indexes have been evaluated, by the application of FOO, Karmiol and Bracha methods, through a Functional and FMECA Analysis, starting from the RBD developed (only series-configuration). The following tables show the allocation results for each top event using FOO Method (Table 8, Fig. 10), Karmiol Method (Table 9, Fig. 11) and Bracha Method (Table 10, Fig. 12):

Bracha method, differently from the previous ones, does not refer to Top Events identified in PHA. The starting point is simply a reliability target identified by a

Table 8 FOO method

Unit	T.E. 1	T.E. 2	T.E. 3	T.E. 4
	90.48%	81.87	81.87	81.87
1. Manual valves	0.992267	0.984916	0.98532	0.988216
2. Safety valves	0.996542	0.991703	0.989993	0.992863
3. Restraint valves	0.996542	0.990964	0.991471	0.992014
4. On-off valves	0.98881	0.977761	0.97827	0.97934
5. Solenoid valves	0.996852	0.993339	0.994276	0.995282
6. Breaking discs	0.988111	0.97827	0.97882	0.977121
7. Valves at static	0.997861	0.994687	0.995185	0.995992
8. Self-regulation valves	0.996732	0.993729	0.995714	0.997201
9. Pressure-regulation valves	0.993875	0.987541	0.988295	0.989225
10. Level valves	0.994894	0.989567	0.990063	0.991244
11. Cryostat	0.997731	0.991503	0.99202	0.992334
12. Liquid nitrogen tanks	0.996323	0.99299	0.993498	0.997111
13. Separation tank	0.995304	0.990964	0.991471	0.995082
14. Collection tank	0.995304	0.990964	0.991471	0.995082
15. Main evaporators	0.988111	0.97827	0.97882	0.977121
16. Secondary evaporators	0.988111	0.97827	0.97882	0.977121
17. Heater	0.988111	0.97827	0.97882	0.977121
18. Cryogenic pumps	0.995833	0.991703	0.99181	0.993163
19. Compressed air system	0.996133	0.992441	0.992948	0.993713
20. Measure modules	0.996892	0.993808	0.994346	0.995232

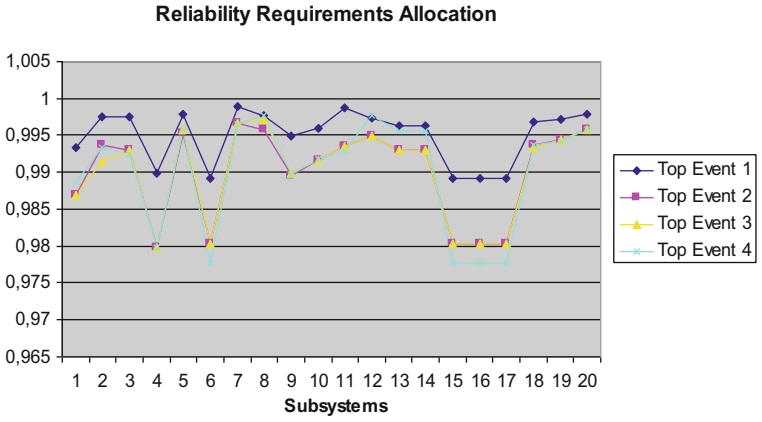


Fig. 10 Top event comparison—FOO method

numerical goal. To realize a comparison, the analysis was developed on two targets of PHA.

The analysis carried out with FOO Method has meant results not empirically verifiable (break discs would seem to be critical in terms of single Top Events).

Table 9 Karmiol method

Unit	T.E. 1	T.E. 2	T.E. 3	T.E. 4
	90.48	81.87	81.87	81.87%
1. Manual valves	0.99656	0.99258	0.99297	0.99263
2. Safety valves	0.99563	0.99191	0.99233	0.99320
3. Restraint valves	0.99563	0.99258	0.99297	0.99376
4. On-off valves	0.99219	0.98315	0.98340	0.98526
5. Solenoid valves	0.99406	0.98854	0.98723	0.98810
6. Breaking discs	0.99750	0.99460	0.99489	0.99546
7. Valves at static	0.99375	0.98989	0.99042	0.99150
8. Self-regulation valves	0.99625	0.99191	0.99106	0.98810
9. Pressure-regulation valves	0.99219	0.98584	0.98404	0.98696
10. Level valves	0.99157	0.98584	0.98659	0.98696
11. Cryostat	0.99375	0.99258	0.99297	0.99376
12. Liquid nitrogen tanks	0.99656	0.99258	0.99297	0.98866
13. Separation tank	0.99656	0.99258	0.99297	0.98866
14. Collection tank	0.99656	0.99258	0.99297	0.98866
15. Main evaporators	0.99750	0.99460	0.99489	0.99546
16. Secondary evaporators	0.99750	0.99460	0.99489	0.99546
17. Heater	0.99750	0.99460	0.99489	0.99546
18. Cryogenic pumps	0.99406	0.98854	0.98914	0.98923
19. Compressed air system	0.99594	0.99123	0.99170	0.99263
20. Measure modules	0.99344	0.98786	0.98531	0.98866

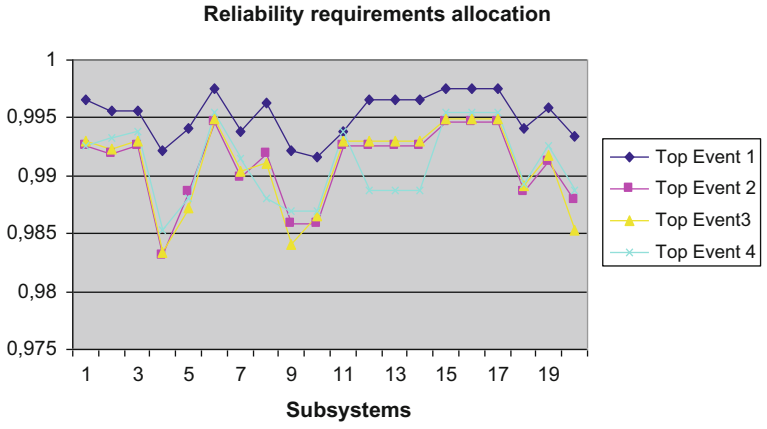


Fig. 11 Top event comparison—Karmiol

The results of Karmiol Method led to the following assessments:

– there are high values of allocated reliability (series configuration);
– the values dispersion is around a mean value: it is possible to note a good difference between the values allocated.

Table 10 Bracha method

Unit	Target goal	
	90.48%	81.87%
1. Manual valves	0.99816	0.99633
2. Safety valves	0.99472	0.98948
3. Restraint valves	0.99394	0.98793
4. On-off valves	0.99341	0.98686
5. Solenoid valves	0.99343	0.98691
6. Breaking discs	0.99801	0.99603
7. Valves at static	0.99489	0.98981
8. Self-regulation valves	0.99392	0.98788
9. Pressure-regulation valves	0.99313	0.98632
10. Level valves	0.99285	0.98576
11. Cryostat	0.99416	0.98836
12. Liquid nitrogen tanks	0.99584	0.99169
13. Separation tank	0.99394	0.98793
14. Collection tank	0.99394	0.98793
15. Main evaporators	0.99646	0.99295
16. Secondary evaporators	0.99690	0.99382
17. Heater	0.99967	0.99934
18. Cryogenic pumps	0.99455	0.98914
19. Compressed air system	0.99507	0.99507
20. Measure modules	0.99314	0.98633

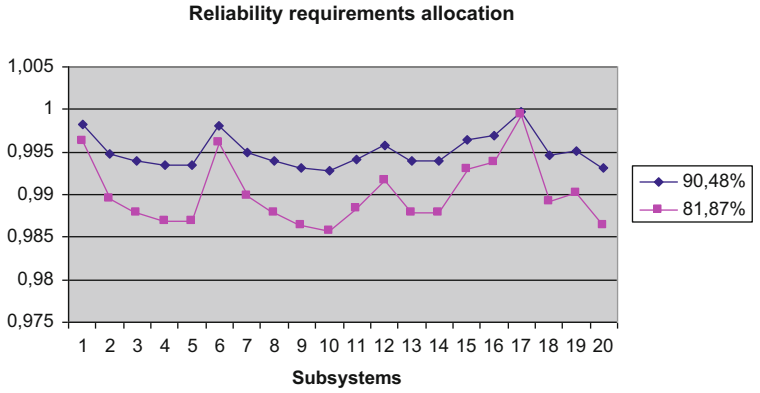


Fig. 12 Top event comparison—Bracha

Differently, the results of Bracha Method led to other considerations:

- there are high values of allocated reliability (series configuration);
- it is clear what are the main weaknesses of the plant. There are some low values, but they are quantitatively very comparable;
- the values are characterized by a lower dispersion around the average value.

Table 11 Methods comparison

Method	Corresponding to CS	Not corresponding to CS
FOO	Analysis oriented through indexes	Reference to the functional units The analysis does not calculate the buffer effect
Karmiol sum	Analysis oriented through indexes Reference to the link between unity and Top Event	No information on operating cycles The analysis does not calculate the buffer effect
Bracha	The allocation parameters are based on intrinsic nature of units, on the operating conditions and on possible stress	No reference to the link between unity and Top Event All elements have the same functional importance The analysis does not calculate the buffer effect

Finally, it was noted that there isn't any reference to a potential "buffer effect" (parallel configuration) that means a single unit failure balanced by another or more elements. In the analyzed RDB, there is no functional duplicate installed in parallel, but only components in series. In summary (Table 11):

Starting from the comparison results we proposed a new reliability approach. The guidelines for the development of a proper allocation model can be summarized in the following four points:

- generality;
- standardization of input data;
- economy;
- definition of realistic and achievable requirements.

4.3 Reliability Allocation Using Critical Flows Method

Starting from PHA, the proposed method was applied, and was based on goals established for each Top Event.

The reality RBD of the Cooling System is not a series-configuration, but a series-parallel configuration.

In particular, the group of elements is relating to the investigated Top Event. In reality, not all 20 units are relating to every Top-Event as we have to considerate to apply conventional methods. That's why RBD, for each of the four Top Events, was constantly modified according to F-FMECA tables. The mathematical structure of CFM allows identifying preliminary critical path, composed by the subgroups of elements that have influence in the analysis and its "buffer effects" (parallel configuration).

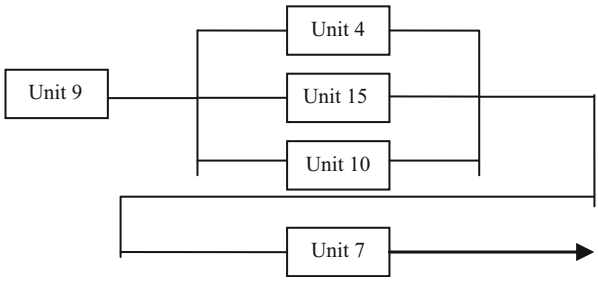


Fig. 13 RBD for the second Top event

Table 12 Allocation of units' indexes

Elements	n	A_1	A_2	A_3	A_4	A_5	IG	w_i	$R(t)$	λ_{CFM}
Unit 9	1	1	0.50	1	1	0.66	1.32	0.224957	0.955998	0.02999
Unit 4	3	0.33	0.16	1	1	1	2	0.340843	0.934091	0.04545
Unit 15	3	0.33	0.25	1	0.50	0.33	0.21	0.037118	0.992603	0.00494
Unit 10	3	0.33	0.50	1	0.50	1	0.33	0.056239	0.988813	0.00749
Unit 7	1	1	0.50	1	1	1	2	0.340843	0.934091	0.04545

During the reliability modelling, the "buffer effect" is realized by the structuring of some parallel subgroups in RBD, and with a quantitative allocation of indexes of redundancy. This procedure was implemented for all Top Events. The following diagram describes the implementation of CFM to the second Top Event (low pressure in the cryostat). The reliability block diagram for this Top-Event is showed in Fig. 13:

The diagram shows that the maintaining of pressure depends on the cycle of pressurization, but also by the presence of liquid nitrogen in the collection tank. Some nitrogen, present in the tank, evaporates, contributing to maintain a fixed level of pressure in the cryostat. In the below Table 12, there is the allocation of indexes for the units under analysis:

The results show two problems relating to units 7 and 9 (level regulation valve and pressure regulation valve). The method suggests to fill the collection tank, through unit 7, in order to contribute to the pressurization of the cryostat, otherwise the risk increases. A similar critical state is highlighted in the cycle of pressurization, in which a failure of unit 9 could close the access to gaseous nitrogen cryostat. In the same cycle, unit 10 shows less importance, because it works in operating conditions less stressful, being subject to a reduced number of cycles of opening and closing. Finally, as unit 10 evaporators and valves are not so important (parallel configuration) ; therefore the method assigns relatively high values of reliability. In order to verify the CFM approach, we calculate the reliability system with allocated reliability value. The result is:

$$\mathbf{R}^*(\mathbf{t} = \mathbf{2mission/year}) = \mathbf{0.8929} > \mathbf{R_{target}}(\mathbf{t} = \mathbf{2mission/year}) = \mathbf{0.8713}$$

4.4 Results Comparison

Subsequently, we have compared the CFM results with the reliability data (Table 13), obtained from databanks supplied by manufacturers or obtained experimentally.

It is possible to notice that:

– the allocated reliability values are comparable to the supplied reliability ones;
– the units performances are respected (Fig. 14)

The comparison showed that the methodology introduced provides data consistent with literature, respecting and highlighting hierarchies of performance among units. So it's possible to affirm that the new methodology gives output-data in conformity with those coming out from data banks or manufacturing firms, pointing out the different reliability levels of the system units. The reason is simply: the proposed method is designed to series-parallel configuration not only to series configuration. Then, we have compared the values obtained by the application of the literature allocation techniques with reliability data coming out from data banks or manufacturing firms, and we calculated the Mean Absolute Deviation percentile (MAD) of error percentile (ε) between values calculated (CFM, FOO, Karmiol and Bracha) and values of data banks (Table 14).

Table 13 Reliability data banks

Databanks					
	Unit 9	Unit 4 (experimentally)	Unit 15	Unit 10	Unit 7 (experimentally)
λ	0.03016	0.05301	0.00371	0.00500	0.03840

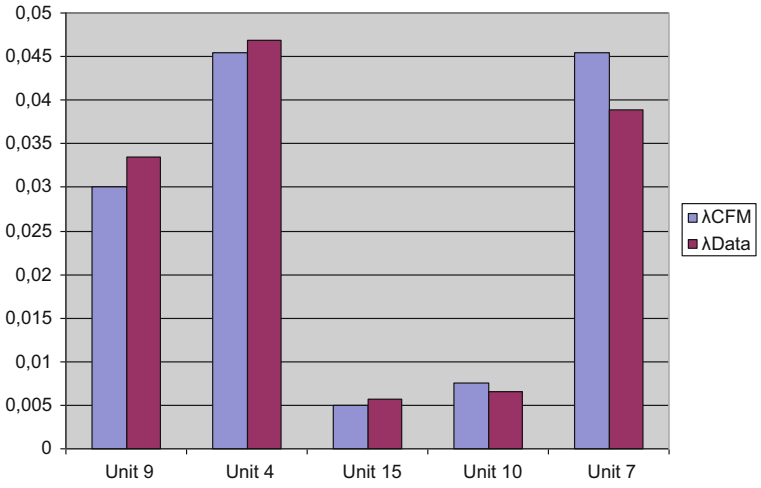


Fig. 14 Reliability data comparison

Table 14 Comparison of failure rate with different methods

	λ_{CFM}	λ_{Data}	$\acute{\varepsilon}$ (%)	λ_{FOO}	λ_{Data}	$\acute{\varepsilon}$ (%)	$\lambda_{Karmiol\text{-}sum}$	λ_{Data}	$\acute{\varepsilon}$ (%)	λ_{Bracha}	λ_{Data}	$\acute{\varepsilon}$ (%)
Unit 9	0.02999	*0.03352*	**10.53103**	0.007179	*0.03352*	**78.5844**	0.009507	*0.03352*	**71.63642**	0.009183	*0.03352*	**72.60455**
Unit 4	0.04545	*0.0468*	**2.884615**	0.014646	*0.0468*	**68.70431**	0.011329	*0.0468*	**75.79263**	0.008818	*0.0468*	**81.15799**
Unit 15	0.00494	*0.005642*	**12.4424**	0.014272	*0.005642*	**152.9542**	0.00361	*0.005642*	**36.01994**	0.004717	*0.005642*	**16.40117**
Unit 10	0.00749	*0.00661*	**13.31316**	0.00666	*0.00661*	**0.753723**	0.009507	*0.00661*	**43.83469**	0.009562	*0.00661*	**44.65317**
Unit 7	0.04545	*0.03891*	**16.80802**	0.003221	*0.03891*	**91.72166**	0.006774	*0.03891*	**82.58982**	0.006828	*0.03891*	**82.45134**
		MAD_{CFM}	**11.19%**		MAD_{FOO}	**78.54%**		$MAD_{Karmiol\text{-}sum}$	**61.97%**		MAD_{Bracha}	**59.45%**

The result shows that the CFM method obtains a more reasonable reliability allocation rating than the conventional methods. Concluding, it's possible to affirm that the new methodology gives output-data more in conformity with data banks.

$$MAD_{CFM} < (MAD_{FOO}; MAD_{Karmiol-sum}; MAD_{Bracha})$$

Furthermore, it is possible to note that λ_{FOO}, $\lambda_{\text{Karmiol-sum}}$, λ_{Bracha} (10^{-3}) failure rate allocated are lower than λ_{CFM} (10^{-2}) ones. This is a very important factor in economical analysis. In reality, to design and manufacture a subsystem with such an extremely low failure rate would consume a considerable amount of resources.

5 Conclusion

The investigation of different allocation methods, made it possible to evaluate the advantages and capabilities of each one. The unreliability allocation by using of a large number of influencing factors seems to be more capable of considering appropriately the importance of each factor and each unit of the specific system under consideration. Definitely, a more careful characterization thanks to many factors, produces a detailed allocation. The application confirmed a better matching reliability data provided by databanks and literature.

Initially, in the chapter, an overview of traditional allocation methods is presented, then in order to overcome some limits of those methods, two innovative methods and their applications are proposed. Therefore, a comparison of results is described for:

- The "Integrated Factors Method", applied to a production sub-system for sintered products. In particular, the considered sub-system makes it possible to carry out the drying of dusts.
- The "Critical Flows Method", applied to a cooling system of the toroidal system for thermonuclear fusion.
- The application of IFM to the case study, made it possible to investigate the mathematical structure. The obtained results confirmed a better match to the hierarchies of reliability provided by the databanks and literature; a less restrictive target than other allocation techniques.
- The application of CFM showed that the developed methodology provides data consistent with literature, respecting and highlighting hierarchies of performance among units. The proposed method is designed for series–parallel configurations, not only for series ones. The result shows that CFM Method obtains a more reasonable reliability allocation rating than the conventional methods.

The new methodologies give output data more conforming with data banks and allows a more economical design of subsystems. The proposed methods can accurately and efficiently allocate reliability ratings throughout reasonably assigned

reliability levels in subsystems, meet customer needs, control reasonable support costs, and decrease manufacturing and maintenance costs.

The methods can also be used in a wide variety of different industries.

References

Barbarino F (1990) Product Safety Engineering. ISEDI

Balaban HS, Jeffers HR (1999) The allocation of system reliability. Vol. I. Development of procedures for reliability allocation and testing. Arinc Research Corporation, Washington DC

Boyd JA (1992) Allocation of reliability requirements: a new approach. Proceedings annual reliability and maintainability symposium

Jarrell G (2003) Supplier reliability program guide. The Cessna Aircraft Company, Wichita, KS

Advisory Group of Reliability of Electronic Equipment (AGREE) (1957) Reliability of military electronic equipment. Office of the Assistant Secretary of Defense Research and Engineering, Washington, DC

Karmiol ED (1965) Reliability apportionment. Preliminary report EIAM-5, Task II, General Electric, Schenectady, NY, pp 10–22

Bracha VJ (1964) The methods of reliability engineering. Mach Des 7:70–76

Department of Defense of USA (1988) MIL-HDBK-338B. Electronic design reliability handbook, pp 6/13–6/16

Falcone D, De Felice F, Di Bona G, Silvestri A (2004) R.A.M.S. analysis in a sintering plant by the employment of a new Reliability Allocation Method. Modelling and simulation. Marina del Rey, CA, pp 1–3, marzo 2004

Di Bona G, Silvestri A, Forcina A (2016) Critical flow method: a new reliability allocation approach for a thermonuclear system. Qual Reliab Eng Int 32(5):1677–1691. ISSN: 0748-8017

Domenico Falcone, degree in Mechanical Engineering, is full Professor of Industrial Plant at the University of Cassino and Southern Lazio. He worked with the Engineering Faculty of Naples, 1984–1994, and with the Engineering Faculty of Rome "TorVergata", 1987–1990. Since 1998, he is the Scientific Director of the laboratory of Management and Safety of Industrial Plants. His research interests include, process optimisation, simulation and quality management.

Alessandro Silvestri received a degree with full marks in Mechanical Engineering, University of Cassino. His awards are 'Young researcher project', University of Cassino (Process of identification and allocation of RAMS parameters: development and implementation of a new methodology for the reliability allocation), 'Six Sigma challenge', Italian Academy of Six Sigma (Six Sigma application to the optimization of the process parameters in a molding company). He is an Assistant Professor and a researcher of Industrial Plants at University of Cassino and Southern Lazio. He has more than 70 national and international publications (topics: logistics; reliability; process control).

Gianpaolo Di Bona is an Assistant Professor of Industrial Plants at University of Cassino and Southern Lazio. He received his Doctorate in Civil and Mechanical Engineering from University of Cassino. His recent publications include 'Assessment of the effectiveness of maintenance-oriented design' (International Journal of Engineering Business Management, 2014) and 'Validation and application of a reliability allocation technique (advanced integrated factors method) to an industrial system' (Proceedings of the IASTED International Conference on Modelling, Identification and Control, 2014). His research interests include RAMS analysis, process optimisation and statistical process control.

Antonio Forcina is an Assistant Professor of Industrial Plants at University of Naples 'Parthenope'. He received his Doctorate in Mechanical Engineering from University of Cassino and Southern Lazio. His recent publications include 'Proposal of a weighing algorithm for checking missing components in pharmaceutical packaging' (International Journal of Engineering Business Management, 2014) and 'A new method for reliability allocation: critical flow method (C.F.M.)' (Lecture Notes in Control and Information Sciences, 2015). His research interests include RAMS analysis, process optimisation, simulation and inventory management.

Integrated Engineering Approach to Safety, Reliability, Risk Management and Human Factors

Vanderley de Vasconcelos, Wellington Antonio Soares, and Raíssa Oliveira Marques

Abstract Nuclear industry has important engineering legacies to share with the conventional industry. As a result of nuclear accidents at Three Mile Island, Chernobyl, and Fukushima, many countries have incorporated new steps into the licensing processes of Nuclear Power Plants (NPP), in order to manage accident risks. Probabilistic Safety Analysis has been used for improving safety, reliability and availability in the design and operation of NPP. Despite the close association between these subjects, there are some important different approaches. The reliability engineering approach uses several principles and criteria to minimize the component failures. These include, for instance, redundancy, diversity, and standby systems. System safety is primarily concerned with risk management, that is, the evaluation and control of hazards, which requires the assessment of interactions among system components. Events that cause accidents can be complex combinations of component or instrumentation failures, faulty maintenance, design errors, or human actions. Then, system safety deals with a broader spectrum of risk management, including human factors (ergonomics), licensing requirements, and quality control. Taking care of these topics individually can compromise the completeness of the analysis and the measures associated to risk reduction, and increasing safety and reliability. This chapter presents an integrated framework for analyzing engineering systems, operational procedures, and the human factors based on the application of systems theory. An application example assessing safety, reliability, risk, and human factors issues related to a complex task of Non-destructive Inspection of piping segments of a primary circuit of a NPP shows the benefits of using the proposed integrated approach.

Keywords Safety • Reliability • Human errors • Risk management • Probabilistic Risk Assessment

V. de Vasconcelos (✉) • W.A. Soares • R.O. Marques
Centro de Desenvolvimento da Tecnologia Nuclear—CDTN, Belo Horizonte, Brasil
e-mail: vasconv@cdtn.br; soaresw@cdtn.br; raissaomarques@gmail.com

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_4

1 Introduction

Current developments for ensuring safe and competitive operation of industrial plants, such as nuclear facilities, in most countries, is largely based upon deterministic criteria using multiple layers of Defense-in-depth (DiD). Design basis accidents (DBAs) are then defined and safety systems incorporated into the design to respond to these accidents. In general, risk methods are not explicitly considered in the regulatory process although the selection of DBAs and their inclusion on Safety Analysis Reports implicitly include consideration of their risk potential (IAEA 2009).

As result of the nuclear accidents at Three Mile Island, Chernobyl, and Fukushima, many countries have incorporated additional steps to the licensing processes of Nuclear Power Plants (NPPs) in order to control accident risks. Lessons learned included recommendations to improve plant systems, resources, and operator training to effective responses to severe accidents (IAEA 2012). Probabilistic Risk Assessment (PRA) is used in the nuclear industry in the United States and in many other countries for analyzing accidents beyond-design-basis, such as Fukushima event. Sometimes named Probabilistic Safety Analysis—PSA, this approach is useful for improving safety, reliability and availability in design and operating of NPPs (NAS & USNRC 2014).

Although risk assessment is an integral part of evaluating NPP safety, the main strategy for designing and regulating such facilities remains in DiD philosophy. This involves the use of multiple redundant systems for preventing and mitigating components and human failures. In addition, Human Reliability Analysis (HRA) is typically performed as part of these PRAs (or PSAs) to quantify the likelihood of omission and commission errors, as well as fail in recovery actions.

The United States is an example of country where many application of PRA to regulatory issues have been carried out. Both the U.S. Nuclear Regulatory Commission (USNRC) and the regulated industry have made significant advances in the development and application of risk-based technology (USNRC 2011). Overall, there is clear evidence in all countries that PRA methods have become an important part of the safety, reliability, and risk management processes in support to regulation. These questions are normally treated individually and without considering systematically human factors that have significant impact on operational effectiveness and risk assessment and management (Cox and Tait 1998).

On the other hand, the use of common tools in the analysis of each one of these subjects, as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), and Event Tree Analysis (ETA), is a clear indication that an integrated evaluation is feasible (USNRC 2001). This integrated approach is also particularly important when implementing Quality, Safety, Health, and Environment Integrated Management Systems following ISO 9001, BS 8800, OHSAS 18001, and ISO 14001 standards. Such systems cannot assure legal compliance, but if they are effective, they can help the organizations to know better their compliance status, so that

preventive and corrective actions can be efficiently implemented (Vasconcelos et al. 2009).

This chapter proposes an integration of safety, reliability, risk management and human factors issues based on the application of systems theory. Section 2 presents main terminology and concepts related to safety assessment, risk management, reliability engineering, human factors and ergonomics. Section 3 presents an overview of the integrated framework based on systems theory. Section 4 describes briefly the common tools used in the integrated analysis, as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), Event Tree Analysis (ETA), and Technique for Human Error Rate Prediction (THERP), including mathematical and statistical basis. Section 5 presents a simple representative example to illustrate the benefits of integrated engineering approach to safety, reliability, risk management and human factors for a generic Loss of Coolant Accident (LOCA) in a Nuclear Power Plant. Finally, the conclusions about the integrated framework and summary about application example are presented in Sect. 6.

2 Terminology and Concepts

In the scope of this chapter, there are many concepts and terminology adopted within an integrated engineering approach to safety, reliability, risk management and human factors.

2.1 Safety Assessment

ALARP "As Low as Reasonably Practicable" is a principle usually applied to risks in some areas as radiation protection and chemical accident prevention, preparedness and response that fall below a defined level of "intolerable" risk. This principle recognizes that not all risk can be eliminated; there will be always a residual risk of an accident since it may not be practicable to take further actions to reduce the risk or to identify the potential accidents (HSE 2017). The associated term used in Nuclear Regulatory Commission (NRC) standards is ALARA (As Low As Reasonably Achievable). ALARA means making every reasonable effort to maintain exposure to ionizing radiation as far below the dose limits as practical, consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, economic factors, and public interest (USNRC 2017).

Safety Assessment Safety can be seen as a practical certainty that adverse effects will not result from exposure to an agent under defined circumstances (Christensen et al. 2003). Safety assessment is therefore a systematic process that is carried out throughout the design process (and throughout the lifetime of the facility or the

activity) to ensure that all the relevant safety requirements are met by the proposed (or actual) design. Safety assessment includes the formal safety analysis, i.e., it includes the evaluation of the potential hazards associated with the operation of a facility or the conduct of an activity (IAEA 2016a, b).

Defence-in-depth (DID) It is an established safety philosophy, in which multiple lines of defence and safety margins are applied to the design, operation, and regulation of plants to assure that public health and safety are adequately protected. NRC statement for DID is a safety philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs. This philosophy ensures that the public is adequately protected, and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the safety philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility (ANS 2016).

Design Basis Accidents (DBA) Design-basis accidents are postulated accidents that are used to set design criteria and limits for the design and sizing of safety-related systems and components. When developing a nuclear power plant, DBAs are selected to ensure that plant can withstand and recover from these accidents (USNRC 2013).

Deterministic Safety Analysis It is the engineering analysis of a plant response using validated models, calculations and data that predict transient response of the plant to an event sequence typically uses conservative estimates, safety margins and DBAs, and it is based on expert judgement and knowledge of the phenomena being modelled (ANS 2016).

Probabilistic Safety Assessment (PSA), also referred to as Probabilistic Risk Analysis (PRA) PSA or PRA is a qualitative and quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release and its effects on the health of the public, in the case of NPP (ANS 2016).

2.2 Risk Management

Risk There are many different definitions of risk. In the scope of this chapter, risk is a comprehensive set of event sequences, a quantitative assessment of the event sequence frequencies and their consequences, and an evaluation of the uncertainties in the assessments (Christensen et al. 2003; WHO 2004; ANS 2016). Mathematically this can be expressed as a product of frequency of occurrence and severity, as shown in Eq. 1 (USNRC 1975).

$$Risk\left[\frac{consequence}{time}\right] = frequency\left[\frac{event}{time}\right] \times severity\left[\frac{consequence}{event}\right] \quad (1)$$

Hazard It is an event or a natural phenomenon that poses some risk to a facility. Internal hazards include events such as equipment failures, human failures, and flooding and fires internal to the plant. External hazards include events such as flooding and fires external to the plant, tornadoes, earthquakes, and aircraft crashes (Lees 2012).

Hazard Analysis It is the determination of material, system, process, and plant characteristics that can produce undesirable consequences, followed by assessment of hazardous situations associated with a process or activity. Qualitative techniques are normally used to pinpoint weaknesses in design or operation of the facility that could lead to hazardous material releases. The hazard analysis examines the complete spectrum of potential events that could expose members of the public, facility workers, and the environment to hazardous materials (Lees 2012).

Risk Assessment Refers to technical estimation of nature and magnitude of a risk. It involves basically answers to three questions: What can go wrong? How frequently does it happen? What are the consequences? Figure 1 illustrates the risk assessment process. Risk assessment is a process for measuring, qualitatively and quantitatively, the risks a particular agent represents for a specific system or facility (Stamatelatos 2002).

Risk Management It is a systematic application of management policies, procedures and practices of establishing the context, identifying, analyzing, planning, implementing, controlling, communicating and documenting risks in a way that will enable organizations minimizing loss and maximizing opportunity in a cost-effective way (Stamatelatos 2002; IAEA 2001). A risk management process is illustrated in Fig. 2.

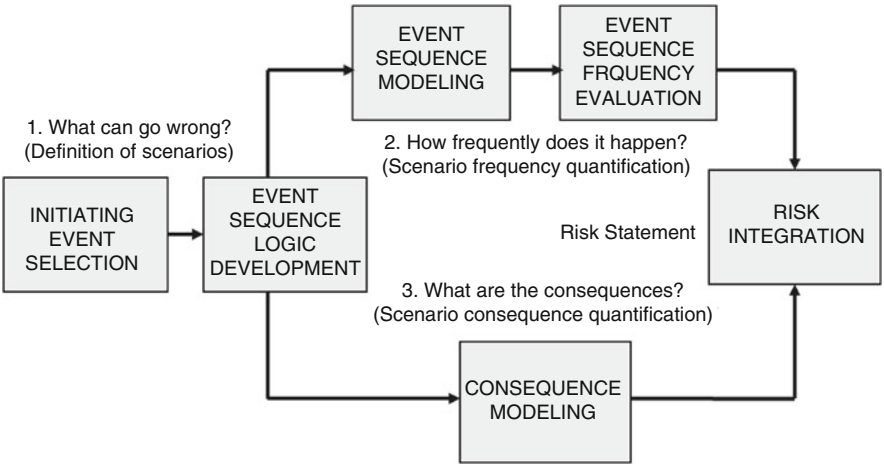


Fig. 1 Illustration of a risk assessment process (adapted from Stamatelatos 2002)

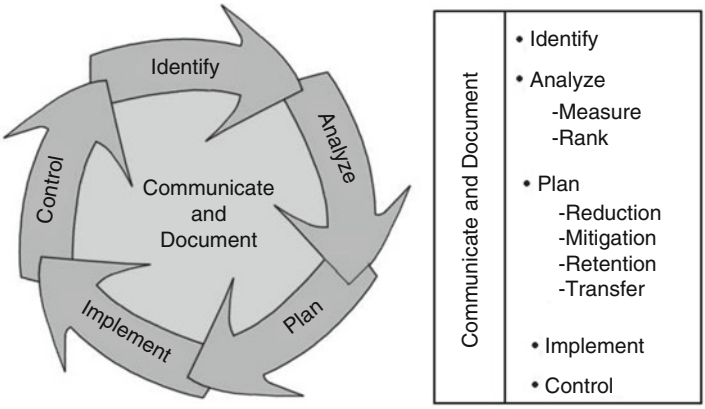


Fig. 2 Illustration of risk management process

Risk management activities encompass the following steps:

- **Identify**. States the risk in terms of conditions and consequences; capture the context of risk; e.g., what, when, where, how, and why.
- **Analyze**. Evaluates probability and severity, prioritizes and classifies groups with similar or related risks.
- **Plan**. Identifies techniques or strategies to manage the risk, including actions to mitigate, transfer or retain risks.
- **Implement**. Carries out the chosen techniques or strategies.
- **Control**. Analyzes results, decides how to proceed (re-plans, closes the risk, invokes contingency plans, continues tracking, etc.) and executes control decisions, providing feedback so that risk analysis is always updated.
- **Communicate and document**. Essential risk status is to be documented and communicated on a regular basis to the entire team.

2.3 Reliability Engineering

System is a collection of interrelated parts (components) that work together by way of some driving process. In this context, reliability is defined as the probability that an engineering system will perform its intended function satisfactorily for its intended life under specified environmental and operating conditions. Reliability is basically a design parameter and must be incorporated into the system at the design stage. Then, it is an inherent characteristic of the system, just as is its capacity or performance. To analyze and measure the reliability characteristics of a system, there must be a mathematical and a logical model of the system that shows the functional relationships among all the components, the subsystems, and

the overall system. The reliability of a system is a function of the reliabilities of its components. A system reliability model consists of some combination of a reliability data through use of techniques like block diagrams or fault trees. A definition of all equipment failure and repair distributions and a statement of spare and repair strategies are necessary (IAEA 2016a).

Since component failure characteristics can be described by distributions, the system reliability is actually time-dependent (ReliaSoft 2015). Assuming an exponential life distribution, the reliability of the component i as function of time, t, $R_i(t)$, is:

$$R_i(t) = e^{-\lambda_i t}, \tag{2}$$

where λ_i is the failure rate of component i.

Mean life (or Mean Time to Failure, MTTF) can be obtained by integrating system reliability function from zero to infinity:

$$MTTF = \int_0^\infty R_i(t)dt = \int_0^\infty e^{-\lambda_i t}dt = \frac{1}{\lambda_i}. \tag{3}$$

As reliability of a system is the probability that a system will operate successfully by a given time, in dealing with repairable systems, these definitions need to be adapted to deal with the case of the renewal of systems/components. Repairable systems receive maintenance actions that restore system components when they fail. These actions change the overall makeup of the system.

Maintainability, $M_i(t)$, is defined as the probability of performing a successful repair action within a given time, t. In other words, maintainability measures ease and speed a system can be restored to its operational status after a failure occurs. In maintainability, the random variable is time-to-repair, in the same way, as time-to-failure is the random variable in reliability (Mobley et al. 2008). As an example, consider the maintainability equation for a system in which repair times are distributed exponentially. Its maintainability is given by:

$$M_i(t) = 1 - e^{-\mu_i t}, \tag{4}$$

where μ_i is repair rate.

Mean Time to Repair, MTTR, can be obtained by integrating maintainability function from zero to infinity:

$$MTTR = \int_0^\infty M_i(t)dt = \int_0^\infty e^{-\mu_i t}dt = \frac{1}{\mu_i}. \tag{5}$$

If one considers both reliability (probability an item will not fail) and maintainability (probability an item is successfully restored after failure), then an additional

metric is needed for probability a component/system is operational at a given time, (i.e., has not failed or it has been restored after failure). This metric is availability. Availability is then a performance criterion for repairable systems that accounts for both reliability and maintainability properties of a component or system. Availability, *A(t),* is defined as probability a system is operating properly when it is requested for use. In other words, availability is the probability a system will not fail or undergoing a repair action when it needs to be used. In case of a single component, *i*, $A_i(t)$ is given by:

$$A_i(t) = \frac{System\ up\ time}{System\ up\ time + System\ downtime} = \frac{MTTF}{MTTF + MTTR} = \frac{\mu_i}{\lambda_i + \mu_i}. \quad (6)$$

2.4 Human Factors and Ergonomics

Human Factors It is a discipline concerned with the development and application of human system interface technology to systems analysis design and evaluation. This technology includes human machine, human task, human environment, and organization machine interfaces. Efforts of human factors engineering are directed to improving operability, maintainability, usability, comfort, safety and health characteristics of systems in order to improve human and system effectiveness and to reduce the potential of injury and error (Stanton et al. 2005).

Ergonomics It is a term often used interchangeably with human factors that commonly refers to designing work environments for maximizing safety and efficiency. Ergonomics nowadays has great importance because companies have learned that designing a safe work environment can also result in greater efficiency and productivity. Today, around the world, there are many laws requiring safe work environment. Design of workplace results in a great impact on both safety and efficiency. The easier is to do a job, the more likely is to gain productivity due to greater efficiency. Analogously, the safer is to do it; also, the more likely it is to see gains in productivity due to reduced time off for injury. Ergonomics can address both these issues concurrently by maximizing workspace, equipment and activities needed to do a job (Stanton et al. 2005).

Human Reliability Assessment (HRA) HRA is a method that involves systematic prediction of potential human errors when interacting with a system. Once such errors are identified, this method tries to eliminate or reduce their occurrence, in order to maximize safety and performance of a system or facility. Results of HRA can be entered into risk management actions to reduce risk to ALARP, both by system re-design and implementation of controls and mitigations (USNRC 2005).

HRA, in general, encompasses the identification of error types, likelihood of error occurrence, opportunities to recover from errors and consequence of errors. This method should analyze current design and recommend how to mitigate errors

identified. Many reliability and risk analysis tools as FTA and ETA can help HEP steps. There are also many HRA specific techniques like THERP (Technique for Human Error Rate Prediction), SHERPA (Systematic Human Error Reduction and Prediction Approach), HEART (Human Error Assessment and Reduction Technique), CREAM (Cognitive Reliability and Error Analysis Method) and ATHEANA (A Technique for Human Event Analysis) (Calixto 2013). THERP will be briefly discussed in Sect. 4.4.

3 Integrated Framework for Assessing Safety, Reliability, Risk and Human Factors

Management systems in complex facilities like Nuclear Power Plants encompass several areas such as Quality (ISO 9001 standards), Environment (ISO 14001 standards), and Safety, Health and Risk Assessment (BS 8800 and OHSAS 18001 standards). Such management systems are often treated as independent functions within organizations. However, corresponding elements between these management systems are compatible and it is feasible integrating them. An integrated management and a systemic approach, i.e. an approach relating to the system as a whole in which the interactions among technical, human and organizational factors are fully considered, are essential to the specification and application of adequate safety measures and the fostering of a safety culture (IAEA 2016b).

3.1 Systems Theory

To understand complex systems, scientists usually try to envisage phenomena of nature and processes as simplified versions of reality known as a system. As defined, system can be envisaged as a collection of interrelated parts that work together by way of some driving process. They can be visualized as component blocks that have connections between them. Systems can be modeled using tools like block diagrams, facilitating evaluations of safety and reliability, for instance (ReliaSoft 2015).

Most systems share the same common characteristics. These common characteristics include the following (Cox and Tait 1998):

- Systems have a structure defined by its parts and processes.
- Systems are generalizations of reality.
- Systems tend to function in a same way. This involves inputs and outputs of material (energy or matter) that is then processed, causing it to change in some way.
- Various parts of a system have functional as well as structural relationships between each other.

- The fact of having functional relationships between parts suggests flow and transfer of some type of energy or matter.
- Systems often exchange energy or matter beyond their defined boundary with outside environment, and other systems, through various input and output processes.
- Functional relationships can only occur because of the presence of a driving force.
- The parts that make up a system show some degree of integration; in other words, the parts work well together.

Within the boundary of a system, three kinds of properties can be found:

- *Elements*—kinds of parts (things or substances) that make up a system. These parts may be hardware, software, raw materials, and persons, for instance.
- *Attributes*—characteristics of elements that may be perceived and measured. Examples: production, reliability, safety, and availability.
- *Relationships*—associations that occur between elements and attributes. These associations are based on cause and effect. In an organizational system, for example, there is a close relationship between human factors and production, safety and availability.

The state of a system is defined by the value of its properties (elements, attributes, and/or relationships).

3.2 Overview of Human Factors Integration

Figure 3 can be used to support the definition the objective of integrated analysis. It shows an overview of possibilities of integration of human factors (ergonomics), life-cycle step of the project (design, implantation, operation or decommissioning), target (quality, occupational health and safety, or environmental management), and focus of analysis (safety, reliability, or risk).

3.3 Integrated Framework

Figure 4 shows the steps for the proposed methodology considering safety, reliability, risk management and human factors integrations.

Identification of a system to be analyzed is carried out with the aid of systems theory. Figure 5 illustrates a systematic model of an organization adapted to an industrial facility (Cox and Tait, 1998). The first box represents inputs into the systems and includes physical, human and financial resources, as well as service and knowledge. The transformation process integrates plant (hardware), human resources (liveware) and policies, procedures, rules, and processes (software). The

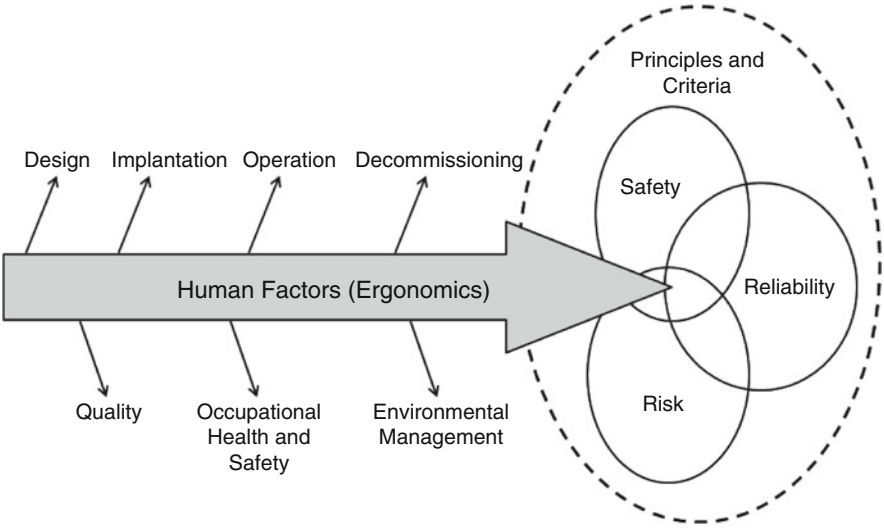


Fig. 3 Overview of framework for human factors integration (Vasconcelos et al. 2009)

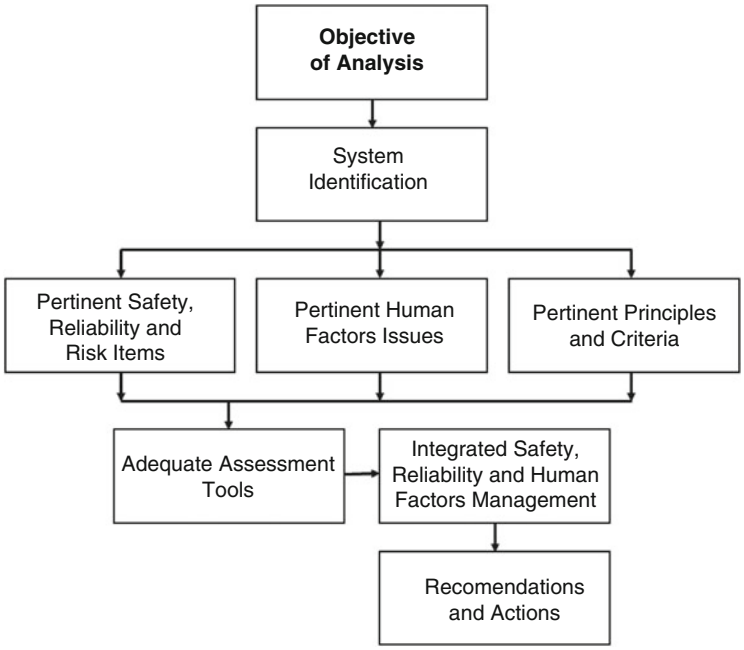


Fig. 4 Proposed methodology for safety, reliability, risk management and human factors integration (Vasconcelos et al. 2009)

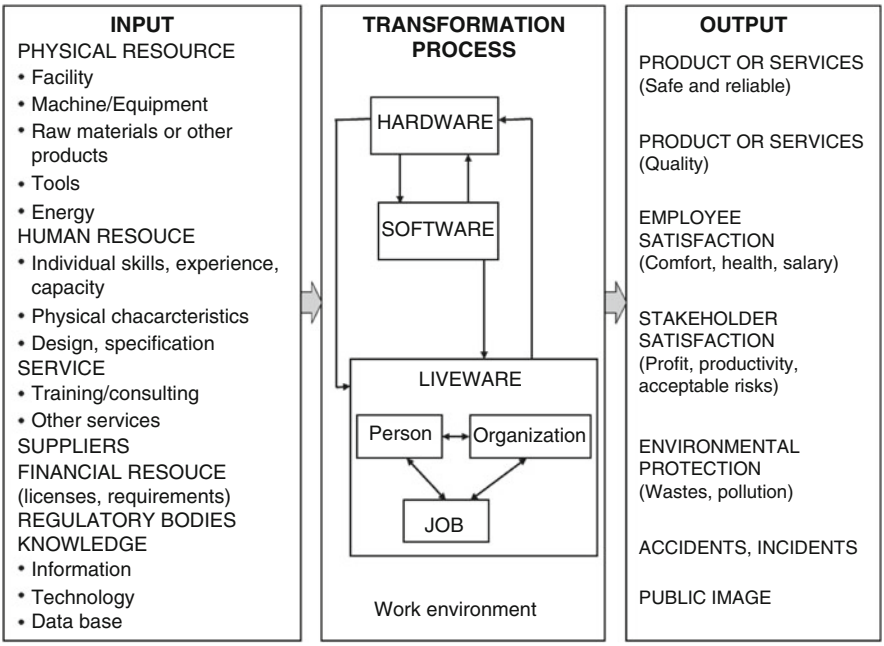


Fig. 5 Systemic model of an organization (adapted from Cox and Tait 1998)

box at right represents outputs and depending on targets of analysis, elements of quality, occupational health and safety, or environmental management can be selected.

The overview of framework for human factors integration, illustrated in Fig. 3 through the intersection of human factors (ergonomics) arrow with characteristics in focus (safety, reliability, or risk) or their intersections is best illustrated in Fig. 6. This figure illustrates some identified pertinent safety and reliability items, as well as common pertinent human factors issues. By this way, systems to be analyzed are identified systematically under all focus combination, within the life-cycle step and the required target (EUROCONTROL 2004). At each selected focus, applicable principles and criteria are chosen (examples in Table 1). Human factors to be considered in analysis are grouped in six areas in order to warrant that all issues will be considered and can be adequately prioritized. Six human factors areas and some example issues within each one are shown in Table 2. The integrated analysis can be carried out using common tools referred in Sect. 4 of this chapter.

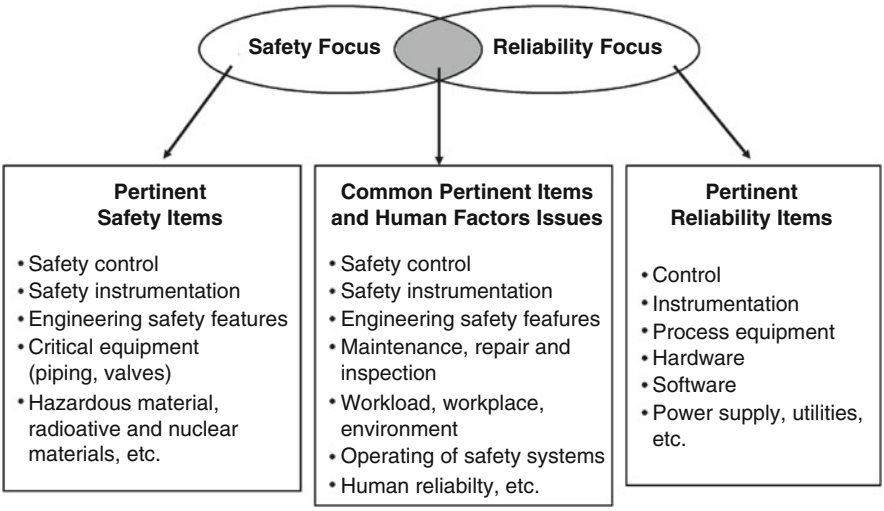


Fig. 6 Examples of pertinent items and Human Factors within an integrated safety and reliability focus (adapted from EUROCONTROL 2004)

4 Applied Models and Methods

Event Tree Analysis (ETA), Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD), and Technique for Human Error Rate Prediction (THERP) are examples of common safety, reliability, and risk evaluation tools that can support the team in proposed integrated framework for analyzing process systems and identifying potential accidents.

4.1 Event Tree Analysis (ETA)

Modeling of accident scenarios within a risk assessment process proceeds with inductive logic and probabilistic tools called Event Trees (ETs). An event tree starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events (Defence-in-depth levels), until an end-state is reached. (Stamatelatos 2002). Figure 7 illustrates an event tree for a generic initiating event and two levels of Defence-in-depth. Considering λ_{ie} as the frequency of occurrence of an initiating event, and p_1 and p_2, as the probabilities of failure of Defence-in-depth levels 1 and 2, respectively, the frequency of occurrence, *F*, for four possible accident scenarios (no-consequence, and accident scenarios 1, 2 and 3) can be calculated as shown in Fig. 7. Notice that these estimates are only valid if the events involved in each sequence are independent.

Table 1 Examples of design and analysis principles and criteria applied to safety, reliability, risk and human factors (adapted from Vasconcelos et al. 2009)

Selected focus	Principles and criteria
Safety	Fail-safe design
	Double contingency
	Single failure design
	ALARP
	Defence-in-depth
	Principles of waste management
	Licensing requirements
	Radioprotection
Reliability	Standby and redundancy
	Diversity
	k-out-of-n redundancy
	Fault tolerant systems
	Safety factors
	Availability
	Maintainability
	Sensitivity
Risk	Prevention principle
	Precautionary principle
	Protection principle
	Basic principles of nuclear energy
	Principle of limitation of risks to individuals
	Design basis accidents
	Environmental risks
	IAEA safety principles
Human factors (Ergonomics principles)	Work in neutral postures
	Reduce excessive force
	Keep everything in easy reach
	Maintain a comfortable environment
	Reduce excessive motions
	Accessibility
	Usability and affordance

4.2 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is an analytical technique, whereby an undesired state of a system is specified, usually a state that is critical from a safety or reliability standpoint. The system is then analyzed in the context of its environment and operation, to find all realistic ways in which the undesired event (called top event) can occur. Fault tree itself is a graphic model of various parallel and sequential combinations of faults that will result in the occurrence of the top event. Faults can be events that are associated with component hardware failures,

Table 2 Six human factors areas and examples of human factors issues (adapted from EUROCONTROL 2004)

Human factors area	Example issues
Human-Machine Interaction (HMI)	Input devices, visual displays, information requirements, alarm handling, HMI usability, user requirements, health risks, fatigue, distraction and concentration, noise, lighting, temperature/humidity/air quality, workplace arrangement
Organization and staffing	Staff requirements, manpower availability, human resource profile/selection criteria, job attractiveness, ageing, shift organization
Training and development	Training needs, performance/competence standards, training content, training methods and media, trainer role/responsibilities/competency, On-the-Job Training (OJT), emergency/unusual situation training, testing of training effectiveness
Procedures, Roles and responsibilities	Allocation of functions, involvement, workload, trust/confidence, skill degradation, procedure format and structure, procedure content, procedure realism, documentation
Teams and communication	Team structures/dynamics/relations, team coordination, leadership, workload communication, phraseology, national language differences, changes in communication methods, information content, types of communication
Recovery from failure	Human error potential, error prevention/ detection/recovery, detection of and recovery from system failures, error taxonomies

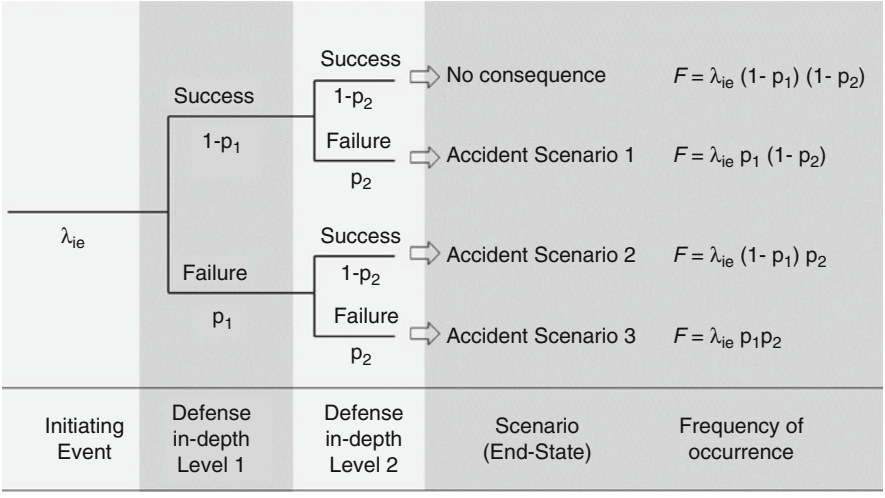


Fig. 7 Event Tree for a generic initiating event and two levels of Defence-in-depth

human errors, software errors, or any other pertinent events, which can lead to the top event. A fault tree thus depicts the logical interrelationships of basic events that lead to the top event of the fault tree (Stamatelatos 2002).

Both qualitative and quantitative evaluations can be performed with the help of fault tree technique. Fault tree itself is a qualitative assessment of events and shows

relationships that lead to the top event. In constructing fault tree, significant insights and understanding are gained concerning causes of the top event. Additional evaluations serve to further refine of the information that fault tree provides.

Qualitative evaluations basically transform a fault tree into logically equivalent forms that provide more focused information. The principal qualitative results obtained are the Minimal Cut Sets (MCSs) of the top event. A cut set is a combination of basic events that can cause the top event. An MCS is the smallest combination of basic events that result in the top event. MCSs relate the top event directly to the basic event causes. A set of MCSs for the top event constitutes all ways that basic events can cause the top event. Because the excessively large number of possible combinations of basic events in MCS, computer programs are necessary to identify MCS. For instance, in a system with 100 basic events there are 100 possible cut sets of one basic event, 161,700 cut sets with two basic events, 3,921,225 cut sets with three basic events, and so on. It is virtually impossible a manual review of these possible combinations and check if they are MCSs. Specialized computer programs are then necessary in order to obtain MCS for more complex fault trees (ReliaSoft 2015).

Quantitative evaluations of a fault tree consist of determining the top event probabilities and relative importance of basic events. Uncertainties in any quantified result can also be determined. Fault trees are quantified, typically, by calculating the probability of each MCS and by summing these probabilities, if the events in MCS are independent. Different types of probabilities can be calculated for different applications. In addition to a constant probability value that is typically calculated, time-related probabilities can be calculated providing the probability distribution of the time of first occurrence of the top event. Occurrence rates and availabilities of top events can also be calculated. These characteristics are particularly applicable if the top event is a system failure. Two examples of fault trees representing series and parallel systems respectively are shown in Fig. 8.

Top event probability is calculated from a fault tree using the probabilities that are input for the basic events. Depending on the specific top event definition, the top event probability can be the probability of the top event occurring during a mission time or in a given period of time, i.e., the probability that the top event exists at a given point in time. In some cases, the top event probability can be also the frequency of the top event occurring or the expected number of occurrences of the top event in some time interval. This only occurs if the inputs are basic event frequencies or expected numbers of occurrences.

Using the set theory concepts (Stamatelatos 2002) the probability equations of the two fault trees in Fig. 8 can be expressed as:

$$\mathrm{P(A\ or\ B)} = \mathrm{P(A \cup B)} = \mathrm{P(A)} + \mathrm{P(B)} - \mathrm{P(A \cap B)}, \tag{7}$$

$$\mathrm{P(A\ and\ B)} = \mathrm{P(A \cap B)} = \mathrm{P(A|B)\ P(B)} = \mathrm{P(B|A)\ P(A)}, \tag{8}$$

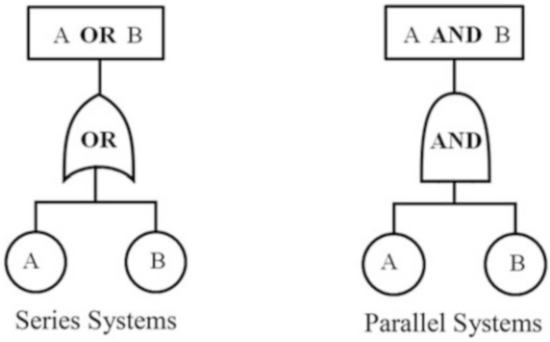


Fig. 8 Fault trees representing series and parallel systems

where P(A) and P(B) are the independent probabilities of basic events, and P(A|B) and P(B|A) are the conditional probabilities. If events A and B are independents, Eqs. 7 and 8 become:

$$\mathrm{P(A\ or\ B)} = \mathrm{P(A \cup B)} = \mathrm{P(A)} + \mathrm{P(B)} - \mathrm{P(A)\ P(B)}, \tag{9}$$

$$\mathrm{P(A\ and\ B)} = \mathrm{P(A \cap B)} = \mathrm{P(A)\ P(B)}. \tag{10}$$

4.3 Reliability Block Diagrams (RBD)

An overall system reliability prediction can be made by looking at the reliabilities of the components that make up the whole system or product. A Reliability Block Diagram (RBD) is a graphical representation of the components of a system and how they are related or connected (ReliaSoft 2015). RBDs for series and parallel systems are shown in Fig. 9.

In a series configuration, failure of any component results in failure of the entire system. In most cases, when considering complete systems at their basic subsystem level, it is found that these are arranged reliability-wise in a series configuration. A failure of any of these subsystems will cause a system failure. In other words, all of components in a series system must succeed for the system to succeed.

The reliability of a series system, R_s, is the probability that all n components in the system succeed. Therefore, the reliability of the system is then given by:

$$\begin{aligned} R_s &= P(X_1 \cap X_2 \cap \ldots \cap X_n) \\ &= P(X_1)P(X_2|X_1)P(X_3|X_1X_2)\ldots P(X_n|X_1X_2\ldots X_{n-1}) \end{aligned} \tag{11}$$

where X_i is the event of component i being operational,
$P(X_i)$ is probability that component i is operational, and
$P(X_i\ |X_1X_2\ X_3\ \ldots\ X_{i-1})$ is conditional probability.

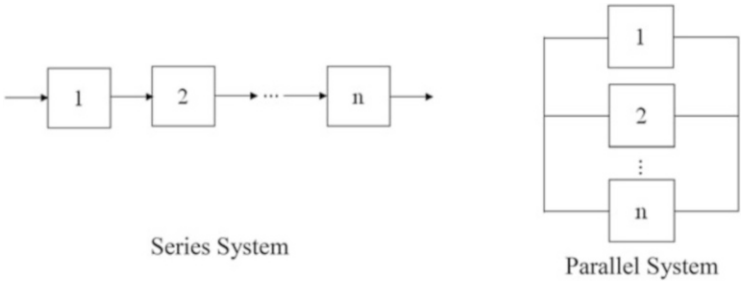


Fig. 9 Reliability block diagrams representing series and parallel systems

In the case where failure of a component affects failure rates of other components, the conditional probabilities in equation above must then be considered.

However, in the case of independent components, the equation above becomes:

$$R_s = P(X_1)P(X_2)P(X_3)\ldots P(X_n) = R_1R_2R_3\ldots R_n, \tag{12}$$

where R_i is the reliability of component i.

In a parallel configuration, at least one of the components must succeed for the system to succeed. For this reason, components in parallel are also referred to as redundant components. Redundancy is a very important method of improving system design and reliability.

Probability of failure, or unreliability, Q_p, for a system with n parallel components is the probability that all components in the system fail. Therefore, the unreliability of a parallel system is then given by:

$$\begin{aligned} Q_p &= P(x_1 \cap x_2 \cap \ldots \cap x_n) \\ &= P(x_1)P(x_2|x_1)P(x_3|x_1x_2)\ldots P(x_n|x_1x_2\ldots x_{n-1}), \end{aligned} \tag{13}$$

where x_i is the event of failure of component i,

$P(x_i)$ is the failure probability of component i, and

$P(x_i|x_1x_2\ldots x_{i-1})$ is conditional probability.

In the case where the failure of a component affects failure rates of other components, the conditional probabilities in equation above must be then considered.

However, in the case of independent components, equation above becomes:

$$Q_p = P(x_1)P(x_2)P(x_3)\ldots P(x_n) = Q_1Q_2Q_3\ldots Q_n\,. \tag{14}$$

So, the reliability of a parallel system, R_p, is then given by:

$$R_p = 1 - Q_p = 1 - (1 - R_1)(1 - R_2)(1 - R_3)\ldots(1 - R_n). \tag{15}$$

4.4 Technique for Human Error Rate Prediction (THERP)

Technique for Human Error Rate Prediction (THERP) is the most structured, detailed, and widely used Human Reliability Analysis (HRA) method in PRAs for NPPs. Swain and Guttmann (1983) define THERP as a method to predict Human Error Probabilities (HEP) and to evaluate the degradation of a man-machine system. This degradation can be caused by human errors alone or in connection with equipment malfunctions, operational procedures and practices, or other system and human characteristics that influence system behavior.

THERP analysis encompasses the following steps (Calixto 2013):

- Understanding the problem to be assessed to see if THERP is the best tool for finding the answer.
- Understanding of human error context and how human tasks influence activity or system being assessed.
- Listing and analyzing the related human tasks.
- Estimating error probabilities for each task using database, expert opinion or literature data.
- Estimating the final HEP for the whole activity using a THERP tree event.
- Proposing recommendations to reduce HEP.
- Estimating the effects of recommendations on HEP after they are implemented.

THERP depends heavily on a detailed and properly performed task analysis. Upon completion of the task analysis, Human Interaction (HI) is logically represented by an HRA event tree, which is used to combine HEPs associated with various HI tasks/subtasks, including cognitive response and action response. Figure 10 shows an example of an HRA event tree for an HI with two tasks A and B (Swain and Guttmann 1983).

As can be seen in Fig. 10, the probability of success P(S) or failure P(F) of a task is the sum of the probabilities for respective sequences. So, for the series system:

$$\mathrm{P(S)} = \mathrm{a(b|a)}, \tag{16}$$

$$\begin{aligned}\mathrm{P(F)} &= 1 - \mathrm{a(b|a)} \\ &= \mathrm{a(B|a)} + A\mathrm{(b|A)} + \mathrm{A(B|A)}.\end{aligned} \tag{17}$$

For the parallel system:

$$\begin{aligned}P\mathrm{(S)} &= 1 - \mathrm{A(B|A)} \\ &= \mathrm{a(b|a)} + \mathrm{a(B|a)} + \mathrm{A(b|A)},\end{aligned} \tag{18}$$

$$P\mathrm{(F)} = \mathrm{A(B|A)} \tag{19}$$

Many dependency models were developed to account for potential dependencies among multiple tasks or human interactions (Zhou et al. 2017; Su et al. 2015). In the model proposed by Swain and Guttmann (1983), the dependency level between two HI/tasks is broken into five levels, as shown in Table 3: Zero Dependence (ZD),

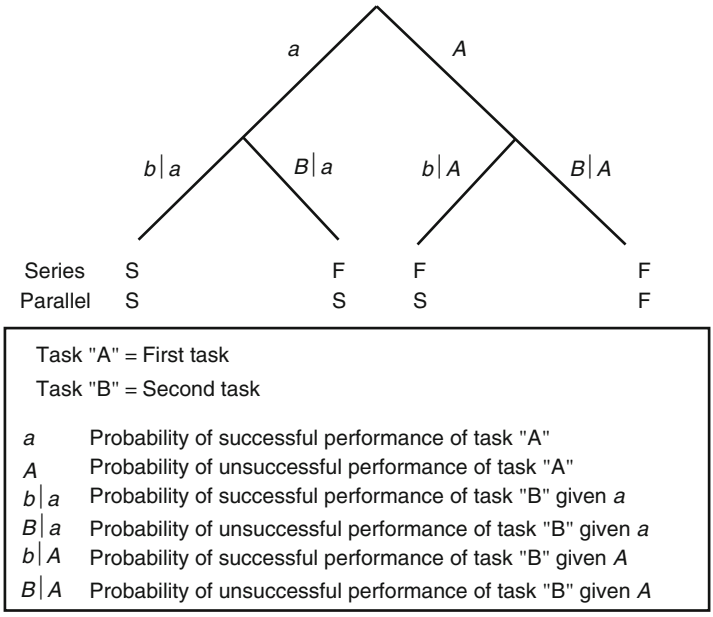


Fig. 10 HRA event tree example for series or parallel system (adapted from Swain and Guttmann 1983)

Table 3 Dependence model for Human Error Probability System (Swain and Guttmann 1983)

Dependency level	Dependent probability
ZD—Zero Dependence	HEP_n
LD—Low Dependence	$\frac{1+19HEP_n}{20}$
MD—Moderate Dependence	$\frac{1+6HEP_n}{7}$
HD—High Dependence	$\frac{1+HEP_n}{2}$
CD—Complete Dependence	1

Low Dependence (LD), Moderate Dependence (MD), High Dependence (HD), and Complete Dependence (CD). In Table 3 HEP_n is the HEP for Task n given Zero Dependence to Task $n-1$.

Many authors consider the assessment of dependence level in THERP highly subjective and dependent of a considerable amount of expert judgment. The criticisms also include the absence of specific guidance that makes the use of THERP dependence method difficult and the results may lack traceability and repeatability (Su et al. 2015). Despite such methodology does not consider human performance-shaping factors that cause human error, which is a characteristic of first generation of HRA methodologies, the longevity of THERP is a testament of its significance. THERP started the field of HRA, and newer methods can be seen as extensions of this pioneering work (Boring 2012).

5 Application Example

In this section, a simple representative example is presented in order to illustrate the benefits of integrated engineering approach to safety, reliability, risk management and human factors for a generic Loss of Coolant Accident (LOCA) in a Nuclear Power Plant (NPP).

5.1 Objective of Analysis

The objective of analysis is to improve Non-destructive Inspection (NDI) process of pipe segments of a core cooling system of a NPP, reducing LOCA probability, increasing system reliability and managing risks through acting on human factors issues. The life-cycle focus of analysis is the operation phase of the NPP.

5.2 System Identification

Figure 11 shows a simplified block diagram of a generic core cooling system (primary system) of a NPP and pertinent safety and reliability items that act as DID levels in case of a LOCA.

In this example, LOCA consequences are prevented or mitigated through actuating of safety systems, flaw detection, leak detection, or maintenance and repair. Piping flaws can be identified using NDI techniques, like ultrasonic inspection. Maintenance and repair actions can prevent leak and avoid accidents. If the NDI method fails, a leak will occur and could be detected by leak detection systems. The leak detection system can have the functions of initiating safety, maintenance and repair actions, mitigating the consequences.

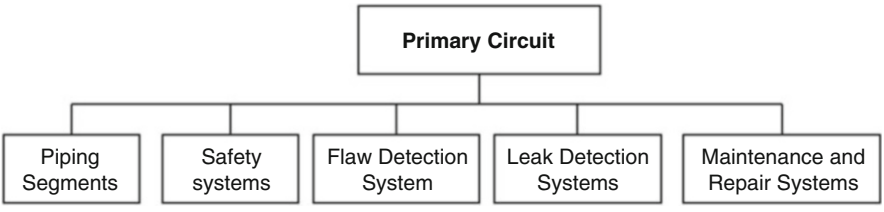


Fig. 11 Simplified block diagram of a primary circuit of a NPP

5.3 Pertinent Safety, Reliability and Risk Items

The identified pertinent safety items are piping segments, safety instrumentation, flaw detection systems, leak monitoring systems, and engineering safety features (safety systems). Reliability items include piping segments, control instrumentation and engineering safety features. Common pertinent safety and reliability items include piping segments, safety instrumentation, and engineering safety features. Risk management of a generic LOCA in the primary circuit is the pertinent risk item.

5.4 Pertinent Human Factors Issues

Table 4 shows examples of human factors issues related to a generic LOCA analysis, taking into account the six human factors areas defined in Table 2.

5.5 Pertinent Principles and Criteria Issues

According the pertinent principles listed in Table 1, the following issues were identified to the selected application example.

The pertinent safety principle and criteria of the operation phase of NPP is Defence-in-depth (DID) against LOCA. DID level 1 includes the use of operational

Table 4 Examples of human factors issues related to generic LOCA

Human factors area	Example issues
Human-Machine Interaction (HMI)	Automatic/manual In-service Inspection (ISI) systems, leakage alarm handling, ISI system usability, user requirements, health risks, workplace accessibility, redundant detection systems
Organization and staffing	Staff requirements for ISI, operator capability and limitation, job attractiveness
Training and development	Training needs, On-the-Job Training (OJT), testing of training effectiveness, ISI training, maintenance and repair training
Procedures, roles and responsibilities	ISI planning, ISI procedure, complementary ISI procedures due to task complexity, maintenance and repair procedure, leak detection procedure
Teams and communication	Team coordination, feedback in sustaining effective inspection performance, communication of existing plant data, communications of ISI and leak detection groups to maintenance and repair, report inspection data, methods and results, manual/automatic recording
Recovery from failures	Human error potential due to task complexity of ISI, supervisory tasks, detection and recovery from inspector errors

experience, planning of safety improvements, maintenance and training. DID level 2 includes ISI and leakage detection. Automatic and manual actuation of safety systems are part of DID level 3. The pertinent reliability principle and criteria are maintainability of piping segments and redundancy of leakage detection and safety systems. LOCA is the Design Basis Accident (DBA) criteria considered in risk management and some human factors should be considered in order to reduce risks. Workspace accessibility, usability of ISI, leakage, maintenance and repair systems, as well as cognitive ergonomics features of related operating plans and procedures are some pertinent criteria for human factors that can be cited.

5.6 *Adequate Assessment Tools*

In order to analyze safety, reliability, risk management and human factors for a generic LOCA in a NPP, using the proposed integrated engineering approach, a set of tools should be selected.

Sequences of plant end-states after an initiating event involving flaw occurrence in a pipe segment of primary circuit and the actuation of DID levels can be analyzed using Event Tree Analysis (ETA) technique.

Occurrence of piping rupture (that can cause LOCA or core damage) can be analyzed qualitative or quantitatively using Fault Tree Analysis (FTA) technique, which can involve hardware failures and human errors.

Evaluation of human errors occurring through the completion of selected complex tasks as NDI and typical action sequence for inspection can be carried out using THERP. Human performance issues can then be analyzed and improvements of NDI process of pipe segments of NPP can be suggested. In this example, only a qualitative use of these tools is done.

5.7 *Integrated Assessment*

Considering as pertinent safety items the pipe segments, NDI, leakage detection and safety systems, an event tree considering as initiating event "Flaw occurrence in a pipe segment" is shown in Fig. 12. This example is based in a previous work of Holmberg and Nirmark (2008) related to risk-informed assessment of Defence-in-depth of a generic LOCA.

The following event sequences were considered. The occurrence of the initiating event can be avoided by DID level 1, as use of operational experience, planning of safety improvements, maintenance and training. If the initiating event occurs, the flaw can be identified by In-service-Inspection (ISI), using NDI methods (DID level 2). If the NDI method fails, a leak will occur. This leak, assumed to be a small LOCA, can propagate to a large LOCA if the leakage detection system fails. Both

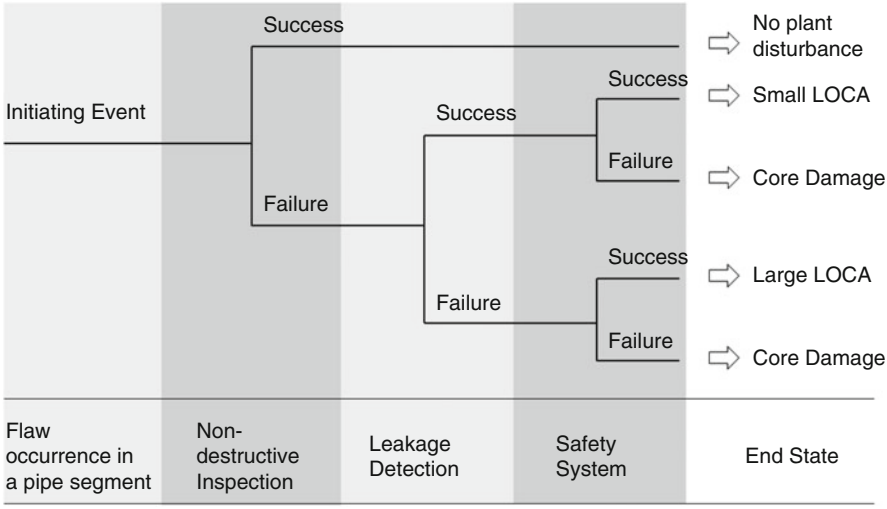


Fig. 12 Example of a simple event tree for LOCA (adapted from Holmberg and Nirmark 2008)

the small and large LOCA can lead to Core Damage, if safety systems fail. The leak detection system and the safety systems are DID level 3 methods in this example.

A fault tree was constructed in order to evaluate qualitatively the likelihood of occurrence of piping rupture taking into account the reliability of ISI and leak detection systems. Considering "Piping failure" as top event and ranking piping states into four types, "successive state", "detectable flaw state", "detectable leakage state" and "failure state", a fault tree model can be constructed as shown in Fig. 13. The descriptions of the primary events of the fault tree are listed in Table 5. The parameters expressing primary events rates in fault tree depends on both historical generic component data and plant specific data. Among the necessary data for estimating primary event parameters, can be highlighted: effectiveness rate to inspect flaw, piping flaw probability, piping rupture probability, effectiveness rate of leakage detection, and leakage occurrence rate. A qualitative evaluation of such fault tree can be performed through identification of Minimal Cut Sets (MCS), i.e., the minimal combination of events that can cause the top event occurrence.

In order to estimate the effectiveness rate to inspect flaw, a THERP event tree evaluating the likelihood of human errors occurring throughout the completion the task of piping inspection is constructed and shown in Fig. 14.

The tasks considered in this THERP are: define inspection strategy, select inspection technique, prepare equipment and procedures, acquire data, analyze data, record data, and report inspections (Parris 1988). The Human Error Probability (HEP) of NDI task depends on HEP for each action of the sequence, and they are described as follows.

Define Inspection Strategy To be effective, an inspection must be based on existing information about location, geometric profile, frequency of inspection,

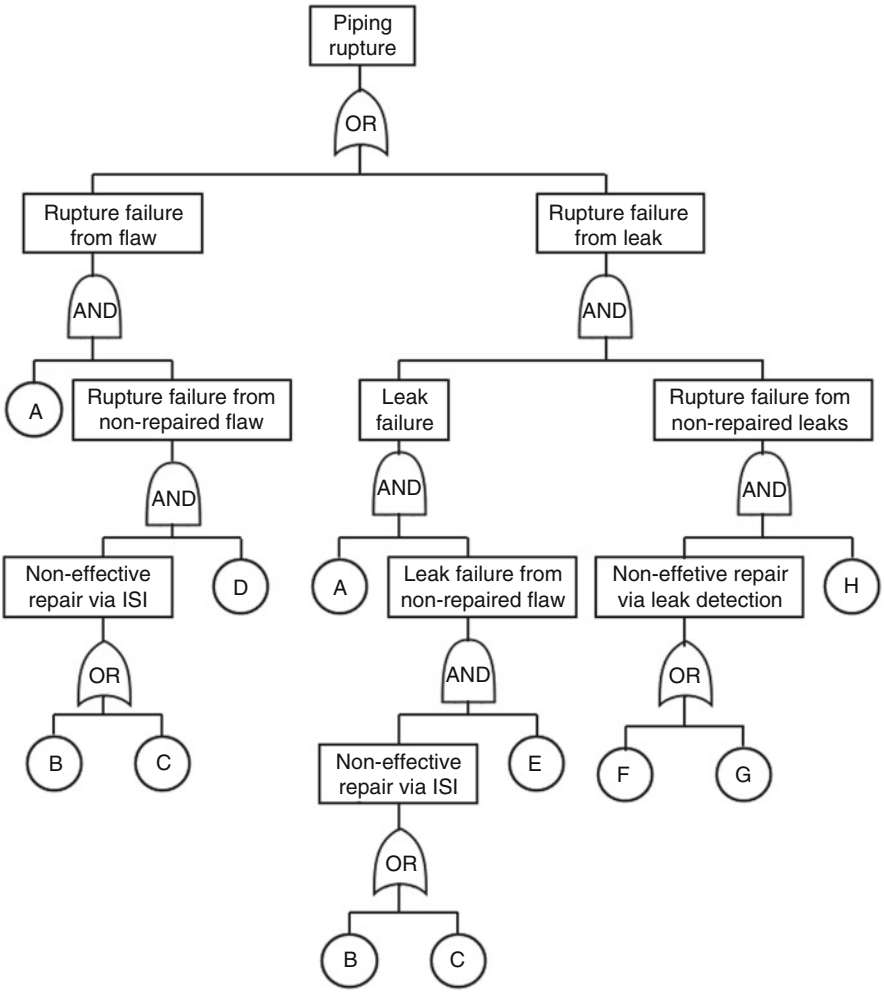


Fig. 13 Fault tree model for piping failure (adapted from Vasconcelos et al. 2016)

Table 5 Description of the primary events of fault tree of Fig. 13

Symbol	Description
A	Flaw occurrence
B	Non-effective repair
C	Non-effective ISI
D	Rupture failure given flaw
E	Leak failure given flaw
F	Non-effective repair
G	Non-effective leak detection
H	Rupture failure given leak

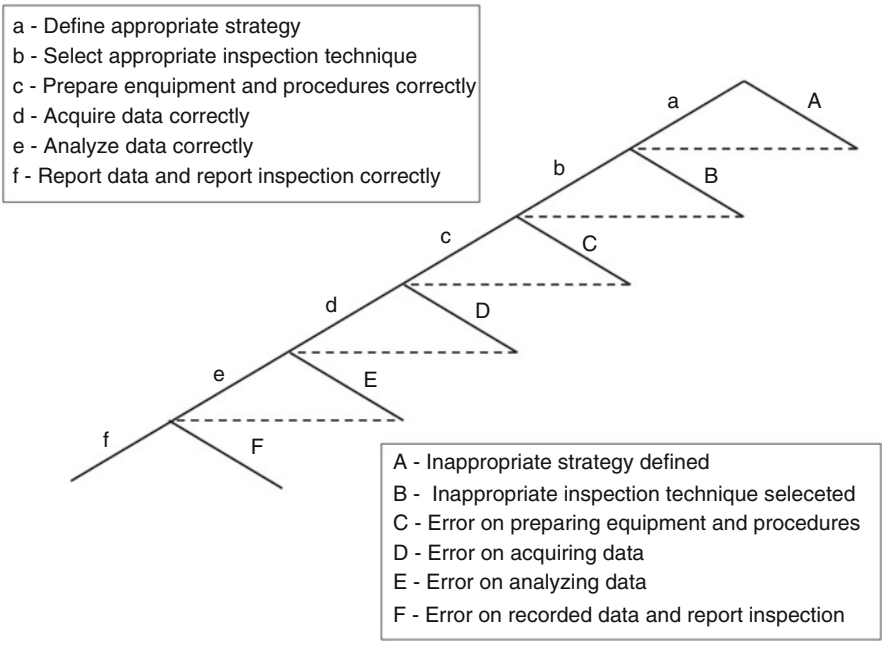


Fig. 14 THERP for evaluating the probability of human errors occurring throughout the completion the task of piping inspection

history, risks, etc., in order to define inspection strategy. Critical human function must be performed more automatically and remotely, reducing radiation exposure and improving results of inspections.

Select Inspection Technique The selection of most effective inspection technique for flaw detection involves considerations of geometry and materials properties, and detailed procedures to be carefully followed.

Prepare Equipment and Procedures The preparing involves calibration, equipment set and tests, establishing team coordination, and following written and trained procedures.

Acquire Data Acquiring data needs explicitly written and trained procedures, i.e., specific steps must be prescribed and followed invariably. Sometimes this is not possible due to task complexity and the number of variables and conditions that must be addressed in ISI.

Analyze Data Interpreting flaw data and discriminating them from another signal depends on many equipment sets, inspector skill and training, and accurate procedures.

Record Data and Report Inspections In manual data recording and inspection reporting, data such as, relevant parameters and defect indications and locations,

are collected and analyzed at the same time, increasing error possibilities. Automatic data recording and analyses do not need proceed simultaneous with data collection, reducing HEP.

5.8 *Improvements on Safety, Reliability and Risk Management*

A quantitative assessment of safety, reliability and risk including human factors for complex tasks as NDI in this application example is not easy to do, because it depends on specific data and HEP for each step of THERP, which are usually unavailable. However, the qualitative integrated assessment illustrated in this application example can be helpful for understanding the human error context and identify many improvements that can be made in human factors issues and, accordingly, in safety, reliability and risk management.

Among the improvements of generic NDI process of pipe segments of a core cooling system of a Nuclear Power Plant (NPP) can be highlighted:

- **Definition of an optimal strategy of inspection**. There are different possible inspection strategies involving locations, techniques, frequencies, etc. A Risk-Based Inspection approach, for instance, prioritizing locations and higher risks systems should be considered (Soares et al. 2015).
- **Development of guidelines for operator-control interface design**. Use of human-factors principles and criteria in design of new inspection systems. This guidelines can be used to design more effective systems, and reduce the time and expense required for inspection tasks (Stanton et al. 2005).
- **Reduction of complexity of manual NDI**. Manual NDI are typically too complex to produce reliable results, because many variable must be addressed in order to preparate and conduct inspections. In NPP, the task is usually performed in radioactive areas, with time pressure and protective clothes that difficult the tasks. Manual NDI should only be peformed where accessibility limitations preclude automatic ones (Parris 1988).
- **Application of human factors principles and criteria to the preparation of written instructions**. NDI procedures usually offer many opportunities for human performance errors. Many inspections are in general, similar, but different in significant details. The principal means of countering error potentials is to provide understandable, action-oriented instructions combined with labels on controls and indicators, for instance, taking into account ergonomic principles as usability and accessibility. As an example, instructions that emphasizes graphics and decision tables rather than narrative presentation of information are less error-prone (Stanton et al. 2005).
- **Collection and analysis of NDI performance data**. Many studies have shown that inspection accuracies are typically lower than expected. It is necessary to know what might be done to redesign the tasks or instrumentation to yield better

results. Collected performance data should be interpreted and transformed into specific recommendations to task, instrumentaion, and training improvements (Parris 1988).

- **Development of method for feedback information of effectiveness of NDI**. Task performance tends to deteriorate if feedback is lacking or not adequate. Complete, accurate, and timely information on task performance is one of the best ways to improve and sustain human performance of complex task as NDI and to better the risk management (IAEA 2001).

6 Conclusions

This chapter proposes and applies a systematic methodology for integrated analysis of safety, reliability, risk and human factors. Interactions among technical, human and organizational factors can be fully considered by using systems theory.

The systematic approach directs the analysis, starting from the selection of applicable life-cycle step and the required target (quality, occupational health and safety, or environmental management). The analyses of the attributes in focus (safety, reliability, or risk) or their intersections are carried out through the integration of human factors that are selected, prioritized and analyzed, considering applicable principles and criteria, and using common applicable safety, reliability, and risk tools. Merging of these various assessment and management systems could reduce duplication of efforts and costs, and increase the effectiveness of management systems, among others.

Main terminology and concepts related to safety assessment, risk management, reliability engineering, human factors and ergonomics were presented. Concepts of systems theory, supporting the integrated framework for assessing safety, reliability, risk and human factors, were also introduced. Mathematical and statistical basis for assessment of reliability, unreliability, maintainability and availability were described. The systematization of the application of the methodology was driven by the use of figures and tables, helping the definition of objectives of analysis, detailing their steps, as well as defining the pertinent items, principles and criteria applied to safety, reliability and human factors.

Common tools used in integrated analysis, as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), Event Tree Analysis (ETA), and Technique for Human Error Rate Prediction (THERP), including mathematical and statistical basis, were briefly described. So, an event tree for a generic initiating event and two levels of Defence-in-depth was presented, showing the frequency of occurrence estimation for possible accident scenarios, as function of frequency of occurrence of initiating event and probabilities of failure of Defence-in-depth levels. Concepts of Fault Trees and Reliability Block Diagrams were presented, including theoretical basis for qualitatively and quantitatively assessment of likelihood of failures and reliability for series and parallel systems. THERP was also presented through a Human Reliability Analysis event tree for series and parallel systems, illustrating

how to estimate the probability of successful and unsuccessful performance of tasks.

Finally, a simple representative example was presented, in order to illustrate the benefits of the integrated engineering approach to safety, reliability, risk management and human factors for a generic LOCA in a Nuclear Power Plant (NPP). The qualitative assessment demonstrated the benefits of using the proposed integrated approach. The application example illustrated an integrated assessment of safety, reliability and risks, including human factors for a complex task of Non-destructive Inspection (NDI) of piping segments of primary circuit of a NPP. A quantitative assessment of complex tasks as NDI involved in the application example is difficult to do, because it depends on specific data and human error probabilities for each step of developed THERP, which are usually unavailable. However, this qualitative integrated assessment was helpful for understanding the human error context and identify many improvements that can be made in human factors issues and, consequently, in safety, reliability and risk management. Some generic improvements for NDI process of piping segments of primary circuit were then presented for the purpose of reducing LOCA probabilities.

Acknowledgments The authors would like to thank the following Brazilian institutions that supported the writing of this chapter: Nuclear Technology Development Center (CDTN), Brazilian Nuclear Energy Commission (CNEN), Financier of Studies and Projects (FINEP), Brazilian Council for Scientific and Technological Development (CNPq), and Minas Gerais State Foundation for Research Development (FAPEMIG).

References

ANS. American Nuclear Society (2016) Glossary of definitions and terminology. American Nuclear Society, La Grange Park, IL, 186 p

Boring RL (2012) Fifty years of THERP and human reliability analysis. Proceedings of the 11th probabilistic safety assessment and management conference. International—PSAM11, Idaho Falls, ID, June

Calixto E (2013) Gas and oil reliability engineering. Modeling and analysis. Elsevier, Amsterdam, 545 p

Christensen FM, Andersen O, Duijm NJ, Harremoës P (2003) Risk terminology—a platform for common understanding and better communication. J Hazard Mater 103:181–203

Cox S, Tait R (1998) Safety, reliability and risk management: an integrated approach, 2nd edn. Butterworth-Heinemann, Oxford, 325 p

EUROCONTROL. European Organization for the Safety of Air Navigation (2004) The human factors case: guidance for human factors integration—HRS/HIS-003-GUI-01. Brétigny, 114 p

Holmberg JE, Nirmark J (2008) Risk-informed assessment of Defence-in-depth, LOCA example phase 1: mapping of conditions and definition of quantitative measures for the Defence-in-depth levels. Rev 0. VTT Technical Research Centre, Espoo, Finland, 42 p (SKI Report 2008:33)

HSE. Health and Safety Executive (2017) Principles and guidelines to assist HSE in its Judgements that duty-holders have reduced risk as low as reasonably practicable. Retrieved 7 Apr 2017, from http://www.hse.gov.uk/risk/theory/alarp1.htm

IAEA. International Atomic Energy Agency (2001) Risk management: a tool for improving nuclear power plant performance. Vienna, 88 p (IAEA-TECDOC-1209)
IAEA. International Atomic Energy Agency (2009) Deterministic safety analysis of nuclear power plants. Specific Safety Guide N° SSG-2. Vienna, 84 p
IAEA. International Atomic Energy Agency (2012). IAEA report on protection against extreme earthquakes and tsunamis in the light of accident of the Fukushima Daiichi Nuclear Power Plant. International Expert Meeting. Vienna
IAEA. International Atomic Energy Agency (2016a) Safety glossary terminology used in nuclear safety and radiation protection. Vienna, 219 p
IAEA. International Atomic Energy Agency (2016b) Leadership and management for safety. General Safety Requirements No. GSR Part 2. Vienna (STI/PUB/175)
Lees FP (2012) Loss prevention in the process industries: hazard identification, assessment and control, 4th edn, 3 vol. Butterworth-Heinemann, Oxford
Mobley RK, Higgins LR, Wikoff DJ (2008) Maintenance engineering handbook, 7th edn. McGraw Hill, New York, NY, 1244 p
NAS & USNRC. National Academy of Sciences and U.S. Nuclear Regulatory Commission (2014) Lessons learned from the Fukushima nuclear accident for improving safety of U.S nuclear plants. National Academies Press, Washington, DC, 394 p
Parris DH (1988) Human performance in non-destructive inspections and functional tests. EPRI NP-6052. Final Report. Palo Alto, CA, October
ReliaSoft (2015) System analysis reference: reliability, availability and optimization. ReliaSoft Publishing, Tucson, AZ
Soares WA, Vasconcelos V, Rabello EG (2015) Risk-based inspection in the context of nuclear power plants. Proceedings of the International Nuclear Atlantic Conference—INAC 2011, São Paulo, October 4–9
Stamatelatos M (2002) Probabilistic risk assessment procedures guide for NASA managers and practitioners—version 1.1. Office of Safety and Mission Assurance, NASA Headquarters, Washington DC, 323 p
Stanton N, Hedge A, Brookhuis K, Salas E, Hendrick H (2005) Handbook of human factors and ergonomics methods. CRC Press, Boca Raton, FL, 685 p
Su X, Mahadevan S, Xu P, Deng Y (2015) Dependence assessment in human reliability analysis using evidence theory and AHP. Risk Anal 35(7). doi:10.1111/risa.12347
Swain AD, Guttmann HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278. U.S. Nuclear Regulatory Commission
USNRC. U.S. Nuclear Regulatory Commission (1975) WASH-1400—Reactor Safety Study, NUREG-75/014, Washington, DC
USNRC. U.S. Nuclear Regulatory Commission (2001) Integrated safety analysis—guidance document. NUREG-1513. Office of Nuclear Material Safety and Safeguards, Washington, DC, 65 p
USNRC. U.S. Nuclear Regulatory Commission (2005) Good Practices for implementing Human Reliability Analysis (HRA). NUREG-1792. Washington, DC, 103 p
USNRC. U.S. Nuclear Regulatory Commission (2011) An approach for using probabilistic risk assessment in risk-informed decisions on plant specific changes to the licensing basis. Regulatory Guide 1.174—Revision 2. Washington, DC, 37 p
USNRC. U.S. Nuclear Regulatory Commission (2013) Glossary of risk-related terms in support of risk-informed decision-making. NUREG 2122. Washington, DC, 187 p
USNRC. U.S. Nuclear Regulatory Commission (2017) Full-text glossary. Retrieved 31 Mar 2017 from https://www.nrc.gov/reading-rm/basic-ref/glossary/full-text.html
Vasconcelos V, Silva EMP, Reis SC, Costa ACL (2009). Safety, reliability, risk management and human factors: an integrated engineering approach applied to nuclear facilities. Proceedings of the International Nuclear Atlantic Conference—INAC 2009, Rio de Janeiro, , September 27–October 5

Vasconcelos V, Soares WA, Costa ACL, Rabello EG, Marques RO (2016) Evaluation of piping reliability and failure data for use in risk-based inspections of nuclear power plants. Proceedings of "Congresso Brasileiro de Engenharia e Ciência dos Materiais", 12th CBECIMAT, Natal, November 6–10

WHO. World Health Organization (2004) IPCS risk assessment terminology. International Programme on Chemical Safety (ICPS). World Health Organization, Geneva, 122 p

Zhou X, Deng X, Deng Y, Mahadevan S (2017) Dependence assessment in human reliability analysis based on D numbers and AHP. Nucl Eng Des 313:243–252

Vanderley de Vasconcelos was born in Brazil, in 1956. He received the B.E. degree in Electrical Engineering from the Federal University of Uberlândia, Brazil, in 1978, his M.Sc. degree in Nuclear Science and Technology, in 1985, and his Ph.D. degree in Metallurgical and Mining Engineering from the Federal University of Minas Gerais, Belo Horizonte, Brazil, in 1997. He has experience in system analysis, reliability, probabilistic risk assessment, accident analysis, environmental management, and licensing of radioactive and nuclear facilities. He was head of the Department of Environment, Waste and Radiation Protection, coordinating a variety of environmental and nuclear licensing processes. Since 2006, he has been Professor of Production Engineering Department at Itaúna University Foundation, Itaúna, Brazil, and his research interests cover industrial risk management, ergonomics, and occupational safety engineering. He is currently senior researcher in the Nuclear Technology Development Center, a research institute from the Brazilian Nuclear Energy Commission.

Wellington Antonio Soares was born in Brazil on April 16, 1950. He received the B.E. degree in Civil Engineering from the University of Brasília, Brasília, Brazil, in 1975, his M.Sc. degrees in Nuclear Science and in Engineering of Structures in 1983 and 1991, respectively, from the Federal University of Minas Gerais, Belo Horizonte, Brazil, and the Ph.D. degree in Nuclear Technology from the University of São Paulo, São Paulo, Brazil, in 1999. He has experience in areas such as nuclear power plants licensing, stress analysis and mechanical vibrations, fracture mechanics, design of explosion-resistant structures, photoelasticity and risk-based inspection in nuclear facilities. He has also experience in management and in social communication. He coordinated the 10th Meeting on Nuclear Applications held in Belo Horizonte, Brazil, in 2011. He is currently senior researcher in the Nuclear Technology Development Center, a research institute from the Brazilian Nuclear Energy Commission.

Raíssa Oliveira Marques was born in Brazil, in 1992. She received the B.E. degree in Control and Automation Engineering from the Federal University of Minas Gerais, Belo Horizonte, Brazil, in 2015. She had developed works on prospecting technological innovation demands, in order to identify strategic opportunities in Research & Development for the automotive industry, and implemented methodologies and software to assist management of risks and waste in nuclear and radioactive facilities. Her main areas of research interest are risk management, probabilistic safety analysis, reliability and human factors. She is currently a master student in Science and Technology of Radiations, Minerals and Materials from the Nuclear Technology Development Center, a research institute of Brazilian Nuclear Energy Commission. Her master's dissertation in progress involves Risk-Based Inspection methods applied to nuclear research reactors.

A Fuzzy Modeling Application for Human Reliability Analysis in the Process Industry

Zoe Nivolianitou and Myrto Konstantinidou

Abstract Having presented the general Human Reliability Analysis (HRA) principles and the special branch of Fuzzy/CREAM methodologies for Human error probability estimation, the chapter continues with some more details on CREAM which is the base for the fuzzy model developed. Some basic principles of fuzzy logic will then be covered before proceeding to the detailed description of the model itself. Special applications of the model i.e. the definition of critical transitions, the assessment of operators' response times during a critical task performed in the chemical process industry along with a shorter tailored made version of the model will be presented in the remainder of this chapter.

Keywords HRA • CREAM • Fuzzy theory • Industry • Critical task

1 Introduction

Human Reliability Analysis (HRA) is a significant part of every risk assessment study. The main issue of HRA is the subjectivity of the methods used to evaluate human reliability and the uncertainty of the data concerning human factors, together with the complexity of the human behaviour per se. Many methods have been developed to assist the analysis of human errors and human reliability (indicatively Swain and Guttmann 1983; Embrey 1992; Hollnagel 1998; Cooper et al. 2000). Starting with THERP (first generation method) passing through CREAM (second generation method), and arriving to ATHEANA (third generation), all methods have tried in different ways to approach the most difficult and subjective part of PRAs—the modeling and assessment of human performance. Most of them include expert judgment, statistical data analysis and simulation proofs.

The Technique for Human Error Rate Prediction (THERP) is the most widely used technique to date. It is a basically hybrid approach as it models human errors

Z. Nivolianitou (✉) • M. Konstantinidou
National Center for Scientific Research Demokritos, Athens, Greece
e-mail: zoe@ipta.demokritos.gr; myrto@ipta.demokritos.gr

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_5

using both probability trees and models of dependence on the one hand, considering also Performance Shaping Factors (PSFs) affecting the operator actions on the other. The technique is linked to the database of Human Error Probabilities (HEPs) included in THERP handbook, which contains data derived from a mixture of objective field data and judgements by the developers of the technique. This database, coupled with an engineering approach and with the fact that THERP was the first methodology to be accepted and used in the field, accounts for its popularity (Swain and Guttmann 1983).

The use of first generation methods caused limitations in the analysis of Human Factors because they are lacking a well-defined classification system, an explicit model and an accurate representation of dynamic system interactions. Most of them characterize each operator action with a success or failure path. Additionally the representation of PSFs influence on human performance was quite poor. These deficiencies led to the development of the second generation of human reliability methods. The main progress in each generation of methods is the model on which the former are built and their ability to provide quantitative results as well. However, the problems of subjectivity and lack of data still exist.

Among the second generation methods for the estimation of Human Reliability, the most well-known is CREAM, established by Hollnagel in 1998 and having been applied extensively to human error quantification of safety-critical systems. CREAM can be used both in retrospective and prospective analyses for industrial accidents and events' diagnosis and prediction. The prospective analysis comprises two steps for human error quantification (a) the basic method and (b) the extended method. The basic method is used for determination of control modes and corresponding error rate intervals in a screening stage and the extended method for error quantification of cognitive functions. However, according to the developers themselves the inherent deterministic approach in traditional CREAM still lacked capability of dealing with the uncertainties of common performance condition (CPC) configuration and different weight assignments to the CPCs. This fact led the developers to undertake research efforts for the improvement of CREAM and HEP estimation by means of probabilistic techniques; namely Fujita and Hollnagel (2004) designed a new version of basic method of CREAM, while Kim et al. (2006) described a probabilistic approach for determining the control modes. A parallel school of thought used the fuzzy theory to best describe the quantification of HEP as will be seen below in this chapter.

CREAM has been very popular among Human reliability researchers in the years after its presentation. Lee et al. (2011) designed a CREAM-based analysis method for Nuclear reactor operators (CEAM) communication error analysis; He et al. (2008) simplified the CREAM for HEP point estimation, while Sun et al. (2012) did the same applying a modified basic method of CREAM on the start-up of a diesel engine in a submarine. Modifications in CREAM proposed also Liao et al. (2016) with the human error causal model of the original CREAM combined with Bayesian parameter estimation to analyse the interactions among the influential variables considering several possible paths. Along the same line, Wu et al. (2017) proposed a modified CREAM as well for estimating the human error probability in

the maritime accident process on the basis of an evidential reasoning approach using a scenario- and barrier-based framework to describe the maritime accident. Meanwhile, Bedford et al. in 2013 made an extensive sensitivity analysis of the CREAM methodology by considering three different aspects: (a) the difference between the outputs of the Basic and Extended methods, on the same HRA scenario; (b) the variability in outputs through the choices made for common performance conditions (CPCs); and (c) the variability in outputs through the assignment of choices for cognitive function failures (CFFs), comparing CREAM's quantitative structure to that of first HRA generation methods.

CREAM has similarities to the third generation technique[1], namely "A Technique for Human Error Analysis" (ATHEANA) that is based on a multidisciplinary framework that considers both the human-centered factors (e.g. PSFs such as human-machine interface design, content and format of procedures, and training) and the conditions of the plant that give rise to the need for actions and create the operational causes for human-system interactions (e.g. misleading indications, equipment unavailability, and other unusual configurations or operational circumstances). However, the human-centered factors and the influence of plant conditions are not independent of each other; in fact, the combined effect of PSFs and plant conditions create a situation in which human error is likely to occur and is an error-forcing context (EFC). According to ATHEANA developers (Cooper et al. 2000) in order to provide error probabilities which are consistent with operational experience, the task of HRA quantification must be based upon the likelihood of such error forcing contexts, rather than upon a prediction of random human error in the face of nominal conditions.

1.1 Coupling Fuzzy Theory with Human Reliability Analysis

In order to improve CREAM capability to deal with the uncertainties of common performance condition (CPC) configuration and of different weight assignments to the CPCs, the use of Fuzzy logic theory (fuzzy sets and fuzzy rules) was proposed simultaneously by Konstandinidou et al. and Marseguerra et al., both in 2006, with applications in the Chemical and Nuclear sectors respectively. Five years later in 2011, more groups of scientists present works of HEP estimation using Fuzzy sets theory; namely, Li et al. (2010) claimed that fuzzy logic can deal with uncertainty and imprecision, when dealing with the operators' response to an emergency accident in a nuclear power plant and the errors that might take place because of the effects of context on human activities; Ung and Shen (2011) proposed a fuzzy logic model in situations where the lack of data exists using a real-world example;

[1]Some analysts do not consider ATHEANA a third generation technique but rather a well advanced second generation one.

and, along the same lines, Wang et al[2]. (2011) presented fuzzy-clonal selection methods for contextual and reliability evaluation in the domain of safety assessment of power systems. A year later Verma et al. (2012) presented a Fuzzy fault tree approach for analysing the fuzzy reliability of a gas power plant, while Kazaras et al.(2013) use the same HEP Fuzzy/CREAM model for assessing the tunnel operator's performance in safety critical situations. The same year, Yang et al. (2013) present a modified Fuzzy/CREAM to human reliability quantification in marine engineering. Monferini et al. (2013) presented an application of the HEP Fuzzy/CREAM model for the assessment of impact of human and organizational factors in hazardous industrial plants through the use of a Virtual Environment. Continuing the string of applications, Saidi et al. (2014) apply fuzzy risk based maintenance (RBM) methods to address the complexity of operations in the oil and gas refineries. Geng et al. (2015) apply Fuzzy/CREAM for Human error probability estimation in an ATEX-HMI area classification of a food industry, while Mandal et al. (2015) use the fuzzy VIKOR method to develop a human-error identification and risk prioritization method in overhead crane operations. In 2016 appear the works of two groups of analysts: Rachid et al. (2016) make the reliability evaluation of a centrifugal pump based on a fuzzy expert model; on the other hand, Baziuk et al. (2016) make a reassessment of the applications and contributions of fuzzy set theory to human reliability analysis (HRA). The authors claim that the main contribution of fuzzy mathematics relies on its ability to represent vague information; several HRA authors have made contributions developing new models, introducing fuzzy quantification methodologies, while others have drawn on fuzzy techniques or methodologies for quantifying already existing models. The same authors also claim that Fuzzy contributions improve HRA in five main aspects: (1) uncertainty treatment, (2) expert judgment data treatment, (3) fuzzy fault trees, (4) performance shaping factors, and (5) human behavior models.

2 The CREAM Basics (Hollnagel 1998)

In order to be able to describe and analyze human interaction with technology it is necessary to model or describe the functions of the human mind. Most analysts agree that erroneous actions are negative events where there is some kind of failure to meet a pre-defined performance standard. The term human erroneous action or even human error does not imply that the action is also a cause.

HRA has traditionally been closely coupled to PSA (Probabilistic Safety Assessment) and there has been a strong emphasis on quantification. The practical need for HRA has grown as part of the requirement to calculate more precisely the probability of an accident in order to guide resource investment, but there is a more

[2]However, the same researchers claim that the fuzzy model of CREAM brings on many redundant, self-contradictory rules, which would consume computational time, and lose the truth degree of the results.

fundamental need to improve the understanding of human action as part of system design and in particular to develop models and methods for the analysis of interaction between people and socio-technical systems.

An action always takes place in a context, and the context is partly the outcome of preceding human activities in, for instance, design, maintenance and management. It is therefore not enough for HRA to develop models of human action during control and operation. It is necessary to develop a comprehensive understanding of human action in context.

The study of human reliability can be seen as a specialized scientific sub-field, a kind of hybrid between psychology, ergonomics (human factors), engineering (hardware) reliability analysis and system analysis.

The tradition from first generation methods was to distinguish between a correctly performed action, the failure to perform an action known as omission and an unintended or unplanned action known as commission. Commissions have received less attention and have mostly been used as conceptual garbage for everything that could not be classified as an "error of omission". From the HRA point of view it was necessary to introduce a new category, which appropriately enough was called cognitive error. Incorrect diagnosis or decision failure therefore became synonymous with "cognitive error". The difference between the two terms is that a commission is a manifestation, while a cognitive error is a cause.

The shortcomings of 1st generation HRA approaches can be described in several ways:

- Less than adequate data
- Less than adequate agreement in use of expert judgment methods
- Less than adequate calibration of simulator data
- Less than adequate proof of accuracy in HRAs
- Less than adequate psychological realism in some HRA approaches
- Less than adequate treatment of some important PSFs

First generation methods are less concerned with what people are likely to do than with whether they will succeed or fail. In CREAM actions are not considered in isolation. In fact CREAM is an acronym for:

Cognitive; the focus on the full complexity of human mind.
Reliability; the probability that a person will perform according to the requirements of the task for a specified period of time.
Error; or rather Erroneous action—the action that actually went wrong.
Analysis; the separation or decomposition of a whole into smaller parts for study and better understanding. It could be replaced by assessment.
Method; a practically useful tool, which is simple and cost effective, yet produces the required results.

Classification schemes as error taxonomies are essential in order to distinguish between causes and manifestations regardless if it is for retrospective or predictive analysis.

Traditional Human factor approaches include Specific Psychological Causes and General Psychological Causes, while Information Processing approaches are vaster and include:

- Human information processing models
- Quantitative methods of erroneous actions
- Qualitative methods of erroneous actions
- Generic error modelling system
- Human error action taxonomy

A well-known approach is the Cognitive Systems Engineering perspective (CSE) which assumes that interactions between the human agent and the automated control system are best viewed in terms of a joint cognitive system, and advocated the position in which the behaviour of the human operator is seen as being shaped primarily by the socio-technical context in which behaviour occurs.

The CREAM methodology has been derived from the Contextual Control Model (COCOM), the purpose of which was to provide the conceptual and practical basis for developing models of operator performance. The objective of COCOM, which will be described in a subsequent paragraph, was not to explain the masked "mental mechanisms" of operator performance, but rather to account for how people are able to maintain control of a situation. COCOM therefore focuses on the principles that can be used to explain and predict the dynamic equilibrium between human actions and system response, which is an essential characteristic of efficient human performance. The basic premise is that human performance is determined largely by the situation. People can do many things and achieve their objectives in many different ways. The classification system proposed by CREAM makes use of the concepts developed in the COCOM model. Specifically, the predictive facet of CREAM makes use of the notion of the control modes to provide a fast, overall assessment of human reliability (Hollnagel and Cacciabue 1991).

2.1 Principles of CREAM

The development of a system to support the analysis of accidents and events must as minimum include a method and a classification scheme. The purpose of the method is to provide an account of how the analysis shall be performed, preferably by describing each step of the analysis as well as how they are organized. The purpose of the classification scheme is to provide a consistent basis for describing details of the events and for identifying the possible causes. A system to support prediction must include the same elements. In addition, it is also necessary that the classification scheme explicitly refers to a model of the phenomena being studied.

A **method** is defined as a regular or systematic way of accomplishing something. In event analysis the method describes how the analysis of actions should be performed in order to find the possible and probable causes, in particular how the concepts and categories used for explanation should be applied. In performance

prediction the method describes how the consequences of an initiating event may be derived and how the performance conditions may affect the propagation of consequences. In both cases the method should explicitly describe how each step is to be carried out, as well as define the principles to determine when the analysis or prediction has come to an end.

A **classification scheme**, as an ordered set of categories, is necessary both to define the data that should be recorded and to describe the details of an event. A consistent classification scheme is also necessary in order to analyze the event and identify the possible or probable causes. A consistent classification scheme is finally necessary to predict how an event may develop. The classification scheme describes the relations between causes and manifestations (effects) and thereby forms the basis for predicting the outcome of specific changes in the causes. In addition a classification scheme must, by definition, refer to an underlying model or description of the domain.

The model provides the principles according to which the classification scheme is organized.

Thus, the system has three essential elements and shall be referred as the MCM framework—M for Method, C for the Classification scheme, and M for the Model. The crucial element is the model of human cognition and the method, which describes the links between the model of cognition and the classification scheme.

An important conclusion about the first-generation HRA approaches is that all of the main approaches have been developed to answer practical needs—although with varying degrees of success. Few, if any HRA approaches have been developed from a theoretical or academic basis alone. The strong need to practical needs is the reason why few of the HRA approaches show any significant connection between the method and the classification scheme, and indeed, why few of them have a really well defined classification scheme. The main distinction made by first generation HRA approaches seems to be between correct and faulty actions- or between success and failure.

Two basic requirements to a second generation HRA approach are therefore that it uses enhanced PSA event trees and that it extends the traditional description of error modes beyond the binary categorization of success-failure and omission-commission. A further requirement is that a second generation HRA approach must account explicitly for how the performance conditions affect performance which in turns leads to a requirement for a more realistic type of operational model.

CREAM has been developed from a principled analysis of existing approaches and therefore explicitly contains a method, a classification scheme and a model. Of these the classification scheme and the method are the most important and they are intrinsically linked. The underlying model serves mainly as a basis for relating some of the groups of the classification scheme. In other words CREAM has not been developed from the underlying model of cognition, but simply uses it as a convenient way to organize some of the categories that describe possible causes and effects of human actions. The primary purpose of CREAM is to offer a practical approach to both performance analysis and prediction.

The main principle of the method is that is fully bi-directional. This means that same principles can be applied for retrospective analysis—in the search for cause- and in performance prediction.

The basic principle in the modeling of cognition is the description of competence and control as separate aspects of performance. The competence describes what a person is capable of doing, while the control describes how the competence is realized. The level of control clearly depends on the situation itself, hence on the context. It stands to reason that if there is better control of the actions, then it is less likely that any given action will fail. Complete control however, does not exclude that an action can be incorrectly performed.

2.2 Models of Cognition

The model is necessary to define the relationship between components of the classification scheme, in particular the ways in which actions are typically produced, hence the ways in which erroneous actions may come about.

Earlier versions of CREAM made use of a simplified model of cognition called **Simple Model of Cognition (SMoC)**. The two fundamental features of the SMoC were (1) the distinction between observation and inference and (2) the cyclical nature of human cognition. The former emphasized the need to distinguish clearly between what can be observed and what can be inferred from the observations.

The model that is used as a basis for CREAM is a further development of the SMoC called the **Contextual Control Model (COCOM).** Cognition is not only an issue of processing input and producing a reaction, but also an issue of the continuous revision and review of goals and intentions, i.e. a loop on the level of interpretation and planning. Cognition should therefore not be described as a sequence of steps, but rather as a controlled use of the available competence (skills, procedures and knowledge) and resources.

Competence can be defined in terms of a relative small range of cognitive functions that appear to a greater or a lesser extent, in most contemporary attempts to model the essential characteristics of human cognition. In addition competence includes the person's skills and knowledge that may have been compiled into familiar procedures and response patterns.

Control can be described by referring to a continuum, going from a situation where a person has little or no control over events to conditions where events are under complete control, and by emphasizing characteristic modes of control along the continuum.

The basic difference between COCOM and SMoC is that the links between the cognitive functions have been relinquished which means that there are no pre-defined cause-effect relations.

2.3 The Four Control Modes

Control is necessary to organize the actions within the person time horizon. Effective control is practically synonymous with the ability to plan future actions. The level of control is influenced by the context as the person experiences it, by knowledge of dependencies between actions and by expectations about how the situation is going to develop, in particular about which resources are and will be available to the person. In COCOM a distinction is made among four characteristic control modes:

In **Scrambled control** the choice of next action is in practice unpredictable or haphazard. Scrambled control characterizes a situation where little or no thinking involved in choosing what to do. This is typically the case when the task demands are very high, when the situation is unfamiliar and changes in unexpected ways, when thinking is paralyzed and there accordingly is a complete loss of situation awareness. The extreme case of scrambled control is the state of momentary panic.

In **Opportunistic control** the next action is determined by the salient features of the current context rather than on more stable intentions or goals. The person does very little planning or anticipation, perhaps because the context is not clearly understood or because time is too constrained. In these situations the person will often be driven either by the perceptually dominant features of the interface or by those which due to experience or habit are the most frequently used, corresponding to the similarity matching and frequency gambling heuristics described by Reason (1990).

In **Tactical control** performance is based on planning, hence more or less follows a known procedure or rule. The planning is, however, of limited scope and the needs taken into account may sometimes be ad hoc. If the plan is a frequently used one, performance corresponding to tactical control may seem as if it was based on a procedure prototype—corresponding to e.g. rule-based behavior. Yet the regularity is due to similarity of the context or performance conditions, rather than to the inherent nature of performance.

In **Strategic control** the person considers the global context, thus using a wider time horizon and looking ahead at higher-level goals. The strategic mode provides a more efficient and robust performance, and may therefore seem the ideal to strive for. That attainment of strategic control is obviously influenced by the knowledge and skill of the person, i.e. the level of competence. In the strategic control mode the functional dependencies between task steps (pre-conditions) assume importance as they are taken into account in planning.

The different levels of control are represented in Fig. 1.

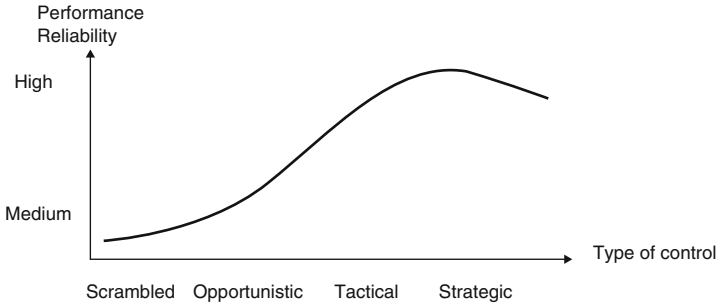


Fig. 1 The four control modes of CREAM

2.4 Basic Principles of the Classification Scheme

On the highest level the classification system makes a distinction between effects (**Phenotypes**) and causes (**Genotypes**). The effects refer to what is observable in the given system (indicated malfunction, releases of mass and energy, changes in speed and direction, overt human actions). In case of retrospective analysis the effects are the starting point for the analysis. On the case of performance prediction the effects are the outcome of the analyzed sequence and typically they represent something that should be avoided or prevented.

The causes are the categories that can be used to describe that which has brought or can bring the effects. They are distinguished between three major categories: (1) causes related to the person, (2) causes related to the technological system, and (3) causes related to the organization or environment.

The first category contains the genotypes that are associated with human psychological characteristics, for instance relating the cognition, to psychophysiological variables, to emotional state, to personality traits.

The second category consists of the genotypes that are associated with the technological system, in particular to the state of the system and to the state changes. This category includes everything that has to do with the state of components, failure of components and subsystems, state transitions and changes. This category also includes everything that has to do with the man-machine interaction and the man-machine interface (information presentation and control).

The third category contains the genotypes that characterize the organization, the work environment and the interaction between people. Examples could be permanent failure of the system, aspects of the organization, and environmental conditions such as noise, temperature.

2.5 Common Performance Conditions

Instead of PSFs CREAM is using the CPCs (**Common Performance Conditions**) to define sets of possible error modes and probable error causes. The CPCs provide a comprehensive and well-structured basis for characterizing the conditions under which the performance is expected to take place. These CPCs have been used for the development of the fuzzy sets of the model which will be described in the subsequent section; therefore are briefly presented hereunder.

Adequacy of organization: Defines the quality of the roles and responsibilities of team members, additional support, organization communication systems, Safety Management System, instructions and guidelines for externally oriented activities, role of external agencies.

Working Conditions: Describes the nature of the physical working conditions such as ambient lighting, glare on conditions screens, noise from alarms, interruptions from the task.

Adequacy of man-machine interface and operational support: Defines the Man-Machine Interface in general, including the information available on MMI and control panels, computerized workstations, and operational support provided by operational specifically designed decision aids.

Availability of procedures and plans: Describes procedures and plans and includes operating and emergency procedures, familiar patterns of response heuristics, routines.

Number of simultaneous goals: Enumerates the number of tasks a person is required to pursue or attend to at the same time (i.e., evaluating the effects of actions, sampling new information, assessing multiple goals).

Available time: Pictures the time available to carry out a task and corresponds to how well the task execution is synchronized to the process dynamics.

Time of day: Denotes the time of day (or night) and describes the time at which the task is carried out, in particular whether or not the person is adjusted to the current time (circadian rhythm). Typical examples are the effects of shift work. It is a well-established fact that the time of day has an effect on the quality of work, and that performance is less efficient if the normal circadian rhythm is disrupted.

Adequacy of training and experience: Describes the level and quality of training provided to operators as familiarization to new technology, refreshing old skills, etc. It also refers to the level of operational experience.

Crew collaboration quality: Declares the quality of the collaboration between crewmembers, including the overlap between the official and unofficial structure, the level of trust, and the general social climate among crewmembers.

There is obviously a significant overlap between the CPCs and the traditional PSFs. This is because the set of possible conditions that may affect performance is limited. The difference between the CPCs and the PSFs is therefore not so much in the names and meaning of the categories that are used, but in how they are used. The main difference is that the CPCs are applied at an early stage of the analysis to characterize the context for the task as a whole, rather than as a simplified way of

adjusting probability values for individual events. In this way the influence of CPCs becomes closely linked to the task analysis.

2.6 Performance Prediction

In HRA and in particularly within PSA, the main purpose is to predict which sequences of events are likely and what the outcomes will be, provided that nothing happens that is not part of the descriptions. This is another way of saying that in order for predictions to be correct, models and reality must correspond.

The general method for performance prediction includes:

1. Application analysis. It is first necessary to analyze the application and the situation. This may involve a task analysis, where the tasks can be derived from the PSA. The analysis must however, include considerations of the organization and the technical system, rather than being confined to the operator and the control tasks.
2. Context description. The context is described by using the CPCs. The principle for the context description is exactly the same as for the retrospective analysis; the difference being the level of detailed information may vary.
3. Specification of initiating events. The initiating events for the human actions/performance can be specified from several points of view. An obvious candidate is the PSA, since the PSA event trees will define the minimum set of initiating events that must be considered. Another is the outcome of the application and task analysis.
4. Qualitative performance prediction. The qualitative performance prediction uses the classification scheme, as modified by the context, to describe how an initiating event can be expected or developed
5. Selection of task steps for analysis. If a quantitative prediction is going to be made, it is necessary to select the cases that require further study. This can be done from the set of outcomes of the qualitative prediction, or from the PSA input.
6. Quantitative performance prediction. The last step is the quantitative performance prediction. To the extent that quantification is required the qualitative analysis may at least be useful in identifying possible dependencies between actions.

CREAM approaches the quantification in two steps, by providing a basic and an extended method. The basic method corresponds to an initial screening of the human interactions. The screening addresses either the task as a whole of major segments of the task. The extended method uses the outcome of the basic method to look at actions or parts of the task where there is a need for further precision and detail.

2.7 CREAM-Basic Method

The purpose of the basic method is to produce an overall assessment of the performance reliability that may be expected for a task. The assessment is expressed in terms of a general action failure probability, i.e. an estimation of probability of performing an action incorrectly for the task as a whole. The basic method consists of the following three steps:

1. Construct the event sequence. The first step in the application of the method requires the identification of the scenarios or events for which a reliability analysis is needed. Additionally one particular scenario must be selected at a time as the focus of the analysis. Following the identification of a scenario to be analyzed, the first step of the basic CREAM is a task analysis in which the objective is to produce a description of the task, with sufficient details to support the following steps.
2. Assess Common Performance Conditions. The CPCs provide a comprehensive and well-structure basis for characterizing the conditions under which the performance is expected to take place. Since the CPCs depend on each other, a combined CPC score cannot be produced simply as a sum of the individual CPCs, not even if they are weighted. Instead the derivation of the combined CPCs score must take into account the way in which CPCs are coupled or dependent. The combined CPC score can be derived simply by counting the number of times where a CPC is expected:

   - To reduce performance reliability
   - To have no significant effect
   - To improve performance reliability

   This can be expressed as the triplet $[\Sigma_{\text{reduced}}, \Sigma_{\text{not significant}}, \Sigma_{\text{improved}}]$
   Altogether this step can be sub-divided in four steps:

   2a. Determine the expected level of each CPC
   2b. Determine the expected effects on performance reliability
   2c. Determine dependencies and indirect influences
   2d. Make a total of combined score of the expected effects and express it in the form $[\Sigma_{\text{reduced}}, \Sigma_{\text{not significant}}, \Sigma_{\text{improved}}]$

3. Determine the probable control mode. The basis for determining the probable control mode is the assessment of the CPCs and the determination of the combined effect on human performance reliability. There are 52 different values of the combined CPC score. Of these 52 values the triplet [9,0,0] describes the least desirable situation, in the sense that all CPCs point to a reduced performance reliability, while triplet [0,2,7][3] describes the most desirable situation

[3]It has to be noted at this point that two out of the nine CPCs can have only a neutral or negative effect on human reliability. The effect of each CPC on human performance will be analytically explained in Sect. 4.2 where the development of the fuzzy model is being described.

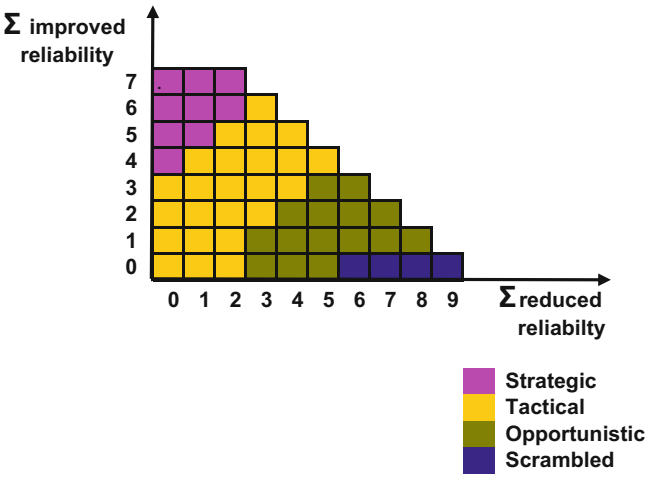


Fig. 2 Basic diagram of CREAM methodology for operator control mode

Table 1 Control modes and relevant reliability intervals in CREAM

Control mode	Reliability interval (Probability of an action failure)
Strategic	0.5 E-5 < P < 1.0 E-2
Tactical	1.0 E-3 < P < 1.0 E-1
Opportunistic	1.0 E-2 < P < 0.5 E-0
Scrambled	1.0 E-1 < P < 1.0 E-0

because it provides the maximum number of CPCs that improve performance reliability.

All the possible combinations of the CPC score form a matrix where the four control modes are defined and indicated. Based to the CPC score the relevant control mode is defined (Fig. 2).

The final step in the basic CREAM is to find a general action failure probability that corresponds to how the situation has been characterized by the CPCs. The probability intervals are defined in Table 1, and are commonly accepted estimations in the available HRA literature.

The basic method of quantification of CREAM has been used as a basis for the developed fuzzy model which will be described along with its applications in the following sections.

3 Fuzzy Logic as a Modelling Tool

Fuzzy logic theory has emerged over the last years as a useful tool for modelling processes which are too complex for conventional quantitative techniques or when the available information from the process is qualitative, inexact or uncertain.

Although it is almost five decades since Loft Zadeh (1965) introduced the fuzzy logic theory, only in the years after 2000 the latter became a popular technique for developing sophisticated models and systems. The reason for this rapid development of fuzzy systems is simple. Fuzzy logic addresses qualitative information perfectly as it resembles the way humans make inferences and take decisions. Fuzzy sets cognitive perspective plays a key role in the application of this methodology to problems of system modelling, control and pattern recognition, as the general intent is to emulate human-like ways of dealing with a variety of control and recognition problems. When a human being is solving a certain complex problem, he tries first to structure the knowledge about it in terms of some general concepts and afterwards to reveal essential relationships between them. This sort of top-down approach allows him to convert these quite general and imprecise relationships into more detailed operational algorithms. Fuzzy logic models fill an important gap in system design methods that is between purely mathematical approaches (e.g. system design), and purely logic-based approaches (e.g. expert systems). While other approaches require accurate equations to model real-world behaviors, fuzzy design can accommodate the ambiguities of real-world human language and logic with its inference techniques.

Fuzzy inference systems have been successfully applied in fields such as automatic control, data classification, decision analysis, expert systems, and computer vision. Because of its multidisciplinary nature, fuzzy inference systems are associated with a number of names, such as fuzzy-rule-based systems, fuzzy expert systems, fuzzy modelling, fuzzy associative memory, fuzzy logic controllers, and simply (and ambiguously) fuzzy systems. Mamdani's fuzzy inference method is the most commonly encountered fuzzy methodology. Mamdani's method was among the first fuzzy set theories used to build control systems. It was proposed in 1975 by Ebrahim Mamdani as an attempt to control a steam engine and boiler combination by synthesizing a set of linguistic control rules obtained from experienced human operators.

3.1 Short Overview of Fuzzy Modelling

Fuzzy logic starts with the concept of a fuzzy set. A fuzzy set is a set without a crisp, clearly defined boundary. The fundamental difference of fuzzy logic compared to conventional modelling techniques is on the definition of sets. Traditional set theory is based on bivalent logic where a number or object is either a member of a set or it is not. Contrary to that, fuzzy logic allows a number or object to be a member of more than one sets and most importantly it introduces the notion of partial membership (Klir and Yuan 1995). A degree of membership in a set is based on a scale

from 0 to 1 with 1 corresponding to complete membership and 0 meaning no membership.

More formally (Pedrycz 1993), a fuzzy set A defined in a universe of discourse X is expressed by its membership function

$$A : X \rightarrow [0, 1]$$

where the degree of membership A(x) expresses the extent to which x fulfills the category described by A. The condition $A(x) = 1$ denotes all the elements that are fully compatible with A. The condition $A(x) = 0$ identifies all elements that definitely do not belong to A. In fuzzy sets, the meaning of the fundamental predicate of set theory "$\in$" (element of) is significantly expanded by accepting a partial membership in a set. The basic operations can be defined as:

$$(A \cup B)\,(x) = \max\,(A(x), B(x))$$
$$(A \cap B) = \min\,(A(x), B(x))$$
$$\bar{A}(x) = 1 - A(x)$$

where $x \in X$

Zadeh's approach in 1965 offered a general method to express linguistic rules that are processed quickly by a computer (Mamdani 1974). Information flow through a fuzzy model requires that the input variables go through three major transformations before exiting the system as output information, which are known as fuzzification, fuzzy inference, and defuzzification. The three steps, representing the structure of a fuzzy logic system are explained briefly below.

- **Fuzzification**. It is the process of decomposing a system input variables into one or more fuzzy sets, thus producing a number of fuzzy perceptions of the input.
- **Fuzzy Inference**. After the inputs have been decomposed into fuzzy sets, a set of fuzzy if-then-else rules is used to process the inputs and produce a fuzzy output. Each rule consists of a condition and an action where the condition is interpreted from the input fuzzy set and the output is determined on the output fuzzy set. In other words fuzzy inference is a method that interprets the values in the input vector and, based on some set of rules, assigns values to the output vector.
- **Defuzzification**. It is the process of weighting and averaging the outputs from all the individual fuzzy rules into one single output decision or signal. The output signal eventually exiting the system is a precise, defuzzified, crisp value.

Fuzzy modeling methodologies are procedures for developing the knowledge base of the system, i.e. the set of fuzzy rules (Klir and Yuan 1995). The natural way to develop such a system is to use human experts who build the system based on their intuition, knowledge and experience. In this case the experts, usually based on a trial and error approach, define the fuzzy sets and the membership functions. The rule structure is then determined based on how the designers interpret the characteristics of the variables of the system.

The most popular fuzzy model suggested in the literature that is also used in this work, is the one proposed by Mamdani in 1974 and has the following formulation with respect to its fuzzy rules:

$$\forall r \in R: \ \textit{if} \ \underset{1 \le i \le n}{\wedge} \left(x_i \in A_i^r\right) \quad \textit{then} \ \underset{1 \le j \le m}{\wedge} \left(y_j \in B_j^r\right)$$

where: n is the number of input variables,
m is the number of output variables,
$x_i, 1 \le i \le n$ are the input variables,
$A_i^r, 1 \le i \le n$ are the fuzzy sets defined on the respective universes,
$y_j, 1 \le j \le m$ are the output variables
and $B_j^r, 1 \le j \le m$ are the fuzzy sets defined for the output variables.

4 Development of a Fuzzy Modelling Application Based on CREAM for Human Reliability Analysis (Konstandinidou et al. 2006)

In probabilistic risk assessments (PRA) human errors of misdiagnosis during unexpected accidents have been identified as major causes of catastrophic disasters (Kim and Bishu 1996). On the other hand, subjectivity, which is related to fuzziness, is inherent in system and human reliability analysis (HRA) as it has been mentioned previously. It is, therefore, necessary to construct a model into which subjectivity data can be incorporated (Onisawa 1996). Besides that, it is well-known that the human operator is considered as an unreliable element and much effort has been put into developing methods for operator modelling (Hollnagel 1996). Another relevant factor associated with the Human Element in the design and safety assessment processes is that it is impossible to conceive a plant that is totally "human-error free", as this is an intrinsic characteristic of any technological system (Cacciabue 2004).

At the same time Zadeh's statement of 1973 is always valid: "the closer one looks at a real world problem, the fuzzier becomes its solution. Stated informally, the essence of this principle is that, as the complexity of a system increases, our ability to make precise and yet significant statements about its behavior diminishes until a threshold beyond which precision and significance become almost mutually exclusive characteristics".

In order to provide a logical solution to the above statements, the fuzzy logic modeling architecture has been selected to build a model for the estimation of the probability of an erroneous human action, a model that was based on the common performance conditions defined in CREAM.

The Mamdani type of fuzzy modeling has been selected and the development of the system has been completed in three steps which will be described hereunder.

4.1 Step 1: Selection of Input Parameters

As the probability of a human erroneous action in the industrial environment is a function of many factors, the selection of the input parameters was made so that all the important influencing factors are considered, while maintaining the system at a reasonable size. Factors that characterize the ergonomy and the working conditions, as well as the operator availability of responding to his duties and the interaction with his colleagues were also included. Organizational factors that affect human performance were not omitted either.

Based on the above criteria, the list of selected input variables consisted of the Common Performance Conditions (CPCs) that are used in the CREAM methodology. These CPCs were described earlier and their associated fuzzy sets will be presented in the following section.

It should be mentioned that many other performance-shaping factors (or common performance conditions) could be used or added. The selection of a well-known system of factors that is tested and widely used was the most appropriate choice in order to test the model. In a more general context, each analyst could be free to use the performance shaping factors (or common performance conditions) of his/her choice, as long as he is able to build the knowledge base of the system on his/her parameters.

4.2 Step 2: Development of the Fuzzy Sets

As explained in Sect. 3, in order to better depict the impact of each input parameter, the risk analyst associates two or more fuzzy sets for the description of this parameter. In the present step, the number and characteristics of fuzzy sets defined for all the input variables, and for the unique output variable, namely, the action failure probability are explained and listed in Table 2. For each of the eight (from the total nine) input variables the interval that the corresponding fuzzy sets cover, lies from 0 (worst case—bad conditions) to 100 (best case—advantageous conditions). Only for the input variable "time of day" the interval of hours that the fuzzy sets cover is between 0:00 (midnight) and 24:00. The relevant fuzzy sets associated in each input variable are presented in Figs. 3, 4, 5, 6, 7, 8, 9, 10 and 11 while for the output variable is presented in Fig. 14. A more detailed description of the fuzzy set headings appointed to each input and the output variable is presented in the following paragraphs. The effects of each fuzzy set in human performance are presented in Table 3.

Adequacy of organization: Four fuzzy sets, namely "Deficient", "Inefficient", "Efficient" and "Very Efficient" were defined on the input space of this variable. The values vary from 0 to 100, depicting the local conditions. From the above four fuzzy sets, the "Deficient" and "Inefficient" ones have a negative effect on human performance while the fourth one "Very efficient" has a positive effect on human

Table 2 Number of fuzzy sets defined for each input and output parameters

	CPCs	Number of fuzzy sets
Input	Adequacy of organization	4
	Working conditions	3
	Availability of procedures and plans	3
	Adequacy of MMI and operational support	4
	Number of simultaneous goals	3
	Available time	3
	Time of day	3
	Adequacy of training and experience	3
	Crew collaboration quality	4
Output	Action failure probability	4

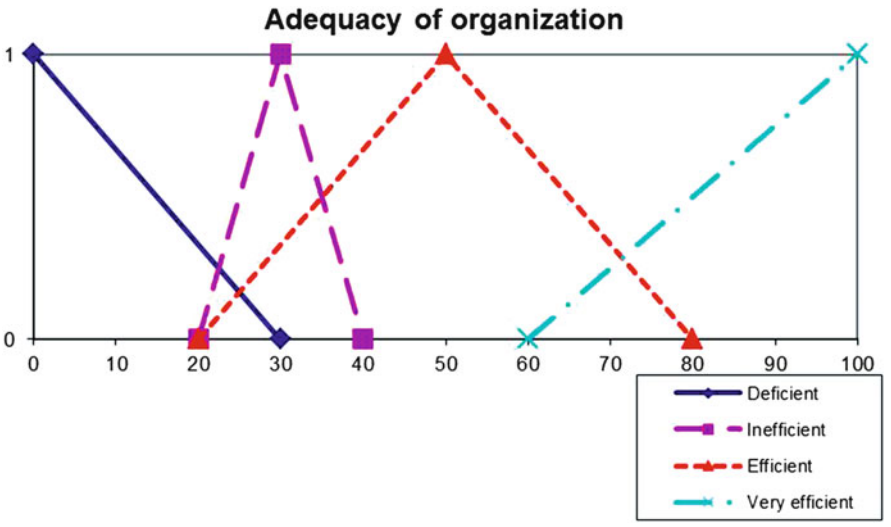


Fig. 3 Fuzzy sets representation of the "Adequacy of organization" input variable

performance. The "Efficient" set has a neutral effect on the final estimated probability. The fuzzy sets for the input variable "Adequacy of organization" are presented in Fig. 3.

Working Conditions: Three fuzzy sets, namely "Incompatible", "Compatible" and "Advantageous" were defined on the input space, which measure the quality of working conditions from 1 to 100 (Fig. 2). The first set "Incompatible" has a negative effect on human performance, while the third one "Advantageous" has a positive one. Again the second (intermediate) set, "Compatible", has a not significant effect on human reliability. The fuzzy sets for the input variable "Working conditions" are presented in Fig. 4.

Availability of procedures and plans: As in the previous input parameter, three fuzzy sets were defined, namely: "Inappropriate", 'Acceptable" and "Appropriate".

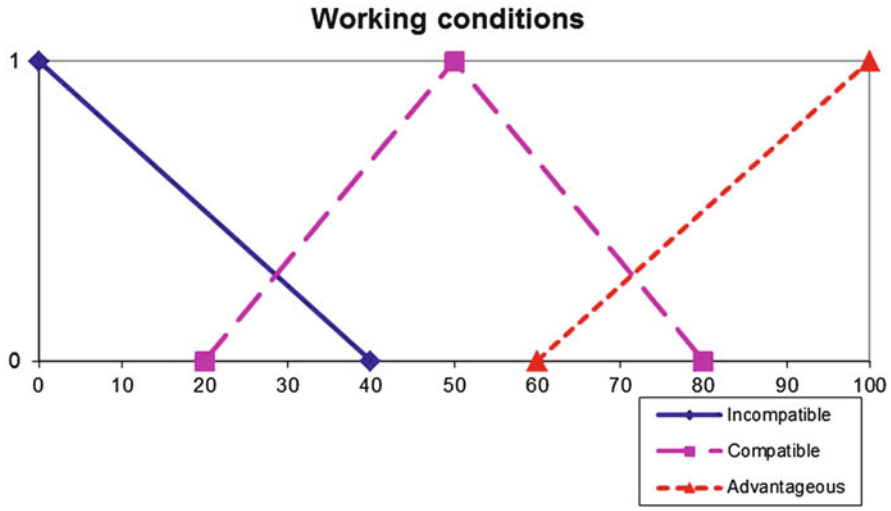


Fig. 4 Fuzzy sets representation of the "Working Conditions" input variable

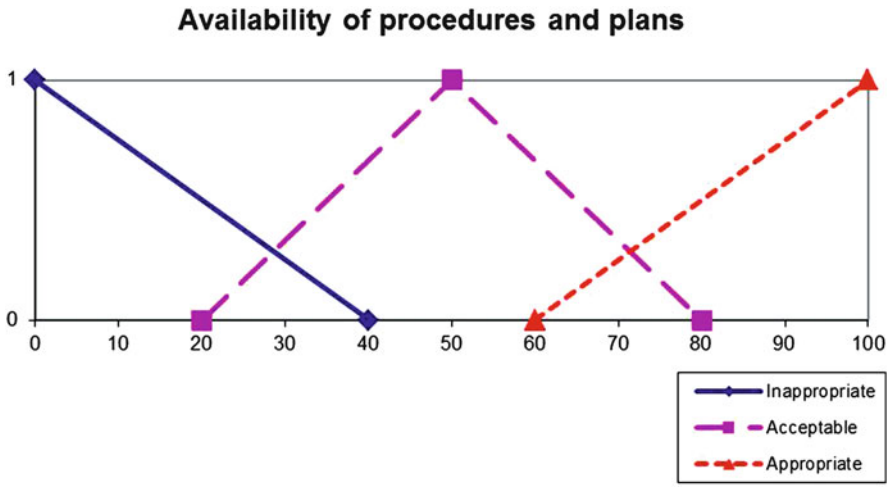


Fig. 5 Fuzzy sets representation of the "Availability of procedures and plans" input variable

Their range and their effect are exactly the same as in the above input parameter. The fuzzy sets for the input variable "Adequacy of procedures and plans" are presented in Fig. 5.

Adequacy of man-machine interface and operational support: Four fuzzy sets were defined for this input parameter named respectively, "Inappropriate", "Tolerable", "Adequate" and "Supportive". Only the first and the last fuzzy set influence human performance with a negative and positive effect respectively. The range of values covers again the interval from 1 to 100 and depicts the quality of

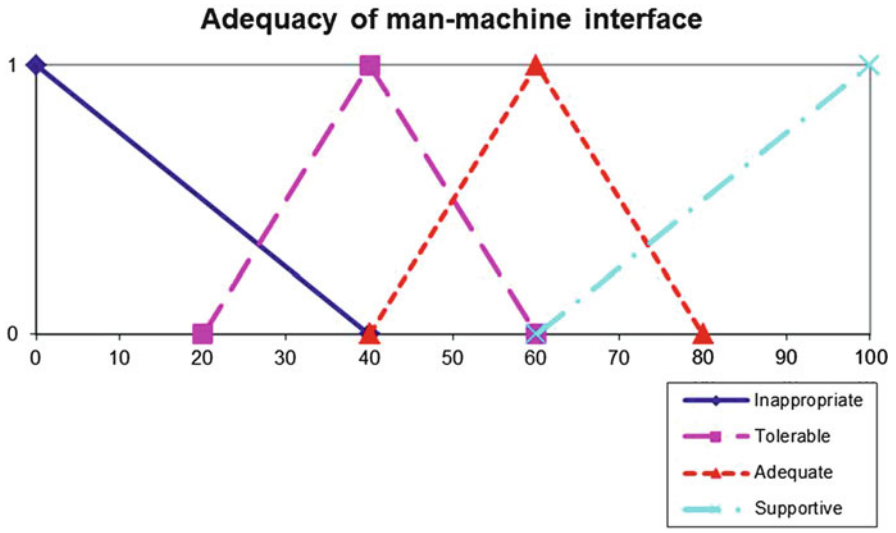


Fig. 6 Fuzzy sets representation of the "Adequacy of man-machine interface" input variable

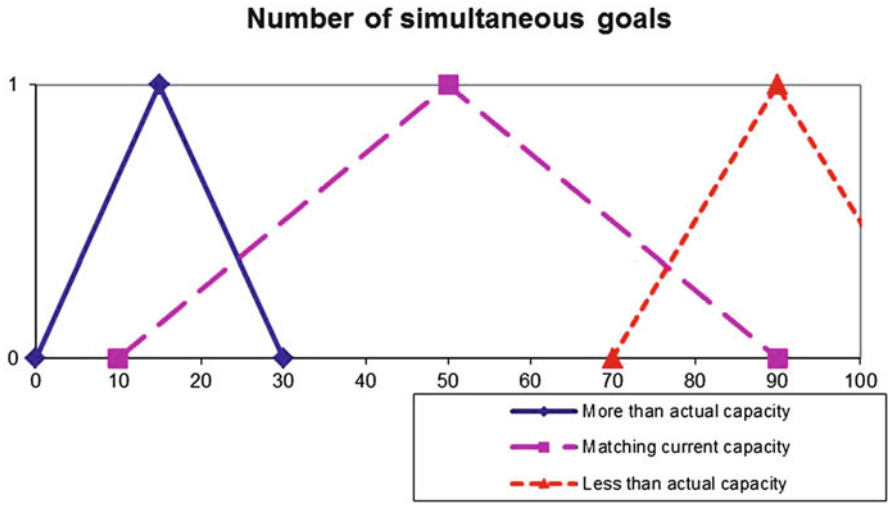


Fig. 7 Fuzzy sets representation of the "Number of simultaneous goals" input variable

man-machine interface and operational support. The fuzzy sets for the input variable "Adequacy of MMI" are presented in Fig. 6.

Number of simultaneous goals: Three fuzzy sets were defined for this input parameter, namely "More than actual capacity", "Matching current capacity" and "Less than actual capacity". The range is again from 1 to 100 and only the first set has a negative effect on human performance. The two remaining ones have neutral

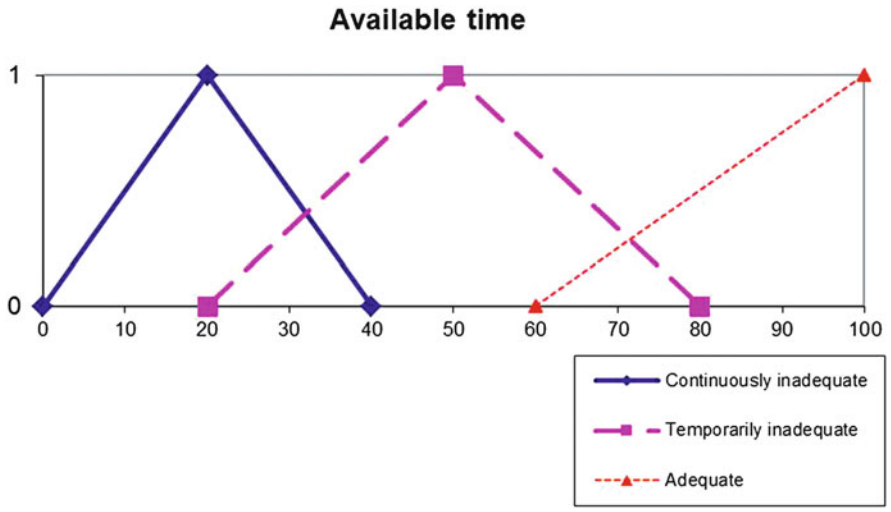


Fig. 8 Fuzzy sets representation of the "Available time" input variable

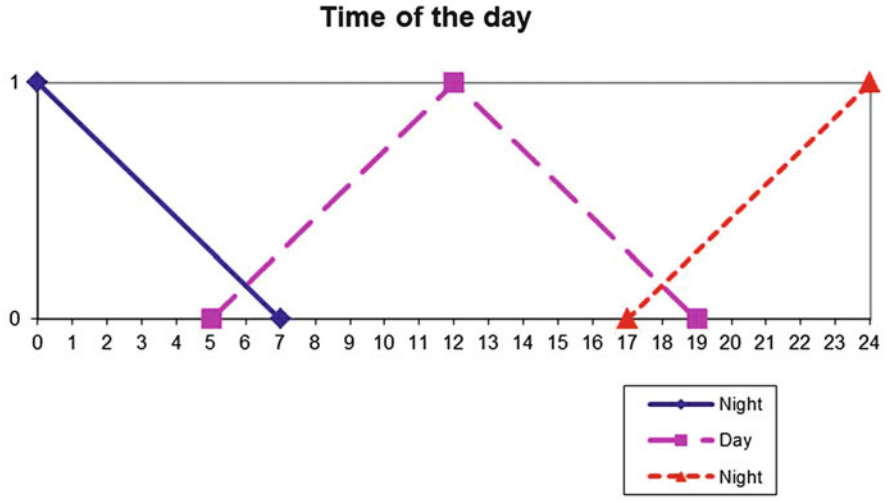


Fig. 9 Fuzzy sets representation of the "Time of the day" input variable

effect on human performance. The fuzzy sets for the input variable "Number of simultaneous goals" are presented in Fig. 7.

Available time: Three fuzzy sets with the names "Continuously inadequate", "Temporarily Inadequate" and "Adequate" were defined for this input variable and range from 1 to 100. The first set "Continuously inadequate", affects negatively the human performance, while the third one "Adequate" affects it positively. The

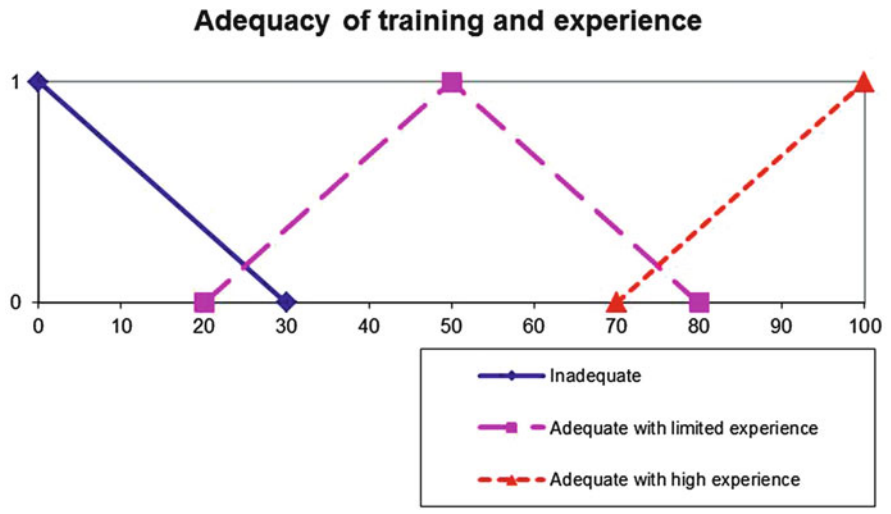


Fig. 10 Fuzzy sets representation of the "Adequacy of training and experience" input variable

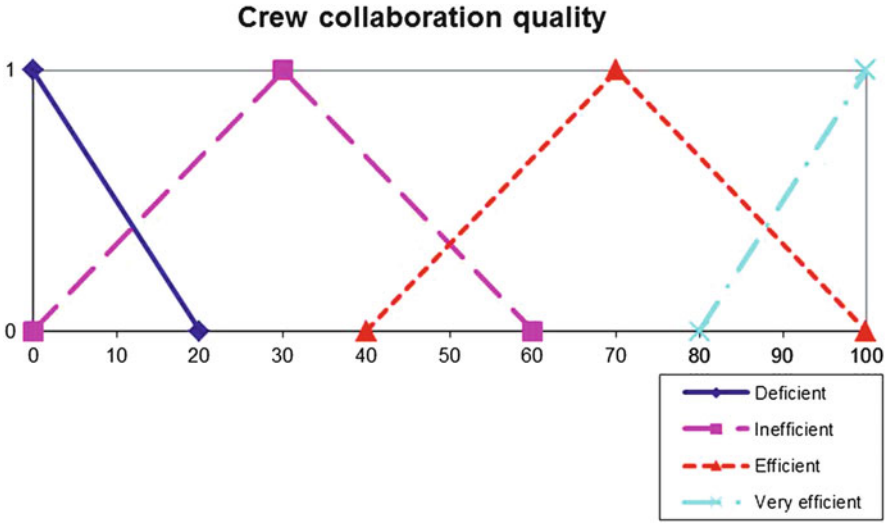


Fig. 11 Fuzzy sets representation of the "Crew collaboration quality" input variable

second one "Temporarily Inadequate" has not a significant effect. The fuzzy sets for the input variable "Available time" are presented in Fig. 8.

Time of day (Circadian Rhythm): Three fuzzy sets representing the 24 hours of the day were defined in this case. The first one covers the period from 0 (midnight) to 7 o'clock in the morning and together with the third one from 5 o'clock in the afternoon (17:00) until midnight are called "Night". The second class "Day" covers

Table 3 Impact of fuzzy sets on human reliability and effect on human error probability

Input variable	Relevant fuzzy sets	Effect on human error probability	Impact on human reliability
Adequacy of organization	Deficient	↑	Negative
	Inefficient	↑	Negative
	Efficient	-	Neutral
	Very efficient	↓	Positive
Working conditions	Incompatible	↑	Negative
	Compatible	-	Neutral
	Advantageous	↓	Positive
Availability of procedures and plans	Inappropriate	↑	Negative
	Acceptable	-	Neutral
	Appropriate	↓	Positive
Availability of MMI	Inappropriate	↑	Negative
	Tolerable	-	Neutral
	Adequate	-	Neutral
	Supportive	↓	Positive
Number of simultaneous goals	More than actual capacity	↑	Negative
	Matching current capacity	-	Neutral
	Less that current capacity	-	Neutral
Available time	Continuously inadequate	↑	Negative
	Temporarily inadequate	-	Neutral
	Adequate	↓	Positive
Time of the day	Night (morning)	↑	Negative
	Day	-	Neutral
	Night (evening)	↑	Negative
Adequacy of training and experience	Inadequate	↑	Negative
	Adequate with limited experience	-	Neutral
	Adequate with high experience	↓	Positive
Crew collaboration quality	Deficient	↑	Negative
	Inefficient	-	Neutral
	Efficient	-	Neutral
	Very efficient	↓	Positive

the period expanding from 6 o'clock in the morning until 6 o'clock in the afternoon (18:00). The sets "Night" have a negative effect on human reliability while the set "Day" has a neutral effect. The sets have been defined in a way to cover the daylight in an approximate way for all seasons of the year. The fuzzy sets for the input variable "Time of the day" are presented in Fig. 9.

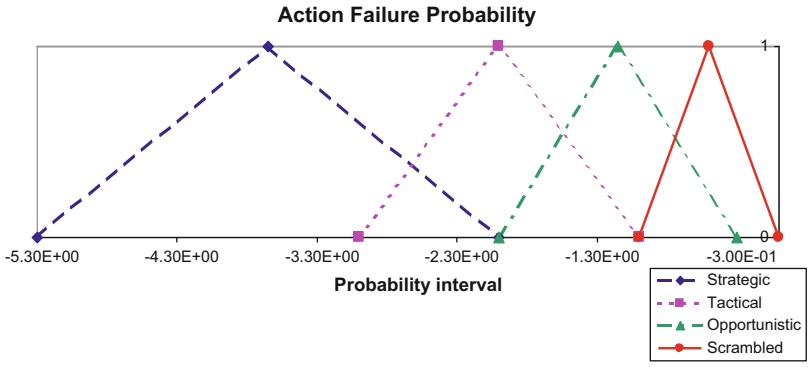


Fig. 12 Fuzzy sets representation of the "Action Failure Probability" output variable

The adequacy of training and experience: Three fuzzy sets were defined for this input variable under the names of "Inadequate", "Adequate with limited experience" and "Adequate with High experience. As in the previous input only the first and the third set have a negative and positive effect respectively, while the second one has neutral effect on human performance. The fuzzy sets for the input variable "Adequacy of training and experience" are presented in Fig. 10.

Crew collaboration quality: Four fuzzy sets, namely "Deficient", "Inefficient", "Efficient" and "Very Efficient" were defined on the input space. From the above the first set "Deficient" has a negative effect on human performance while the fourth one "Very efficient" has a positive effect on human performance. The third set "Efficient" and the second set 'Inefficient" have a neutral effect on the final estimated probability. The fuzzy sets for the input variable "Crew collaboration quality" are presented in Fig. 11.

Action failure Probability: As mentioned above the unique output variable is the probability of a human erroneous action varying from 0.510^{-5} (Strategic mode) to 1.0×10^{0} (Scrambled mode). For this variable, four triangular fuzzy sets were defined according to the probability intervals defined by CREAM. The fuzzy sets for the output variable "Action Failure Probability" are presented in Fig. 12. Figure 12 presents the above fuzzy sets using the logarithm of the probability in the x-axes for better output representation.

4.3 Step 3: Development of the Fuzzy Rules

During this step, a number of fuzzy rules have been developed following the logic of CREAM (Hollnagel 1998) and using its phrasing in the description of the input parameters and their association with the appropriate fuzzy sets. According to CREAM a screening of the input parameters can give an estimation of the mode in which an operator is acting (based on his Contextual Control Mode).

The rules are constructed in simple linguistic terms and can be understood at a common sense level. At the same time these rules result in specific and reproducible results (same inputs give same output). 46656 rules have been developed, taking into consideration the multiple fuzzy sets of each input parameter and using the logical *AND* operation as the building mode. The generation of 46656 rules may sound an extremely loading task; though this is not the case. Namely in the construction of the "if" (input) part of the rule some kind of automation has been used based on combinational synthesis of input parameters. However, the correlation of inputs with the "then" (output) part of each rule demanded some more effort, since manual screening has been applied in the assignment of the corresponding output fuzzy sets.

An example of a fuzzy rule is shown below:

> If the adequacy of organization is deficient AND the working conditions are incompatible AND the availability of procedures and plans is inappropriate AND the adequacy of man-machine interface and operational support is inappropriate AND the number of simultaneous goals is more than actual capacity AND the available time is continuously inadequate AND the time of the day is night AND the adequacy of training and experience is inadequate AND the crew collaboration quality is deficient THEN the operator would act in a SCRAMBLED way.

Acting in a SCRAMBLED way means that the probability of performing an erroneous action is between 1.0×10^{-1} and 1.0×10^{0}.

In the above fuzzy rule the underlined segments correspond to input variable definitions according to CREAM. It should be noticed that the development of fuzzy rules in every application is based on the knowledge and on the experience of the analysts team regarding the specific application. In the present case, the team took advantage of the experienced offered by CREAM in the development of the fuzzy rules.

In fact, as mentioned in Sect. 2.7, the control mode in which the operator is likely to act, is defined by the sums of the positive influence on the one hand and the negative on the other of the various CPCs. This is done by the use of Fig. 2, in which the basic CREAM diagram depicts every possible combination of the sum of the input parameters that have a negative effect on human reliability performance in the x-axis and the sum of the input parameters that have a positive effect on human reliability performance in the y-axis. Every possible combination of these sums corresponds to a point in the diagram correlated with a specific operator contextual control mode (strategic, tactical, opportunistic or scrambled). This very diagram has been used by the analysts team to produce the 46656 fuzzy rules of the proposed fuzzy model.

In the fuzzy rule described above, the point (9, 0) indicates the specific context defined according to CREAM by the input variables, since all 9 CPCs have a negative effect on human reliability (reduced reliability), and 0 parameters have a positive effect on human reliability (improved reliability). The point (9, 0) is located in the "scrambled" control mode relevant area (see Fig. 2 in the description of CREAM methodology section).

Another example of a fuzzy rule for the specific application is the following:

If the adequacy of organization is inefficient AND the working conditions are compatible AND the availability of procedures and plans is acceptable AND the adequacy of man-machine interface and operational support is tolerable AND the number of simultaneous goals is more than actual capacity AND the available time is adequate AND the time of the day is day AND the adequacy of training and experience is high adequate AND the crew collaboration quality is efficient THEN the operator would act in a OPPORTUNISTIC way.

Acting in a OPPORTUNISTIC way means that the probability of performing an erroneous action is between 1.0×10^{-2} and 0.5×10^{0}.

Again the point for the specific context in the CREAM diagram is (3, 1) since 3 CPCs have a negative effect on human reliability, while only one has a positive effect on it. The point (3, 1) is situated in the "opportunistic" control mode relevant area (see Fig. 2).

For the development of the model, the analysts have been based on the basic edition of CREAM method. It is understandable that not all input parameters have equal importance. In this general application though, no weighting schemes have been used, as it has been assumed that all of them have equally important effects. However, for the development of the fuzzy rules, it has been taken into account that if some rules are contradicting themselves (e.g. it is not "logical" to have *very efficient* adequacy of organization and *incompatible* working conditions), their degree of truth will be minimum and hence these rules will be less considered (will have lower priority).

4.4 Fuzzy Model Operations

As explained in Sect. 3.1, a three-step procedure defines the knowledge base of the fuzzy system. When the fuzzy model is to be applied to a set of input parameter values, the information flows through the fuzzification-inference-defuzzification processes, which are depicted in Fig. 13, in order to generate the fuzzy probability estimation that the operator will perform an erroneous action. For this particular fuzzy system, the above-mentioned three processes are executed as follows:

Fuzzification: the fuzzification process consists of determining the degree of truth of each rule premise, (which part of the rule could be activated by a specific input), given that the values for each input parameter have been assigned. This is done through the triangular membership functions (fuzzy sets) defined on each input variable.

Inference: The inference process assigns one output fuzzy set to each rule. Then, the degree of truth for the activation of each rule is computed, and applied to the conclusion part (then part) of the rule. Based on the degree of truth of each part of the rule the *min-max* inference technique is used (Klir and Yuan 1995), in order to define the influence of this rule on the output membership function. According to this technique, if all parts of the rule are activated except for at least one, the entire rule is not activated either. Moreover the inference technique considers the

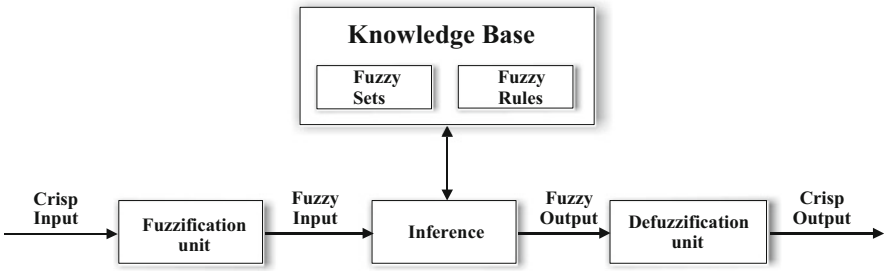


Fig. 13 The structure of a typical fuzzy logic system

minimum degree of activation for each rule and depicts it on the corresponding output set. The combined fuzzy output membership function is then constructed by the combination of the effect of all the fuzzy rules. If an output fuzzy set is targeted by more than one rules, then the maximum value among all hits is retained in the construction of the combined output membership function.

Defuzzification*:* Since the final output of the fuzzy system modeling should be a crisp number for the human probability error, the fuzzy output needs to be "defuzzified". This is done through the centroid defuzzification method (Pedrycz 1993), where a crisp value for the output variable is computed by the analytical calculation of the "gravity" center of the produced area for the combined membership function in the inference step above.

The fuzzy logic system developed using this approach gives very satisfactory results. It can be used to calculate the probability that an operator will perform an erroneous action given any combination of input values, which cover the specific context of the parameters that influence his performance reliability. The user must simply supply the input values for a specific working environment or context (according to his knowledge and experience in the relevant application) and the system will compute the human error probability within the specific context. As an example some results from test runs are presented in Table 4.

The model has been tested for its reliability, sensitivity in input changes, usefulness and velocity. It has been proved that it is consistent (same input produces same output) and sensitive, since even small variations in the input variables induce changes in the results. Concerning the values of the results, according to CREAM all the results are to be found in their appropriate areas of human control mode (strategic, tactical, opportunistic, scrambled). The main improvement by the application of the fuzzy model is that the output is probabilities estimation with exact numbers, which can be directly used in other quantitative risk assessment methods, such as fault trees and event trees, where human error probabilities demanded for action failures are based on specific industrial contexts.

The results of the fuzzy model, which are in the form of crisp numbers, can be used directly in fault trees and event trees calculations for the quantification of specific undesired events that include the interaction of human factors in their

Table 4 Results of test runs for five different scenarios (indicatively)

Sc	Adequacy of organisation	Working conditions	Availability of procedures	Adequacy of MMI	Number of simultaneous goals	Available time	Time of day	Adequacy of training	Crew collaboration quality	Action failure probability
1	22	30	40	50	60	70	4	50	70	1.00×10^{-2}
2	90	90	90	90	90	90	12	90	90	9.81×10^{-4}
3	15	17	38	42	78	45	22	56	78	6.33×10^{-2}
4	10	10	10	10	10	10	2	10	10	2.02×10^{-1}
5	10	12	12	14	15	16	20	18	20	1.91×10^{-1}

modeling. The precision of human error probability is reported with two decimal numbers following the format of standard reliability analyses, used also in most of the reliability databases with comparable magnitude of uncertainty in the reported values. Considering its computational time it is rather quick as long as the knowledge base remains in reasonable sizes.

Other possible uses of the model are presented in the following sections.

5 Critical Transitions (Konstandinidou et al. 2006)

The influencing factors, as mentioned in Sect. 2, present a very important aspect in the calculation of human error probabilities. The context in which the human action will take place is defined by these factors. Moreover, the influencing factors, as indicated by their name, influence the action failure probability of the human operators, by increasing it when they have a negative effect on it (i.e. when their values approach 0), or by decreasing it when they support the action and the operator (i.e. when their values go towards 100). What is common knowledge (but not common practice) is that the better the quality of these factors the more reliable the operator behaviour.

It goes without saying that the engineer could seek the absolute optimization of the influencing factors in the area of his/her responsibility. In this way, by raising all factors to 100% of their quality, the action failure probability of the operator should be minimal. This is not however always achievable, since not all factors can be 'boosted' up to 100% (e.g. training would never come to a 100% level since it is impossible to train one operator for all operational conditions and emergency situations; the same applies to crew collaboration, where the notion of 100% quality is unachievable). For other parameters, like 'working conditions' and 'plans and procedures', there will always be available space for further improvement. Working conditions include many aspects such as lighting, noise, temperature, ergonomy, and workspaces; it is practically impossible to cover all of them and to raise their level to 100% in industrial environments. Procedures and plans should always be updated and available, but this is not always feasible in complex and big industrial units. There are other input parameters such as 'available time', which in conjunction with the input parameter 'number of simultaneous goals' define the level of stress for the operator; this level even with same scores for the two input parameters can be different between two operators in practice. The parameter 'time of day' which deals with the operator's circadian rhythm is another subjective factor that is individual-dependent. Moreover, bringing all nine factors up to 100% of their quality, may sometimes be too expensive. A decrease in human error probabilities (as action failure probabilities) would not always compensate the extremely high cost of the introduction of additional measures and systems to improve the current situation.

What needs to be done is to define critical areas within which these improvement possibilities need to take place and define the critical transitions for specific

Table 5 Values for the input parameters and action failure probability of the specific scenario

Parameter	Value
Adequacy of organization	37
Working conditions	26
Availability of procedures	15
Adequacy of MMI and operational support	4
Number of simultaneous goals	68
Available time	79
Time of day (circadian rhythm)	11
Adequacy of training	83
Crew collaboration quality	92
Action failure probability	1.85×10^{-2}

influencing factors, i.e. the improvement that leads to an important reduction in the human error probability. Not every variation (increase or decrease in the value of the specific relevant input parameter) induces the same variation on the output parameter. Indeed, there are cases in which small variations in specific intervals induce high variations in the probability of action failure, and others in which variations in input parameters do not influence the final result at all. The fuzzy model, which has been developed according to CREAM methodology, can be used in order to determine the critical transitions for the nine input parameters described in Sect. 4.1. What needs to be mentioned here is that in the application of the fuzzy model no weightings are used on the input parameters; in this way the good or poor quality of an input parameter will not bias the impact of the variations in other parameters on the value of the action failure probability.

In order to define the critical transitions of the influencing factors in human reliability, a random scenario with specific values of input parameters describing a specific working context has been selected. The values of the input parameters and the action failure probability are presented in Table 5. The values characterize the specific conditions of the working context where the value '100' represents the best quality conditions and the value '0' represents the worst quality conditions. Initially, the probability of action failure for the defined scenario was calculated with the use of the fuzzy model. Then, variations of 10% (either increasing or decreasing) in the values of the nine input parameters were imported to the model. For the input parameter 'time of day' the variations were increases and/or decreases of 1 h. In each run of the model, eight out of the nine input parameters remained stable and the variation was performed in one of the input parameters only. According to the variation of the output result, the action failure probability calculated by the fuzzy model, the influence of the variation in the input parameter, is depicted.

By testing one parameter at a time, with increases and decreases of 10% in the initial values at appropriately designed model runs, the critical transitions for each parameter have been defined. The importance of the critical transitions is that, within these intervals, the maximum variation in the output result is registered. In this way, the analyst or the engineer is able to achieve a better operator performance without being obliged to reach 100% quality for every input parameter, since this is

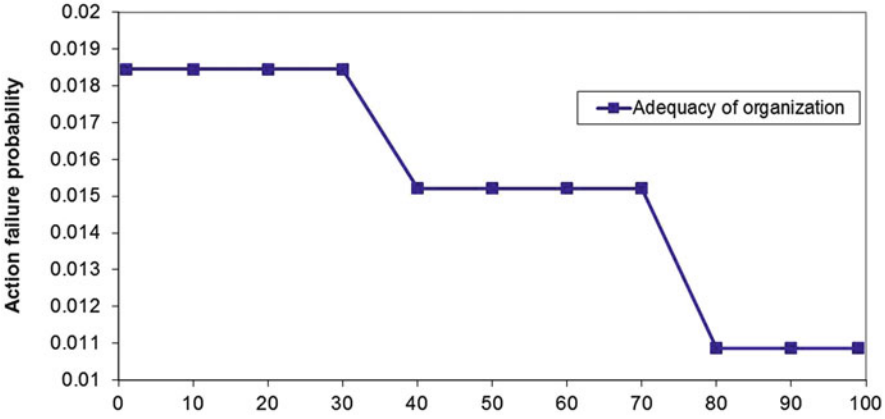


Fig. 14 Critical transitions for the input parameter "Adequacy of organization"

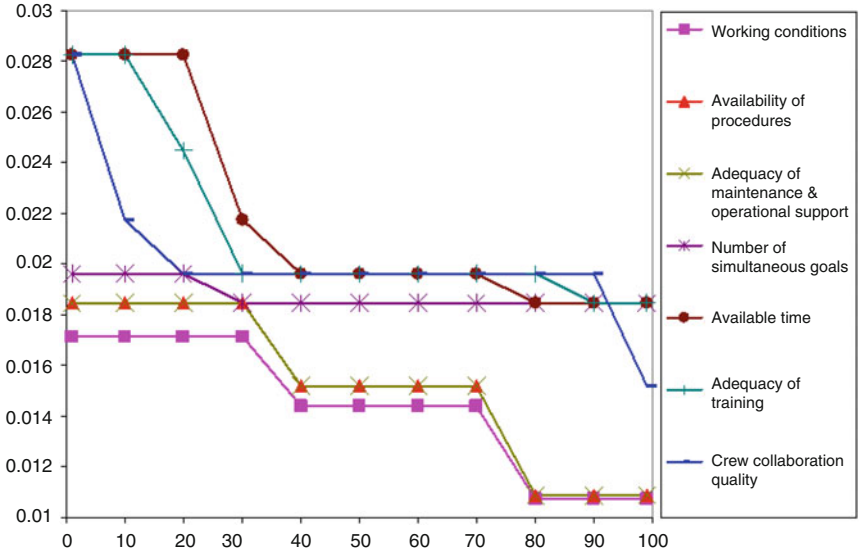


Fig. 15 Critical transitions for all input parameters with values (0–100)

not always affordable or achievable. Results from this "sensitivity analysis" can be seen in Figs. 14, 15 and 16. In Fig. 14 the critical transitions for the input variable "Adequacy of organization are presented", while in Fig. 15 critical transitions for all input parameters (except for "time of the day") are summarized. "Time of the day" input variable is presented in Fig. 16 as it refers to a different scale (0–24 h).

The results of the model after the defuzzification process are human error probabilities that are obtained in the form of crisp numbers; thus they can be used for human reliability purposes as well as for probabilistic assessments of potential

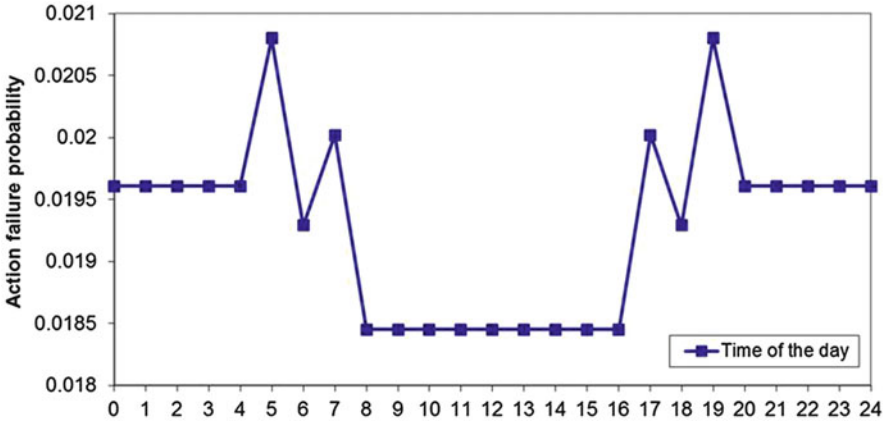


Fig. 16 Critical transitions for the input parameter "time of the day"

accidents in industrial establishments. Additionally, they can be used in cost-benefit analyses by a direct comparison of the parameters' adjustment costs with the impact they have on the performance and reliability of the human operator. The most important point of this analysis is that in the estimation of the action failure probabilities no subjective evaluations and judgments have been used. In this way the results can be used to compare different working contexts when they are in a phase of change or at the design stage. The results of this study offer an additional use of the already developed model; as the results are presented as percentages they can be used in analyses for the improvement of human reliability and performance.

These percentages represent the variations induced on the output result, namely the action failure probability, as a result of the variations in the input parameters. The values of these percentages are not important per se; the most important result is rather the fact that with the use of the fuzzy model it is possible to define the critical intervals within which the significant variations are located. Indeed, the values of the action failure probability change with different initial values and scores. However, the determination of the critical transitions remains the same, highlighting in this way the points on which the analyst should focus and the areas of improvement that are meaningful and essential.

6 Operators Response Time (Konstandinidou et al. 2009)

In Human Reliability Analysis the notion of human error does not correspond only to the likelihood that an operator will not perform correctly the task that he has been assigned to do but also (among other things) to the likelihood that he will not perform the assigned task within the required time. Most of the critical tasks include the concept of time in their characterization as "critical" and most of the error

taxonomies developed specifically for human reliability analysis include errors like "too early/too late", "action performed at wrong time", "delayed action", "operation incorrectly timed", "too slow to achieve goal" and "inappropriate timing" (Embrey 1992, Hollnagel 1998, Isaac et al. 2002, Kontogiannis 1997, Swain and Guttmann 1983). What is thus important for Human Reliability Analysis is the identification and quantification of human error and at the same time the estimation for the response time of the operator in the performance of a critical task. In modeling human performance for Probabilistic Risk Assessment it is necessary to consider those factors that have the biggest effect on performance. The same is also valid for factors that influence operators' response time. Many factors influence human performance in complex man-machine systems like the industrial context but not all of them influence the response time of operators, at least not with the same importance.

The expansion of the model, covers also operators' response time data related with critical tasks. The model disposes also a second output variable that calculates the estimated response time of the operator performing a specific task in a specific industrial context. For the estimation of the response time the model takes into account factors (common performance conditions) that influence the reaction of the operator during this specific task.

6.1 Fuzzy Model Operations with Operators Response Time

In order to produce estimates for response time of operators in industrial context the fuzzy model for Human Reliability Analysis previously developed and described has been used. With this model as a basis the fuzzy model for "Operators' Response Time—ORT" estimation has been built.

The functional characteristics of the initial model remained as they were defined. That means that the same nine input parameters with the same defined fuzzy sets have been used. The phrasing and the linguistic variables have remained the same too. This was very helpful in order to have a correspondence between the two models.

The new model disposes of a new output parameter namely "operators' response time". The output parameter provides the needed estimations for operators' response time. In order to maintain the connection with the initial model the same names and notions in the output parameters were used. The output fuzzy sets correspond to the four control modes of the COCOM model that is the cognitive model used in CREAM (Hollnagel 1998).

For the application of the "ORT" fuzzy model the four control modes were used to define the time intervals within which the operator would act to complete a critical task. Hence quick and precise actions that are completed within very short time are compatible with the "strategic" control mode; "tactical" control mode includes actions within short time intervals slightly more broad than the previous one; "opportunistic" control mode corresponds to slower reactions that will take

Table 6 Control modes and response time intervals

Control mode	Operators' response time (minutes) Min	Max
Strategic	0	$< t < 0.1$
Tactical	0.01	$< t < 1$
Opportunistic	0.1	$< t < 5$
Scrambled	1	$< t < 10$

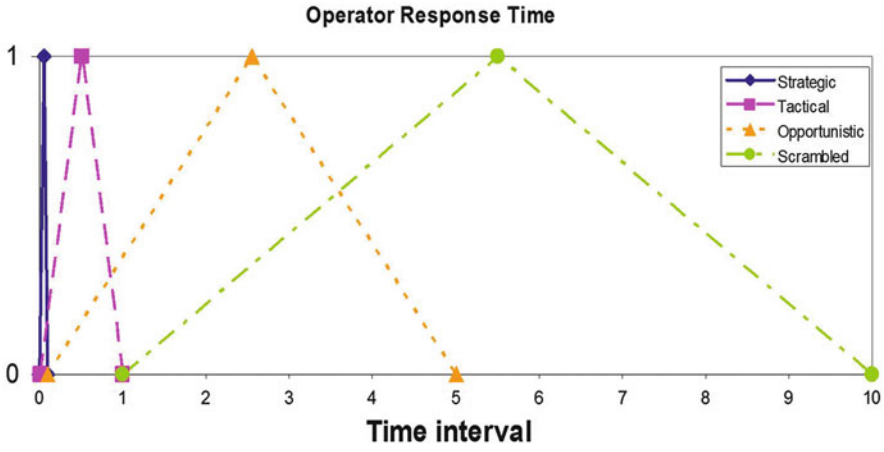


Fig. 17 Fuzzy sets representation for the "Operator Response Time" output variable

longer time while "scrambled" control mode includes more sparse and time consuming reactions.

The relevant time intervals as defined for the four control modes in the "ORT" fuzzy model are presented in Table 6. A graphical representation of the four fuzzy sets is given in Fig. 17.

A crucial step in the development of the model is the development of the fuzzy rules. A cluster of fuzzy rules to include all the possible combinations of the input parameters fuzzy sets has been developed previously. 46656 rules have been defined, taking into consideration the multiple fuzzy sets of each input parameter and using the logical AND operation as the building mode.

The fuzzy rules for the extension of the model retained the "if—part" of the initial model and the "when" part was changed accordingly to include the time notion.

An example (i.e. the first rule) is the following:

> If the adequacy of organization is deficient AND the working conditions are incompatible AND the availability of procedures and plans is inappropriate AND the adequacy of man-machine interface and operational support is inappropriate AND the number of simultaneous goals is more than actual capacity AND the available time is continuously inadequate AND the time of the day is night AND the adequacy of training and experience is inadequate AND the crew collaboration quality is deficient THEN the operator would act

in a SCRAMBLED way. Acting in a SCRAMBLED way means that the response time for the operator is between 1 and 10 minutes.

In this way all the possible combinations of the input fuzzy sets correspond to one (and only one) output fuzzy set and to the relevant control mode with the associated time interval.

In order to have a crisp number as output variable (and not an output set) the centroid defuzzification method (Pedrycz 1993) has been used as in the initial model. In this way the model comes up with specific estimates for operators response time expressed in minutes.

Results from the application of this "extended" model are presented in Table 7.

Results are within the defined range as defined in Table 6. From observations that have been performed in the industry it has been depicted that the response time of operators for situations similar to:

- Scenario 6: records for operators' response time within 4–7 min (i.e. 240–420 s)
- Scenario 7: records for operators' response time within 2–5 min (i.e. 60–300 s).
- Scenario 8: records for operators' response time within 1 min (~60 s).

Therefore the application of the model can be considered satisfactory. However in order to be sure about the results of the model and validate them with real data a specific application for a specific critical task in a petrochemical plant has been developed. This application is presented in the following section.

6.2 *Application Description: Critical Task in Process Industry*

In order to test the model a real life application has been chosen. A specific task, which is the opening/closure of a manual valve in order to maintain a desired pressure drop, is performed regularly in a petrochemical unit. This task may be performed at least twice a day during normal operation in order to unclog the drain channel. The same task is performed during maintenance operation in order to shut down or start up the unit. In case of an abnormality that leads to the trip of the unit or in case of equipment malfunction the operators are called to act immediately and perform the same task in order to maintain the desired pressure drop so that the unit is not jeopardized. This is equivalent to emergency response situations.

The required time frame for the specific task is very tight. Operators must complete their actions within 1–2 min. Otherwise pressure may rise or may drop beyond the safety limits and disturb the operation of the whole unit or even worse (in case of extreme variations) result in equipment failure. Pressure rises and/or drops in few seconds in the specific node so operators' response is crucial and should be prompted. For the completion of the task one operator is needed.

The reaction time of the operators in the execution of this task has been recorded through the pressure drop indication reported in the control room. Data concerning

Table 7 Results from the Operator Response Time model (indicatively)

Sc.	Adequacy of organisation	Working conditions	Availability of procedures	Adequacy of MMI	Number of simultaneous goals	Available time	Time of day	Adequacy of training	Crew collaboration quality	Operator Response Time (s)
1	100	100	100	100	90	100	12	100	100	7
2	90	90	90	90	90	90	12	90	90	8
3	0	0	0	0	15	20	0	0	0	480
4	10	10	10	10	10	10	2	10	10	476
5	50	50	50	50	50	50	12	50	50	59
6	90	20	90	50	90	20	0	0	50	294
7	90	20	90	50	15	20	12	50	50	276
8	90	20	90	50	50	20	12	100	50	59

the specific in—field task of the petrochemical unit has been gathered during a whole year period. From those data it was noticed that normal reaction time is within 10–15 s (when performing the normal—drain operation), reaction time during maintenance was around 1 minute, while reaction time in emergency situations was between 1 and 10 min depending on the case.

After discussion with the key personnel of the unit on the specific events that took place during the one year period the conclusions were that the elements that differentiate the reaction time of the operators is the level of experience each operator has and the number of tasks he is assigned to do in the same time. This number varies between normal operation, maintenance and emergency response situations. What has also been observed through the collected data is that the time of the day plays also an important role in some situations: operators' response time is different between day and night shifts.

Hence for this specific task the influencing factors that have a direct impact on the operators performance are: the circadian rhythm of the operator, expressed in terms of the hour of the day that he/she is requested to perform the task; the experience and the training he/she obtains, expressed in years of presence in the specific unit (and the petrochemical plant); the number of simultaneous goals, expressed in terms of parallel tasks to be performed during normal operation, maintenance (task performed in order to shut down or to start up the unit) or emergency situations (equipment malfunction, trip of the unit).

The conclusions of the observations were the basis for the development of a shorter version of the fuzzy model, a model that would include only the influencing factors of this application with the relevant fuzzy sets. This is meaningful since all the nine parameters that are included in the full version of the "ORT" model do not affect response time in this particular application and the computational cost of the model is significantly decreased with the use of only three input parameters. Additionally by building a new—tailored made model for the specific application new fuzzy sets for the output parameter "operators' response time" can be used and adjusted according to real data.

6.3 The "Short-ORT" Fuzzy Model for a Specific Application:Tailored Made Models

For the development of the tailored made "Operators Response Time—ORT" short model the Mamdani type of fuzzy modelling was used and the development of the system was completed in four steps.

1. Selection of the input parameters

   For the specific application three input parameters have been chosen according to the conclusions stated in the previous section. These input parameters are:

(a) The number of simultaneous goals
(b) The adequacy of training and experience
(c) The time of the day

As unique output parameter was defined the Operators Response Time.

2. Development of the fuzzy sets

In the second step, the number and characteristics of fuzzy sets for the input variables and for the output parameter were defined. The definition of the fuzzy sets was made according to the observations from the real data and the comments of the key personnel as stated previously.

'Number of simultaneous goals': for the first input parameter three fuzzy sets were defined namely "Normal operation", "Maintenance" and "Emergency Situation".

'Adequacy of training and experience': for the second input parameter two fuzzy sets were defined namely "Poor Level of Training and Experience" and "Good Level of Training and Experience".

'Time of the day': for the last input parameter two fuzzy sets were distinguished corresponding to "Day" and "Night".

'Operators' response time': The output parameter had to cover the time interval between 0 and 10 min. Five fuzzy sets were defined to better depict small differences in reaction time and the equivalent time range was expressed in seconds. The fuzzy sets with the time intervals each of them covers are presented in Table 7. More precisely operators' response time is "Very good" from 0 to 20 s, "Good" from 10 to 110 s, "Normal" from 60 to 180 s, "Critical from 120 to 360 s and "Very critical" from 270 to 1170 s. A graphical representation of the five fuzzy sets is given in Fig. 18 in order to visualize the range of each time set.

3. Development of the fuzzy rules

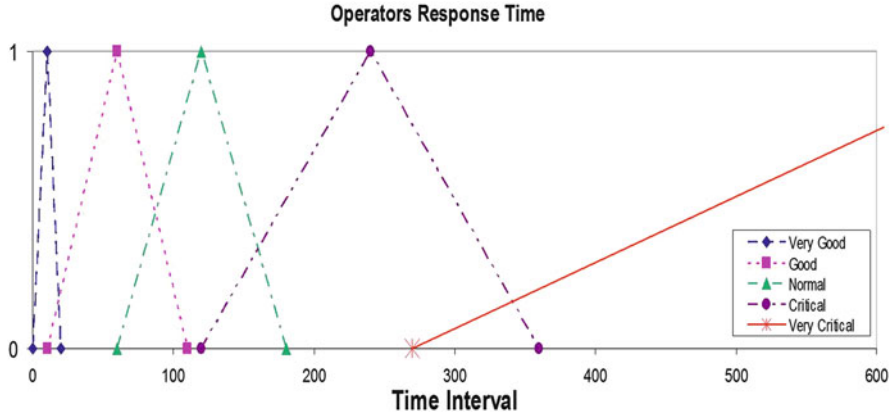


Fig. 18 Fuzzy sets representation for the "Operator Response Time" output variable of the short model

The observation data and the expertise of the key personnel were the knowledge base for the development of the fuzzy rules. The following observations determined the definition of the fuzzy rules:

(a) Time of the day (day/night) does not affect operators' response time during normal operations
(b) Time of the day (day/night) does not affect operators' response time for operators with good level of training and experience

According to the observed data and by taking into account the above mentioned statements 8 fuzzy rules were defined for the short "ORT" fuzzy model:

- Rule 1: "If number of goals is equivalent to normal operation and adequacy of training and experience is good then operators' response time is very good".
- Rule 2: "If number of goals is equivalent to normal operation and adequacy of training and experience is poor then operators' response time is good".
- Rule 3: "If number of goals is equivalent to maintenance and adequacy of training and experience is good then operators' response time is good".
- Rule 4: "If number of goals is equivalent to maintenance and adequacy of training and experience is poor and time is during day shift then operators' response time is normal".
- Rule 5: "If number of goals is equivalent to maintenance and adequacy of training and experience is poor and time is during night shift then operators' response time is critical".
- Rule 6: "If number of goals is equivalent to emergency and adequacy of training and experience is good then operators' response time is normal".
- Rule 7: "If number of goals is equivalent to emergency and adequacy of training and experience is poor and time is during day shift then operators' response time is critical".
- Rule 8: "If number of goals is equivalent to emergency and adequacy of training and experience is poor and time is during night shift then operators' response time is very critical".

4. Defuzzification

Since the final output of the fuzzy system modeling should be a crisp number for the operators' response time, the fuzzy output needs to be "defuzzified". This is done through the centroid defuzzification method (Pedrycz 1993) as in the previously developed fuzzy models (Table 8).

The fuzzy logic system has been built in accordance with the real data coming from the petrochemical unit for the specific application. The testing of the model and its comparison with the full version is shown in Table 9 and discussed in the following section.

Table 8 Output fuzzy sets for Operators Response Time (short model)

Fuzzy set	Time interval (in seconds)
Very good	$0 < t < 20$
Good	$10 < t < 110$
Normal	$60 < t < 180$
Critical	$120 < t < 360$
Very critical	$270 < t < 1170$

Table 9 Results from the application of the two versions of "ORT" fuzzy model

Number of simultaneous goals	Training	Time of day	"ORT" model (s)	"ORT Short" (s)
Normal operation	Good	Day	59	13
Maintenance	Good	Day	59	60
Emergency situation	Good	Day	59	120
Normal operation	Good	Night	59	13
Maintenance	Good	Night	59	60
Emergency situation	Good	Night	59	120
Normal operation	Poor	Day	59	60
Maintenance	Poor	Day	59	120
Emergency situation	Poor	Day	276	240
Normal operation	Poor	Night	294	60
Maintenance	Poor	Night	294	240
Emergency situation	Poor	Night	294	570

6.4 Discussion on the Results

While the original "ORT" model seems quite inflexible in its results (and mainly in the variation of some input parameters), the results from the "ORT-short" model are very satisfactory. According to the estimates of the "ORT-short" model a well experienced operator will react in 13 s during normal operation in day and night shift, in 60 s during maintenance in day and night shift and in 120 s in emergency situations during day and night shift. This is in accordance with observation (a) that the time of the day does not affect the response time of an operator with good level of training and experience. Subsequently an inexperienced operator will react in 60 s during normal operation in day and night shift, in 120 s during maintenance in day time and 240 in night time shifts, and in 240 s in emergency situations during day shift and 570 in night shift. This is in accordance with observation (b) that the time of the day does not affect the response time in normal operations.

Differences between day and night shifts as well as task performed during normal operation, maintenance and emergency situation from experienced and inexperienced personnel are well depicted with relevant differences in operators' response times. In fact in the extreme situation of an emergency during night shift where an inexperienced operator is called to act the estimated response time from the model is 570 s which is in accordance with the observed data of 10 min (600 s).

The fuzzy logic system estimations are in accordance with the real data coming from the petrochemical unit. Indeed, observation data showed very slow and very critical response of inexperienced operators during night shifts and in emergency situations.

The detailed steps of the specific application coming from a real life industrial process can be followed in case similar tailored made models are needed. Indeed with good observations a knowledge based can be built and help the analysts develop their own fuzzy rules according to the observations. Records of real time reactions can be used as the relevant output for the specific applications.

7 Conclusion

When dealing with decision making problems it is necessary to aggregate the available information in order to take decisions. This is particularly true for human operators in the process industry, where the early perception of signals, diagnosis of problems and timely reaction is of utmost importance to business unobstructed operation. Indeed, business failure prediction has been an important research area for many decades. These failure models compare and classify firms according to quantitative indicators, to predict or distinguish between healthy and unhealthy businesses (Vigier et al. 2017). Operation experience of socio-technical systems, such as nuclear power plants (NPPs), chemical plants, petro-chemical plants, commercial airplanes, clearly demonstrated that the accident or incident of such systems is catastrophic resulting in massive casualties, severe environmental damages and enormous financial losses. Thus, it is very important to manage the safety level of the socio-technical systems within an acceptable limit, as it is revealed that one of the significant factors causing accidents or incidents is the performance degradation (e.g., human error) of operating personnel working in the socio-technical systems (Park et al. 2015).

The role of innovations in user interaction technologies is also to be taken seriously into account (Boecker 2015). Nowadays, user interaction technologies play a vital role in providing an excellent user experience and product usability. They are an essential part of the user interface, which is a key element of the user experience: the user interface is the visible and tangible part of the product and the enabler of the interaction, and thereby, of the user. Novel user interaction technologies have the potential for increasing the user's effectiveness, efficiency and easiness with the interaction, in other words, for increasing the product's or system's usability. Furthermore, in some industries, advanced interaction technologies can empower operators' decision making. They can readily convey the necessary information derived from often sophisticated process simulation systems running in the background. However, the evaluation of interaction technologies requires the investment of resources, which raises the question of how to best collect and review interaction technologies, and on which criteria to base the decision on.

In this chapter an application of fuzzy logic has been presented as a potential solution to human error quantification uncertainty. Indeed the results from the application of the model are very promising; if the base of the model is a well-conceived and defined methodology (such as CREAM in this case) the outcome of the model might be used also in subsequent applications. The present model has been expanded to cover also operators' response time in critical tasks and has been also tested in a real life application.

In order to estimate the performance times of operators in safety critical tasks, it is strongly recommended to contact and "benchmark" all the operators that are involved in the specific procedures. For example, if we are able to observe the response time of operators who have to draw a decision on the remedial action of a given expected deviation even with the interaction of other departments of the installation, this information could give a valuable insight in estimating the response time of operators under an abnormal process deviation alarm signing. Similarly, the cognition times of operators, who have to cope with a stressful condition against similar events could play an important role in determining their cognition time in the damage state to arrive. The results of the presented study has shown a promising direction in this respect.

Following the steps described in the section of the "ORT-short" model similar tailored made models based on fuzzy logic architecture can be developed for different tasks and contexts e.g. maintenance tasks, other in-field actions or control room operations in the running of a chemical plant.

The use of the model could be also expanded to other fields of the chemical industry or fields where human factor plays an important role in the triggering and evolution of accidents. Such fields can be the aviation technology and the maritime transports, where the human factor has already "contributed" in the occurrence of several accidents.

References

Baziuk PA, Rivera SS, Núñez Mc Leod J (2016) Fuzzy human reliability analysis: applications and contributions review. Adv Fuzzy Syst. doi:10.1155/2016/4612086

Bedford T, Bayley C, Revie M (2013) Screening, sensitivity and uncertainty for the CREAM method of Human Reliability Analysis. Reliab Eng Syst Saf 115:100–110

Boecker M (2015) Enhancing the effectiveness and efficiency of control room operators—a roadmap-based approach for selecting interaction technologies for defence and safety-critical organisations and industries. Procedia Manuf 3:769–776

Cacciabue P (2004) Human error risk management for engineering systems: a methodology for design, safety assessment, accident investigation and training. Reliab Eng Syst Saf 83:229–240

Cooper S et al (2000) Technical basis and implementation guidelines for A Technique for Human Error Analysis (ATHEANA) NUREG-1624, Rev 1. U.S. Nuclear Regulatory Commission

Embrey DE (1992) Quantitative and qualitative prediction of human error in safety assessments. Major hazards Onshore and Offshore. IChemE, Rugby

Fujita Y, Hollnagel E (2004) Failures without errors: quantification of context in HRA. Reliab Eng Syst Saf 83:145–151

Geng J, Murè S, Gabriele B, Camuncoli G, Demichela M (2015) Human error probability estimation in ATEX-HMI area classification: from THERP to FUZZY CREAM. Chem Eng Trans 43:1243–1248

He X, Wang Y, Shen Z, Huang X (2008) A simplified CREAM prospective quantification process and its application. Reliab Eng Syst Saf 93:298–306

Hollnagel E (1996) Reliability analysis and operator modelling. Reliab Eng Syst Saf 52:327–337

Hollnagel E (1998) Cognitive reliability and error analysis method (CREAM). Elsevier, Amsterdam

Hollnagel E, Cacciabue P (1991) Cognitive modelling in system simulation. In: Proceedings of third European conference on cognitive science approaches to process control, Cardiff

Isaac A, Shorrock ST, Kirwan B (2002) Human error in European air traffic management: the HERA project. Reliab Eng Syst Saf 75(2):257–272

Kazaras K, Konstandinidou M, Nivolianitou Z, Kirytopoulos K (2013) Enhancing road tunnel risk assessment with a fuzzy system based on the CREAM methodology. Chem Eng Trans 31:349–354

Kim B, Bishu R (1996) On assessing operator response time in human reliability analysis (HRA) using a possibilistic fuzzy regression model. Reliab Eng Syst Saf 52:27–34

Kim M, Seong P, Hollnagel E (2006) A probabilistic approach for determining the control mode in CREAM. Reliab Eng Syst Saf 91:191–199

Klir J, Yuan B (1995) Fuzzy sets & fuzzy logic: theory and applications. Prentice Hall, Upper Saddle River, NJ

Konstandinidou M, Nivolianitou Z, Kiranoudis C, Markatos N (2006) A fuzzy modeling application of CREAM methodology for human reliability analysis. Reliab Eng Syst Saf 91:706–716

Konstandinidou M, Nivolianitou Z, Kiranoudis C, Markatos N (2008) Evaluation of significant transitions in the influencing factors of human reliability. Proc Inst Mech Eng O J Risk Reliab 222(1):39–45

Konstandinidou M, Nivolianitou Z, Simos G, Kiranoudis C, Markatos N (2009) Operators' response time estimation for a critical task using the fuzzy logic theory. In: Proceedings of the joint ESREL and SRA-Europe conference on safety, reliability and risk analysis: theory, methods and applications, vol 1, pp 281–290

Kontogiannis T (1997) A framework for the analysis of cognitive reliability in complex systems: a recovery centred approach. Reliab Eng Syst Saf 58:233–248

Lee SM, Ha JS, Seong PH (2011) CREAM-based communication error analysis method (CEAM) for nuclear power plant operators' communication. J Loss Prev Process Ind 2:90–97

Li PC, Chen GH, Dai LC, Li Z (2010) Fuzzy logic-based approach for identifying the risk importance of human error. Saf Sci 48(7):902–913

Liao PC, Luo X, Wan T, Su W (2016) The mechanism of how design failures cause unsafe behavior: the cognitive reliability and error analysis method (CREAM). Procedia Eng 145:715–722

Mamdani E (1974) Application of fuzzy Algorithms for simple dynamic plants. Proc IEE 121 (12):1585–1588

Mamdani E, Assilian S (1975) An experiment in linguistic synthesis with a fuzzy logic controller. Int J Man Mach Stud 7(1):1–13

Mandal S, Singh K, Behera RK, Sahu SK, Raj N, Maiti J (2015) Human error identification and risk prioritization in overhead crane operations using HTA, SHERPA and fuzzy VIKOR method. Expert Syst Appl 42(20):7195–7206

Marseguerra M, Zio E, Librizzi M (2006) Quantitative developments in the cognitive reliability and error analysis method (CREAM) for the assessment of human performance. Ann Nucl Energy 33:894–910

Monferini A, Konstandinidou M, Nivolianitou Z, Weber S, Kontogiannis T, Kafka P, Kay AM, Leva MC, Demichela M (2013) A compound methodology to assess the impact of human and organizational factors impact on the risk level of hazardous industrial plants. Reliab Eng Syst Saf 119:280–289

Onisawa T (1996) Subjective analysis of system reliability and its analyser. Fuzzy Sets Syst 83:249–269
Park J, Kim Y, Kim JH, Jung W, Seung Jang C (2015) Estimating the response times of human operators working in the main control room of nuclear power plants based on the context of a seismic event—a case study. Ann Nucl Energy 85:36–46
Pedrycz W (1993) Fuzzy control and fuzzy systems. Second extended edition. Research Studies Press, London
Rachid B, Hafaifa A, Hadroug N, Boumehraz M (2016) Reliability evaluation based on a fuzzy expert system: centrifugal pump application. Stud Inf Control 25(2):181–188
Reason J (1990) The contribution of latent human failures to the breakdown of complex systems. Human factors in hazardous situations. Oxford Clarendon Press, Oxford
Saidi E, Anvaripour B, Jaderi F, Nabhani N (2014) Fuzzy risk modeling of process operations in the oil and gas refineries. J Loss Prev Process Ind 30(1):63–73
Sun Z, Li Z, Gong E, Xie H (2012) Estimating human error probability using a modified CREAM. Reliab Eng Syst Saf 100:28–32
Swain A, Guttmann H (1983) Handbook on human reliability analysis with emphasis on nuclear power plant application. NUREG/CR-1278. US Nuclear Regulatory Commission
Ung S-T, Shen W-M (2011) A novel human error probability assessment using Fuzzy modeling. Risk Anal 31(5):745–757
Verma M, Kumar A, Singh Y (2012) Fuzzy fault tree approach for analysing the fuzzy reliability of a gas power plant. Int J Reliab Saf 6(4):254–271
Vigier HP, Scherger V, Terceño A (2017) An application of OWA operators in fuzzy business diagnosis. Appl Soft Comput 54:440–448
Wang A, Luo Y, Tu G, Liu P (2011) Quantitative evaluation of human-reliability based on fuzzy-clonal selection. IEEE Trans Reliab 60(3):517–527
Wu B, Yan X, Wang Y, Soares CG (2017) An evidential reasoning-based CREAM to human reliability analysis in maritime accident process. Risk Anal. doi:10.1111/risa.12757
Yang ZL, Bonsall S, Wall A, Wang J, Usman M (2013) A modified CREAM to human reliability quantification in marine engineering. Ocean Eng 58:293–303
Zadeh L (1965) Fuzzy sets. Inf Control 8:338–353
Zadeh L (1973) Outline of a new approach to the analysis of complex systems and decision processes. IEEE Trans Syst Man Cybern 3:28–44

Zoe Nivolianitou works as a senior researcher in the National Centre for Scientific Research (NCSR) "DEMOKRITOS". She is a chartered Chemical engineer, with further consolidated knowledge on the Risk and Safety Analysis of Chemical Plants. This comprises both the assessment and management of risks from technological systems together with the simulation of natural phenomena that result from an accident. She has an over 30 year experience in the area of industrial safety (mainly chemical plants) acquired at the JRC-ISPRA, (grantee of the European Commission 1983–1987, Ph.D. and Diploma in Chemical Engineering from the National Technical University in Athens, Greece) and in NCSR "Demokritos" in Greece in Risk Analysis, Safety Auditing in the process Industry, Decision Making in Land Use Planning around chemical sites, and in Decision Support and Environmental Impact Analysis. She has been among the principal investigators in many EU funded R&D projects and has participated in several international bodies (like NATO and EU) offering expertise in the above areas. She has published more than 80 scientific publications and technical reports and has co-authored two books. Her current research activities are related to Accident Analysis and the estimation of Human Factor as a key contributor to the occurrence of major accidents together with Emergency planning in Natural Hazards.

Myrto Konstantinidou is a Research Functional Scientist at the National Center for Scientific Research "Demokritos" in Greece. She is a Chemical Engineer with a double degree from the

National Technical University of Athens (NTUA) and the Politecnico di Milano. She holds a Ph.D. on Industrial Accidents and a M.Sc. on Computational Engineering. She has more than 15 years' experience in Quantified Risk Assessment of industrial installations and Accident analysis acquired at "Demokritos" and the Joint Research Center of the European Commission at Ispra. Her research focusses on the causes of Industrial Accidents in the chemical industry and especially in the Oil and Gas sector (including offshore), the integration of Human Factors in risk assessment, safety management and investigation of industrial accidents, and the development of tools to estimate human error probabilities based on human cognition methodologies. She has participated in many research projects on Industrial Safety and Human Factors and has also collaborated with numerous other research institutes, chemical industries, and regulatory authorities (on SEVESO, Offshore safety and environmental directives), in Greece and abroad. She has over 50 publications in scientific journals and conference proceedings, and has co-authored more than 120 technical reports in relevant fields of her research.

Prevention of Human Factors and Reliability Analysis in Operating of Sipping Device on IPR-R1 TRIGA Reactor, a Study Case

Maritza Rodriguez Gual, Rogerio Rival Rodrigues, Vagner de Oliveira, and Claudio Lopes Cunha

Abstract The new sipping device constructed at *Centro de Desenvolvimento da Tecnologia Nuclear*—CDTN (Nuclear Technology Development Center—CDTN), Belo Horizonte, Brazil will be used to inspect irradiated fuel elements cladding in the IPR-R1 TRIGA reactor. The sipping test method is important to check the integrity of the irradiated fuel elements cladding of this reactor, which may be affected by corrosion over long periods of time. The sipping test identifies failed fuel elements by measuring Cs-137 radioactive metal ion activity in the surrounding water, collected via the sipping device. This chapter describes the application of the "what if" technique for assessing risk and reliability in sipping test operations, including an analysis to identify human error and equipment failure modes. Results show initiating events, consequences, and recommended safeguards. In addition, measures to reduce human error are also provided. Human error has been identified as the primary cause or contributing factor in failure modes.

Keywords Component failure modes • Risk assessment • Sipping test • IPR-R1 TRIGA reactor • "What if" technique

1 Introduction

Cladding failures have historically been the primary cause for classifying a fuel element as failed. These failures are usually detected via radioactive fission product into the reactor pool. Sipping is the most common technique used to locate fuel cladding failures in both Pressurized Water Reactors (PWRs) and Boiling Water Reactors (BWRs), but is also used in CANDU reactor (Park et al. 2014), WWER (Slugeň et al. 2007) and research reactors (Perrotta et al. 1998; Castañeda et al. 2003; Borio et al. 2004; Jafari et al. 2015; Dyah and Suryantoro 2015).

M.R. Gual (✉) • R.R. Rodrigues • V. de Oliveira • C.L. Cunha
Centro de Desenvolvimento da Tecnologia Nuclear (CDTN/CNEN), Belo Horizonte, Brazil
e-mail: maritzargual@gmail.com; mrg@cdtn.br; rrr@cdtn.br; vagner.oliveira@cdtn.br; ccl@cdtn.br

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_6

Different sipping methods can be applied (e.g. in-core sipping, telescope sipping, canister sipping) in the reactor vessel, in the spent fuel pool or during removal from the core with the refueling machine. There are several countries (Slovakia, India, Czech Republic, The Netherlands and Hungary) where the power reactors have never been shutdown before the planned outage due to leaking fuel rods. Premature shutdown due to leaking rods was decided in several countries (USA, Japan, France, Belgium, Finland, Sweden and Switzerland) (NEA/CSNI/R 2014).

One of the requirements on radiation safety and operation of a research reactor is the absence of radionuclide release from fission products to the environment. Sipping test is one of non-destructive testing techniques for detection of the failed fuel element by detection and identification the presence of fission products in the water such as Cs-137 and others usually by means of gamma-ray spectrometry (Terremoto et al. 2000). The most suitable fission product for use as failure monitor is Cs-137, due to its long half-life (30.14 years), great fission yields and high solubility in water.

The sipping technology used for inspecting defective fuel is largely divided into vacuum sipping, dry sipping, wet sipping, or in-mast sipping, depending on physical phenomena and the state of the fission products to be detected.

The *Centro de Desenvolvimento da Tecnologia Nuclear*—CDTN, Belo Horizonte, Brazil, constructed a new sipping device that will be used for locating defective nuclear fuel elements in the IPR-R1 TRIGA reactor. In the other paper (Gual et al. 2016) are described each part of the system in detail. Also, is presented the major design parameters of the sipping device and was demonstrated that the manual handling of the device by the workers is secure from dosimetry assessment.

Qualitative methods for assessing risk and reliability have proved to be a useful analytical tool in support of decision-making processes. The "What if " analysis is one of many techniques developed to identify hazards in chemical process plants (Doerr 1991) and can be applied to a range of other areas, including engineering, emergency preparedness and biosecurity. This technique is widely used during the design stages of process development, as well as in facility, equipment or system operating procedures and organizations generally. In the 1990s, experts of the International Commission on Radiation Protection (ICRP), focused special attention on the unexpected—namely, the analysis of "What if?" situations that theoretically could expose people to potentially dangerous sources of radiation (IAEA Bulletin 41/3/1999).

The qualitative "What if" technique (WIFT) (Alverbro et al. 2010) will be used to identify risk sources, through a structured brainstorming method. WIFT may be used simply to identify hazards for subsequent quantitative evaluation, or alternatively to provide a qualitative evaluation of the hazards and to recommend further safeguards where appropriate. WIFT can be used on a stand-alone basis, or as an alternative approach for quantitative techniques, which could be a more effective method even than FMEA/FMECA (Gual et al. 2014; Perdomo and Salomon 2016), when there is lack of reliable data to characterize the events with respect to their occurrence frequency, and severity and detectability degrees.

What-if analysis is applied to every type of analysis and especially to those dominated by relatively simple failure scenarios. Occasionally, it can be used alone, but most often is used to supplement other more structured techniques and, in particular checklist analysis (ABS Guidance Notes on Risk Assessment 2000).

The objective of this work is to apply the "What if" technique to the risk evaluation in the operation of the sipping test device constructed for IPR-R1 TRIGA reactor in CDTN and to identify possible failures/errors.

Human factors are of interest because the operation of sipping device is performed manually by reactor operators. The impact and importance of human errors need to be addressed to prevent the different failure modes.

The importance of this work is to identify the causes of adverse events, rather than provide means on how they can best be avoided.

2 Methodology

The "What-if" technique does not require special quantitative methods or extensive preplanning; however, consultation with experienced and knowledgeable specialists is required.

The methodology behind a "What if" analysis (Doerr 1991) is a speculative process whereby questions in the form "What if. . .." are formulated and reviewed. The method has the following basic features:

- Scope definitions,
- team selection,
- review of documentation,
- question formulation,
- response evaluation with consequences, and
- Summary tabulation to the set of questions.

3 Approach

Select system, subsystem or process.

Pre-planned 'What if' questions are identified through:

- Task analysis
- Basis of Design
- Generic Checklists
- Process Description
- Standards, regulations and guidelines, and
- Past incidents and accidents

The main features marking a thorough analysis are summarized as follows:

Multi-disciplinary team (design, operation and maintenance) should answer 'What if' questions.

Should be a systematic study of:

- operator job descriptions,
- process flow diagram,
- other design documents for the facility,
- Operations and maintenance procedures, and
- Operational Safety Standards and control

Easy to use

No specialized technique needed

People with little hazard analysis experience can participate meaningfully

Leads to a deeper insight, especially for person/people conducting the analysis

Tabular summary of results

The analysis of results must be presented in a table and may include:

- What-if questions (that express cause of possible problems and consequences),
- Estimations of probabilities,
- Description of corresponding consequence, and
- Recommendations actions.

Sipping tests procedure in brief:

1. Clean the tank and the basket before starting the test in the outer reactor room with demineralized water and with the high pressure pump.
2. Support the sipping tank with the level setup. Basket water level adjustment is done manually with screws. The tank is placed in a manner that the 'water thief' position ends up above the reactor pool's water level; therefore, avoiding contact between the water from the reactor and test water. This last operation is carried out with visual monitoring.
3. Tie-in basket and the tank together using ropes. The bridge crane is used to keep the ropes during the sipping test. The sipping tank has a flange with two eyebolts for tying. The basket is comprised of the fuel rack with a stem that has an eyebolt on its upper end for tying.
4. Fill and sink the sipping tank with demineralized water using the high-pressure pump.
5. Transfer the fuel elements (FEs) from reactor core and place them into the basket of the sipping tank using the articulated clamp.
6. Each basket receives only three FEs at a time. The sipping tank is positioned between the reactor core and reactor vessel.
7. Raise the sipping tank with the bridge crane.
8. Collect background (control) water samples from the reactor pool using peristaltic pump.
9. Collect water samples from the sipping tank using the peristaltic pump. The samples are put into a Marinelli recipient to determine the presence of Cs-137.

This process will be repeated several times until all the FEs have been tested. After these operations, any FE identified as defective will be replaced. In the subsequent operation any fuel element causing leakage will be removed from the reactor core.

During the sipping test are employing two types of gamma detectors (thermoluminescent dosimeter (TLD) and tele-detector) to increase the reliability of the gamma dose measurements that the reactor operator will be submitted at the time of device manipulation when sipping test is being performed in the reactor pool.

More specific details are provided in Rodrigues (2016).

As noted herein, the sipping test procedure involves multiple steps requiring human action.

The features of the newly constructed sipping device for the CDTN may be summarized as follows (Rodrigues 2016):

1. It is an original design.
2. It is a mechanical actionizing system (bridge crane, cable and hook).
3. Easy maneuverability and simplicity of design and operations.
4. Simple equipment.
5. Low maintenance cost. The main components are replaceable in a relatively short time (pumps, device for sample collection, flexible tube, etc.).
6. Manual controlling.
7. Short set-up time: Only one 8-h shift.
8. Test up to three fuel elements per half hour, depending on fuel movement time.
9. Low costs.
10. Lower radiation.
11. Limited space requirement.
12. The test performs in the reactor pool.
13. Ease of training.
14. Low probability of equipment activation.
15. High sense of correctness in testing, data collection and measurement.

The sipping test has no implication on the radiobiological protection of personnel, since all operations are performed with the reactor shutdown and the experiment is conducted underwater in the reactor pool, maintaining a secure distance from the top surface of the reactor pool for dosimetry assessment (Gual et al. 2016).

Considerations for the analysis:

1. It is assumed that the test is started according to the planning, only if all the necessary conditions for execution are present (reactor is shutdown, reactor pool is full of water, recipient required for water colleting, pressure pump, peristaltic pump, bridge crane and articulated clamping tool in full functional capacity, radiation detector ready, presence of necessary personnel and storage pool available).
2. It is assumed that the articulated clamp for loading and unloading operations of the FE constructed and patented by CDTN (Costa et al. 2011) is always keeping the FE secured.

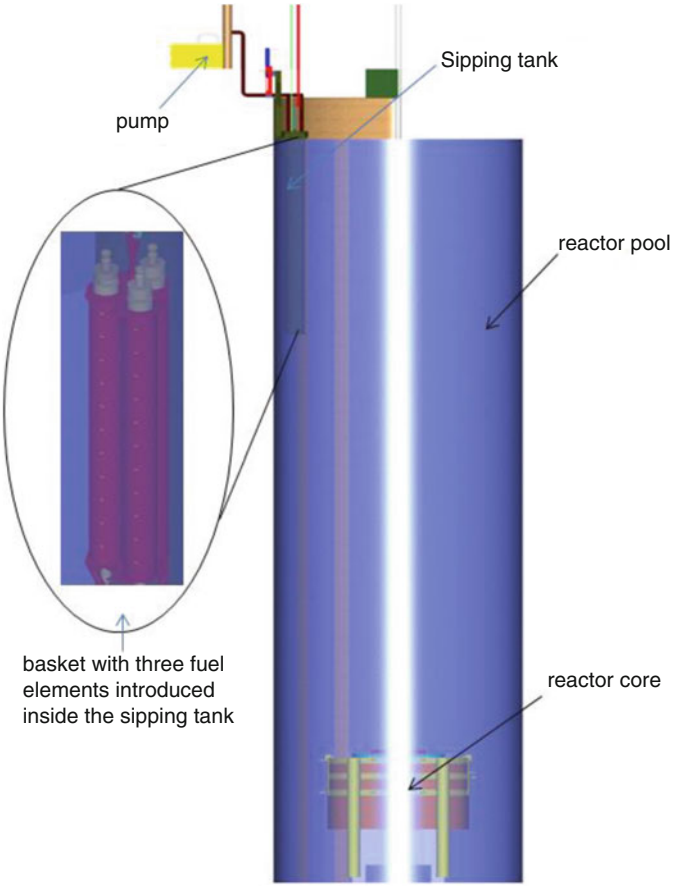


Fig. 1 Schematic representation of the sipping device under IPR-R1 TRIGA reactor pool

3. In accordance with the previous consideration, the following is excluded from the model: the failures for waiting related to the period between successive tests. For example: failure to start of the pressure and peristaltic pumps, rupture of the sipping tank by impact or bad manipulation, rupture of lines by deterioration of materials.
4. Only are included in the analysis: components and/or functions of the sipping test-related system that directly affect the performance of the analyzed function.

Figures 1, 2 and 3 show the schematic representation of the sipping device constructed at CDTN.

The sipping testing device shown in Fig. 3 includes a basket with three fuel elements introduced inside the sipping tank.

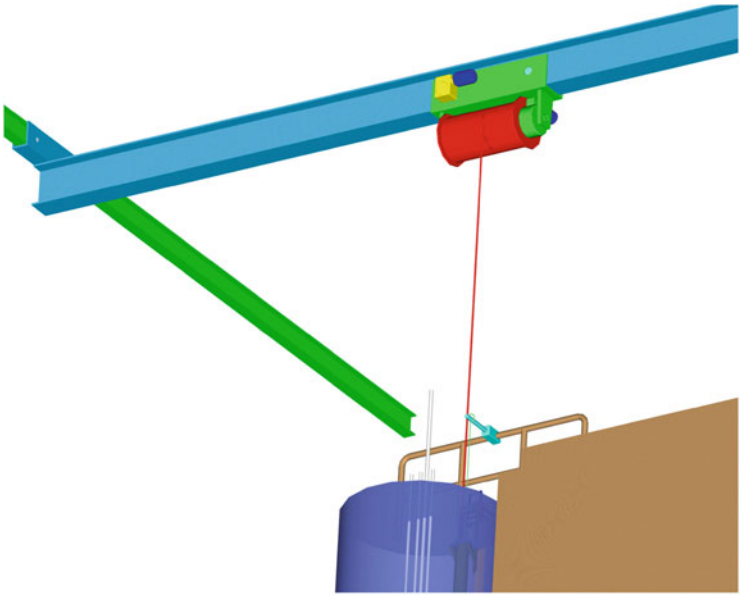


Fig. 2 Schematic representation of the bridge crane used in the sipping test

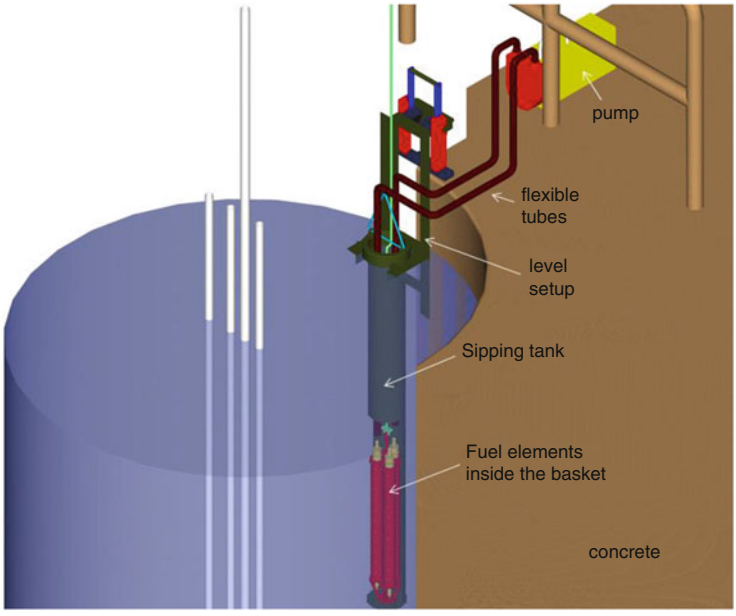


Fig. 3 Schematic representation of the basket with three fuel elements introduced inside the sipping tank

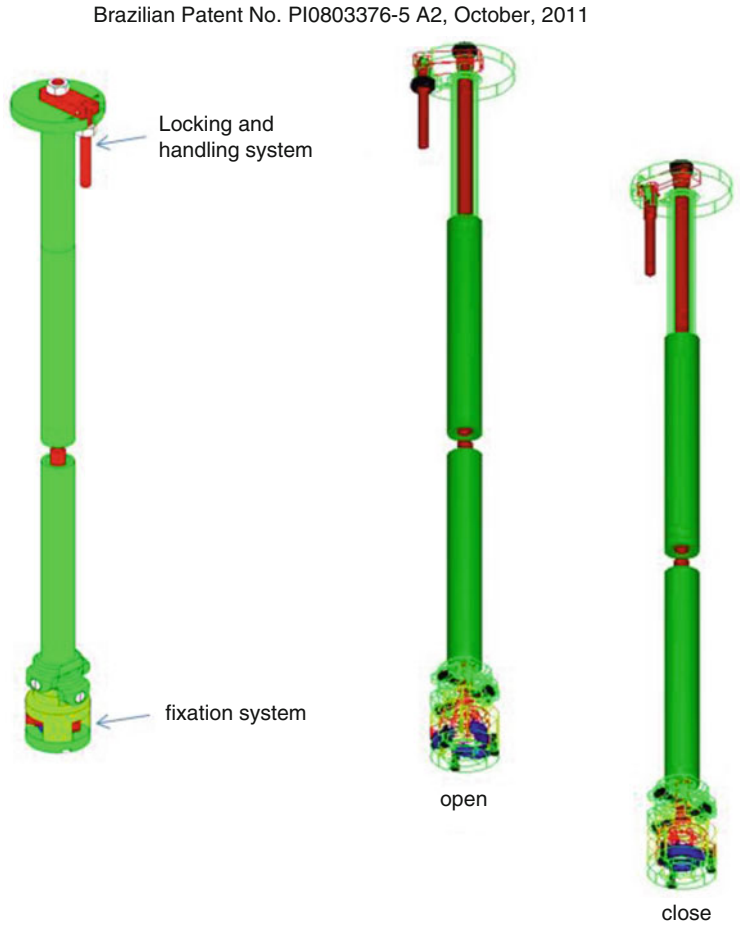


Fig. 4 Schematic representation of the articulated clamp for remote handling constructed and patented by CDTN, in open and close position for FE loading and unloading

The sipping device includes the following active components: peristaltic pump, high pressure pump, and bridge crane. It also contains other passive components, such as nylon ropes, pulleys, hooks, tanks and basket.

The articulated clamp for handling devices and equipment at a distance constructed and patented by CDTN is very safe. This clamp comprises a system for fixation and another for locking that maintaining the desired stiffness. It is remotely operated for operator safety. The loading and unloading operations are performed by top end plugging of the fuel elements (See Fig. 4).

The Process Flow Diagram of the sipping testing device constructed at CDTN for IPR-R1 TRIGA reactor is illustrated in Fig. 5.

The WIFT results are displayed in Table 2 below and may include descriptions of event, causes, probabilities and consequences and recommended actions. This

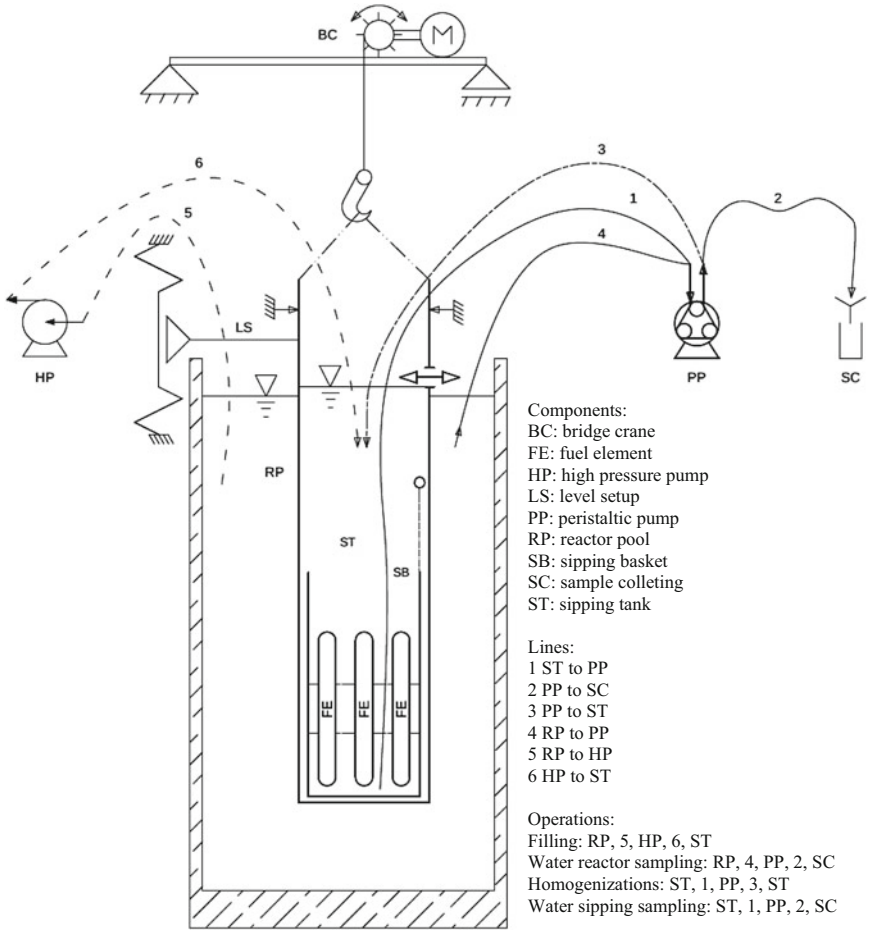


Fig. 5 Process Flow Diagram of the sipping testing device constructed at CDTN for locating defective fuel on IPR-R1 TRIGA reactor

risk and reliability assessment is presented as a qualitative method and not for determining the likelihood of data. It only estimates potential risk. The level of risk of each event is qualitatively assessed a review of its probability occurring and the severity of its consequences.

In the study case the qualitative risks assessment are organized by two criteria:

1. by degree of consequences

- Very serious—undesirable and requires immediate corrective action as soon as possible;
- Serious—undesirable and requires corrective action and requires a plan for incorporating them into current procedure;
- Medium—acceptable with review by senior reactor operator;
- Minor—acceptable without review by senior reactor operator;

Table 1 Key staff functions in sipping test

Tasks	Key staff
Cleaning the tank	Reactor operator
Basket lift	Reactor operator
Submerging the tank under water	Reactor operator
Loading and unloading the fuel element	Reactor operator
Colleting of water samples	Reactor operator/Research manager
Monitoring of radiation doses	Radiation protection supervisor/Reactor operator ad hoc Radiation protection supervisor

2. by degree of probability

- Probable—possibility of isolated incidents;
- Possible—possibility of occurring sometime;
- Remote—not likely to occur;
- Improbable—practically impossible.

Table 1 provides a list of the tasks and key staff members from various disciplines involved in the sipping test.

4 Results

The types of events that can occur when are conducting the sipping test are provided in Table 2, which shows the results of a "what if" analysis that was performed.

An analysis of the outcome revealed two initiating events that might cause accidental radiation exposure. These two events (FE positioning occurs outside water level and imprecise or wrong recording of radiation dose rate) would have consequences for occupationally exposed individuals (OEIs) and, are the result of human error. Among the causes of events that could occur during the sipping test, around 56% are related to human factors, while the rest of them are due to materials or equipment problems.

The likelihood of above-mentioned events is low and this, corroborates the system robustness and reliability.

Consideration of failure of material or components may results in decisions for testing before starting the experiment or having redundant equipment.

The nuclear reactor is within a radiologically controlled area and therefore, the reactor operators are considered as occupationally exposed individuals.

This sipping test would be done by periodically monitoring (every year) the condition of each fuel element, identifying defects of fuel elements claddings.

Table 2 Application of "What if" analysis to sipping test

What if?	Answer	Probability	Consequences	Recommend actions
1. Sipping tank not being cleaned properly	Possible impurities activation and water reactor contamination	Remote	Minor	Train personnel to ensure cleanliness
2. Sipping tank not sunk to bottom of reactor pool	More effort to positioning the basket for loading and unloading the fuel element (FE)	Remote	Minor	Train personnel
3. Basket dropped due to tie rope malfunction	Minimal impact	Remote	Minor	Train personnel
4. When submerging basket in sipping tank, it falls into the nuclear reactor core	Damage to the bottom of the basket and/or top end plugging's FE due to hitting	Remote	Serious	Train personnel
5. FEs not properly introduced into basket and drop into reactor core	Will not cause damage to the reactor core, but may cause damage to the FE cladding. FE can be recaptured again	Remote	Minor	Train personnel
6. FE positioning occurs outside water level	IOE receives a radiation dose level above the safety limit	Remote	Very Serious	Stop test and return the FEs to their initial positions in the reactor core
7. High pressure pump not operating	Disabled test	Possible	Serious	Test pump before start of experiment Incorporate or consider redundant equipment
8. Peristaltic pump not operating	Disabled test	Possible	Serious	Test pump before start of experiment Incorporate or consider redundant equipment
9. FE transport tool (articulated clamp) fails	Disabled test	Improbable	Serious	Test before start of experiment
10. Sipping tank water intake is below water level of the reactor pool	Water from the reactor pool mixes with water of sipping test	Improbable	Minor	Train personnel

(continued)

Table 2 (continued)

What if?	Answer	Probability	Consequences	Recommend actions
11. Overflow of collected water from the reactor and/or sipping test	Loss of cooling water quality control or leakage of Fission Products (PF) in case of failure FE	Possible	Medium	Train personnel Perform decontamination
12. Imprecise or wrong recording of radiation dose rate	IOE receives incorrect dose (too high or too low)	Possible	Serious	Test and calibrate before start of experiment
13. Flexible tube fails	Water leakage from reactor pool or sipping tank	Improbable	Minor	Test before start of experiment Incorporate or consider redundant equipment
14. Nylon rope breaks	Equipment or components fall into reactor pool	Improbable	Medium	Test before start of experiment Incorporate or consider redundant equipment
15. Failure of bridge crane	Interrupting an experiments	Improbable	Minor	Test before start of experiment
16. Marinelli recipient breaks	Leakage of the water sample	Improbable	Minor	Incorporate or consider redundant equipment Perform cleaning
17. Inadequate level setup	Device drops into reactor pool and damage the FE top end plugging's due to hitting	Remote	Serious	Ensure proper assembly Test before start of experiment
18. Replaced FEs back out of their original position in the reactor core after test	Possibility of change in reactivity of reactor core and flux distribution variation in the reactor core	Remote	Serious	Train personnel verify that FEs are replaced back to their original position

The list of sipping test operational events depends on sipping technology used and nuclear reactor type.

Measures to reduce human error that can cause undesired events:

1. The staff should be well trained. It plays an important role in accident scenarios.
2. Perform calibration of gamma radiation detector before starting experiment.
3. Implementation of quality assurance procedures that cover the sipping test process.
4. Check the effectiveness of verification procedures.
5. Evaluation of gamma irradiation dose at the top surface of the reactor pool where the experiments will be conducted by means of Monte Carlo calculations to

ensure that the total cumulative dose will not exceed the limit established by the standards for OEIs in the controlled area, namely 6 mSv/year (CNEN 2011).
6. Communication among staff members (reactor operator, radiological protection supervisor, experts, etc.).

Understanding these human factors is important in the prevention of component failure modes for the reliable and safe operation of the sipping device. This risk evaluation method (qualitative) can be applied in auditing of safety and quality control procedures of sipping test device operation. This study was a requirement of the Committee for Safety Analysis (CAS) of the CDTN to authorize the sipping test to proceed.

The study has identified the possible events, their causes, consequences, safeguards and recommendations to diminish the potential risk by means of the "What if" technique.

The sipping device is a very simple system and therefore, it lacks redundant components and functions. Human errors were the predominant cause triggering the different failure modes, since both, passive and active components have a very low failure frequency.

As a recommendation, a quantitative/semi-quantitative analysis of the system will be performed, specifically a FMECA and a Human Reliability Analysis (HRA).

5 Conclusions

Nuclear reactor requires a method for inspecting fuel elements to verify integrity in service. Fuel element are surrounded by water moderator, causing large variations their cladding due to water-dissolved impurities. These dissolved impurities influence the water radiolysis processes and corrosion process, resulting in galvanic cells formation on a rather long term. Fuel element are also is subjected to intense high temperature, gamma radiation and neutron fluxes that can damage the fuel cladding and cause a radioactive release. The neutron can induce activations in the stainless steel fuel elements cladding and may negatively affect its physical-chemical resistance.

For this reason a providing method to verifying the integrity of these irradiated fuel elements is necessary. The non-destructive testing method, which less exposes the human factor to the fatal radiation doses from the irradiated fuel element for decades has been determined to be the sipping test method in the current state of the art.

The sipping device acts in a way that uses intensely the human labor force. The operations of preparation, the loading and unloading of the sipping device are done manually by the nuclear reactor operator. These operations are based on the human factors, which are more subject to errors associated with handling of the sipping test device. In this way a risk analysis becomes essential to evaluate the situation in which sipping test operation will be subject.

After a comparison of the risk and benefit of using the sipping test method and having addressed all potential risks identified during the "What-if" analysis, it can be affirmed that the sipping test can potentially benefit and ensure the safe operation of nuclear reactor while at the same time it remains a simple humans-managed method.

Although the sipping test did not present a significant radiological hazard on human health and the environment, the risk sources have been identified and assessed. Human error has been cited as a primary cause or contributing factor of failure modes in sipping device operation. There have been determined the dominant failure causes of sipping test operation, which support the decision making, based on the prevention actions. The risk assessment reported here is important for safe sipping test operation of either research reactors or power reactors.

To date, there are no reported incidents related to sipping tests and as a results, there are no tabulated error probabilities on these tests. This is one of the reasons for our study in a qualitative mode. The fact that this is a relatively simple system does not imply that an accident is completely unavoidable. After an analysis of this work, evidence suggests that accidents will most likely be triggered by human error. The latter can be avoided by knowing their causes.

The 'What-if' analysis has generated qualitative descriptions of potential problems in sipping tests. Assessing the 'what-if' scenarios and consequences will be of importance for all aspects of sipping tests and decision management.

In this study, humans errors remain the most probable cause of accident. Theses can be avoived through the identification of their possible causes as already listed herein.

It is recommended that this qualitative risk assessment analysis is implemented by reactor operators, including ad-hoc operators, regulatory managers, radiation protection supervisors and other safety personnel and/or professionals in order to mitigate risks arising from sipping tests.

Acknowledgments This study was supported and funded by the following organizations: Nuclear Technology Development Center, Brazilian Nuclear Energy Commission (CNEN), Research Support Foundation of the State of Minas Gerais (FAPEMIG), Brazilian Council for Scientific and Technological Development (CNPq), and Coordination for Improvement of Higher Education of Personnel (CAPES).

References

Alverbro K, Nevhage B, Erdeniz R (2010) Methods for risk analysis. Printed in Sweden by US AB, Stockholm. ISSN 1652-5442

Borio di Tigliole A, Cagnazzo M, Lana F, Losi A, Magrotti G, Manera S, Marchetti F, Pappalardo P, Salvini A, Vinciguerra G (2004) Identification of a leaking TRIGA fuel element at the reactor facility of Pavia, Vienna University of Technology, Atomic Institute of the Austrian Universities (Austria), 207 p; pp 53–61, INIS-AT--0076, 2nd World TRIGA users conference; Vienna, Austria, 15–18 Sep 2004

Castañeda JG, Delfín LA, Alvarado PR, Mazón RR, Ortega Velázquez B (2003) Diseño y Construcción del SIPPING para Combustibles del Reactor Triga Mark III, Energía Nuclear y Seguridad Radiológica: Nuevos Retos y Perspectivas XIV Congreso Anual de la SNM/XXI Reunión Anual de la SMSR. Guadalajara, Jalisco, México, 10–13 de Septiembre, CDROM (In Spanish)

CNEN Comissão Nacional de Energia Nuclear (2011) Basic guidelines on radiological protection, CNEN-NN-3.01 regulatory position 3:01/004:2011. Dose constraint, occupational reference levels and area classification, Rio de Janeiro, 2011 (in Portuguese)

Costa ACL, Ribeiro E, da Silva LL (2011) Articulated clamp for handling devices and equipment at a distance. Brazilian Patent No. PI0803376-5 A2, October, 2011

Doerr WW (1991) What-if analysis. In: Greenberg HR, Cramer JJ (eds) Risk assessment and risk management for the chemical process industry. Van Nostrand Reinhold, New York, pp 75–90

Dyah Sulistyani, Suryantoro R (2015) Integrity Test of the SNF Using Sipping Test Method, The 2015 FNCA Workshop on Radiation Safety & Radioactive Waste Management (RS&RWM), 17–19 Nov, Serpong, Indonesia,

Gual MR, Mesquita AZ, Campolina DAM, Rodrigues RR (2016) Dosimetry assessment during the sipping test in the IPR-R1 TRIGA reactor using MCNPX. Prog Nucl Energy 93:238–245. http://dx.doi.org/10.1016/j.pnucene.2016.09.002

Gual MR, Perdomo OM, Salomón J, Wellesley J, Lora A (2014) ASeC software application based on FMEAe in a mechanical samples positioning system on a radial channel for irradiations in a nuclear research reactor with continuous full-power operation. Int J Ecosyst Ecol Sci (IJEES) 4 (1):81–88

Guidance Notes on Risk Assessment Applications for the Marine and Offshore Oil and Gas Industries. American Bureau of Shipping, ABS Plaza, Jun 2000

IAEA Bulletin. WHAT IF? ICRP guidance on potential radiation exposure, 41/3/1999

Jafari M, Gholizadeh Aghoyeh R, Toumari R, Khalafi H (2015) A sipping test simulator for identifying defective fuels in MTR type nuclear research reactor. Ann Nucl Energy 77:238–245

NEA/CSNI/R (2014) 10 (2014) Leaking fuel impacts and practices, nuclear energy agency. Committee on the Safety of Nuclear Installations, 18 Jul 2014.

Park J-Y, Shim M-S, Lee J-H (2014) Current status of integrity assessment by sipping system of spent fuel bundles irradiated in CANDU reactor. Nucl Eng Technol 46(6). doi:10.5516/NET.09.2014.018

Perdomo OM, Salomón LJ (2016) Expanded failure mode and effects analysis: advanced approach for reliability assessments. Revista Cubana de Ingeniería VII (2):5–14

Perrotta JA, Terremoto LAA, Zeituni CA (1998) Experience on wet storage spent fuel sipping at IEA-R1 Brazilian research reactor. Ann Nucl Energy 25(45):237–258. https://doi.org/10.1016/S0306-4549(97)00039-X

Rodrigues RR (2016) Development and methodology implementation for integrity structural assessment of IPR-R1 TRIGA nuclear reactor fuel element by sipping method. Thesis project (in Portuguese)

Slugeň V, Mikloš M, Božik M, Vašina D (2007) Monitoring and Leak testig of WWER-440 fuel assemblies in Slovak wet interim spent fuel storage facility. Acta Montanistica Slovaca Ročník 12(1):187–191

Terremoto LA, Zeituni CA, Perrotta JA, da Silva JER (2000) Gamma-ray spectroscopy on irradiated MTR fuel elements. Nucl Instrum Methods in Phys Res Sect A 450(2–3):495–514

Maritza Rodriguez Gual is Doctor in Science and Nuclear Technologies from Higher Institute for Technologies and Applied Sciences (InSTEC), Havana/Cuba in 2011, Master of Science in Nuclear Reactor Technologies from Budapest Technical University (BME)/Hungary in 1990. She is graduated from FCTN, Havana University, Cuba as a Nuclear Energetic engineer on July of 1987. Post-doctoral Research Associate in Department of Nuclear Engineering (DEN) at Federal University of Minas Gerais (UFMG) from 2012 to 2014. Currently, work as postdoctoral researcher in Department of Reactor Technology Service (SETRE) at Nuclear Technology Development Centre (CDTN), Belo Horizonte/Brazil. Expertise in radiation particle transport simulation with Monte Carlo codes (MCNPX) applied to Nuclear Reactor Physics, Medical Physics, Radiation Protection and Shielding and Patient-specific dosimetry. Apply risk assessment tools and techniques to nuclear reactors. A complete CV in: http://lattes.cnpq.br/9079020125523928

Rogerio Rival Rodrigues is Master degree in Nuclear Technical Sciences from the School of Engineering at Federal University of Minas Gerais (UFMG)/Brazil in 1996, graduated in Chemical Engineering from Department of Chemical Engineering, School of Engineering/UFMG on November of 1987. He works as Full Technician in Department of Reactor Technology Service (SETRE) at the Nuclear Technology Development Centre (CDTN), Belo Horizonte/Brazil since 1996. He has experience in neutron activation analysis and water chemical control in research nuclear reactor.

Vagner de Oliveira is graduated as Mechanical Engineering from Federal University of Minas Gerais (UFMG)/Brazil on 1994. He works as Mechanical Technician researcher in Department of Reactor Technology Service (SETRE) at Nuclear Technology Development Centre (CDTN), Belo Horizonte/Brazil since 1996. He has experience in Mechanical Engineering, with emphasis on Heat Transfer and product designer.

Claudio Lopes Cunha is graduated as Mechanical Engineering from Pontifícia Universidade Católica (PUC), Minas Gerais/Brazil on December of 1998. He works as Mechanical Technician researcher in Department of Reactor Technology Service (SETRE) at Nuclear Technology Development Centre (CDTN), Belo Horizonte/Brazil since 1995. He has experience in Mechanical Engineering, with emphasis on Machining and Forming Machines, CAD Designer and product designer.

Human Factors Challenges in Disaster Management Scenario

Fabio De Felice, Antonella Petrillo, and Federico Zomparelli

Abstract The present chapter aims to propose a model to manage complexity during a disaster accident caused by human factors and errors. The model allows to evaluate the human error probability under critical conditions and stress conditions. A hybrid model based on Simulator for Human Error Probability Analysis (SHERPA) is proposed and analyzed. A specific area of application is investigated concerning the human behavior during an emergency situations in a petrochemical plant. Furthermore, the chapter proposes an innovative approaches for monitoring the human factors in industrial plant through KPIs indicators. The model is implemented in a real case study concerning a petrochemical company.

Keywords Human factors • emergency management • SHERPA • KPIs • HRA

1 Introduction

In recent decades, most of accidents occurred in industrial plants and critical infrastructures were caused by human errors. A research by ASME has analyzed 23,338 industrial accidents, 83% of them are due to human error (Carayon 2006). MARS database (Major Accident Reporting System) identifies 180 industrial accidents in critical infrastructure in Italy during the period (2005–2010). 47% of these are caused by human error. Human error affects worker safety, but also system performance (Neumann and Village 2012). For this reason, the research on human reliability is growing significantly (Mosleh and Chang 2004). Particular attention is related to the human behaviour analysis during an emergency condition, because a wrong choice could generate dramatic consequences. Human reliability study identifies all factors that influence the environment where operators work (De Felice et al. 2016a). Thus, it would be essential to avoid emergency conditions applying preventive actions. Unfortunately, the considerable complexity of the industrial plants makes it difficult (Turoff et al. 2004). In this context, it is useful

F. De Felice • A. Petrillo • F. Zomparelli (✉)
University of Cassino and Southern Lazio, Cassino, Italy
e-mail: defelice@unicas.it; antonella.petrillo@uniparthenope.it; f.zomparelli@unicas.it

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_7

to develop simulation models in order to analyze several scenarios and human responses. Outputs simulation are a set of key performance indicators (KPIs) that define and monitor the state of system. Through the analysis of these indicators it is possible to change the system to increase the whole human system reliability (De Felice et al. 2016b). The purpose of the study is the human error probability evaluation. The research develops a design plan to improve environmental conditions in order to reduce human error probability. Human error probability evaluation is realized through the development of a hybrid human reliability analysis methodology which considers "internal" human factors and "external" environmental factors. Outputs of the model are analyzed through a set of KPIs indicators to monitor operators' safety conditions in industrial plant. The model is applied in a real petrochemical case study.

The rest of the chapter is organized as follows: in Sect. 2 a brief analysis of literature is presented. Section 3 describes the methodological approach adopted. The case study is developed in Sect. 4, while the last section describes conclusions.

2 Literature Analysis

Emergency conditions in industrial plant arise from external events or internal events. External events are related to environment, while internal events are dependent on system failures and human error (Weber and Thomas 2005). Many studies have been conducted to analyze factors affecting industrial accidents (De Koster et al. 2011). About the 90% of accidents are due to human error in chemical companies (Mendonca et al. 2001). Human error influences the performance of the company. Furthermore, human error develops inefficiencies and long-term costs (Grosse et al. 2015). Human analysis also considers working environment. HRA is born with the same intent of the system analysis (Kim 2001). In recent decades, scientific publications in the field of HRA are growing, as this subject is becoming relevant to process management (Kim and Jung 2003). Considering the importance of the topic, we conducted a research on Scopus database, the largest abstract and citation database of peer-reviewed literature. Search string used in the literature survey was "human reliability analysis". String was defined according to the standards of Scopus database. Only articles in which the string "human reliability analysis" was found in key words were analyzed. The analysis on Scopus pointed out that from 1964 until February, 2017 a set of 41,010 documents have been published divided in 32,913 articles, 2102 conference chapters and the remain part on books, editorials, letters, etc. The result showed that the scientific production on this topic is very wide and covers many scientific areas (engineering, medicine, social science, etc.). Historically, HRA techniques have evolved in three different "generations", each with its own characteristics, advantages and disadvantages (Konstandinidou et al. 2006). First generation of HRA was developed between 1970 and 1990 and it assesses risk with little attention to behavior. Second generation of HRA was developed from 1990 to 2005 and it

Table 1 HRA methodology

Method	Framework	Data
THERP	Behavioral	Curves and tables
HEART	Cognitive	Tables
CREAM	Cognitive	Nominal HEP
SPAR-H	Cognitive	Nominal HEP

focuses on internal and external factors that affect human performance. The last generation is still being studied and implemented only in nuclear power plants, it is used to define dynamic HRA analysis.

Table 1 shows some of the most used HRA methodologies with their characteristics.

It is important to distinguish HRA methods by HRA simulators. Simulators take advantage of model theory, but they are dynamic and quantitative. Some of the most popular HRA simulators are:

- Probabilistic Cognitive Simulator (PROCOS): it is a quantitative model that simulates operator's behavior and it analyzes his mistakes (Trucco and Leva 2007);
- Cognitive Environment Simulation (CES): it is a semi-qualitative simulator for control operator's behavior in a nuclear power plant during an emergency situation (Woods et al. 1987);
- Simulation System for Behavior of an Operating group (SYBORG): it is a qualitative model that simulates a group of workers in a nuclear plant. It shows some possible combinations of operator errors that can lead to sequences of accidents (Kirwan 1998);
- Simulator for Human Error Probability Analysis (SHERPA): it is a quantitative model that evaluates human error probability. It can be used both in a preventive phase and in a retrospective phase (Di Pasquale et al. 2015).

Performance measurement is a fundamental principle of human factors management in order to improve human reliability and to reduce the number of accidents. Thus, it is useful to develop a set of key performance indicators (Lo et al. 2014). The result of model is the human error probability evaluation.

Performance measurement identifies current performance gaps between current and desired performance and it provides an indication of progress toward closing gaps. Selected key performance indicators define how improve the performance of company (Weber and Thomas 2005). KPIs indicators allow to monitor conditions of analyzed process (Del-Rey-Chamorro et al. 2003). They are used in continuous improvement system, "Plan-Do-Check-Act" (Deming and Edwards 1982) to monitor process improvement (Imam et al. 2013).

3 Methodological Approach

Literature analysis shows a long list of human reliability analysis models. Some models analyze human reliability by considering internal factors which influence the operator (eg. type of activity), other models analyze human reliability considering the influence of external environment (eg. stress). Thus, the first criticality is the lack of analysis models that consider internal and external factors in the same analysis. Another criticism is related to the staticity of HRA models. Only HRA simulators and the third-generation of HRA methodologies have dynamic characteristics.

The research proposes a new hybrid approach that analyzes human reliability during an emergency conditions. In particular the model calculates the human error probability, considering both internal and external factors. In addition, the model was born as a simulator, it is very flexible and it allows to evaluate in real time the human error probability, including the possibility of introducing the improvement activities to mitigate the error probability during the analysis.

The methodological approach is characterized by different steps. Figure 1 shows the methodological approach.

Here below is a description of each steps:

Step #1 This step defines causes that generate emergency conditions. It may be due to several reasons: random accidents, system failure, human error, etc.

Step #2 In this step operator's choice is simulated. Operator can make the right choice and he closes emergency or he makes the wrong choice. Wrong choice worsens emergency conditions.

Step #3 The third step evaluates error probability through a hybrid model based on HRA methodology. The model considers internal human factors using Weibull function and it considers external factors, related to the environmental conditions, using performance shaping factors (PSFs).

The development of a hybrid HRA model is the fundamental element of the research. Figure 2 shows a hybrid HRA model chart. The hybrid model incorporates the principles of several HRA models known in the literature, overcoming their limitations. The goal is to create a model that identifies the human error probability, considering internal and external factors which could influence human reliability. The presented model uses a mathematical algorithmic approach based on Weibull's function.

The hybrid HRA model is divided into five different phases:

– Emergency conditions. The developed model aims to calculate the human error probability of operator during emergency conditions. So the first step is to identify and describe the emergency condition at time "t". It is essential to define the emergency condition, as in these cases, human reliability decreases very quickly, and it may arise critical situations;

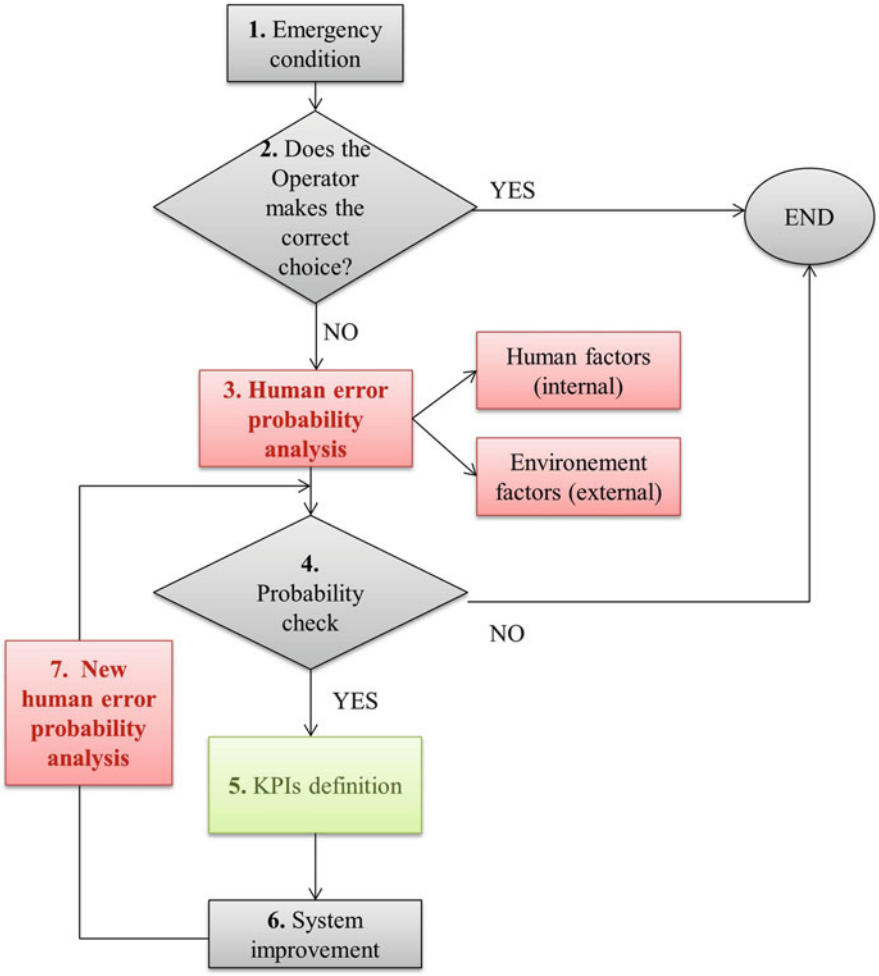


Fig. 1 Methodology approach

– Generic task choice. Generic tasks (GTTs) are standard operations defined by Kirwan (1996) associated with human reliability values. It is necessary to associate each GTTs with the single operator. GTT consists of three values: α, β and k associated with each operation;
– Weibull function. The values reported on each GTT allow to calculate the nominal human error probability, using Weibull distribution, which describes human behavior. Weibull function calculates human error probability, distinguishing between the first hour of work and the other, using the following formula:

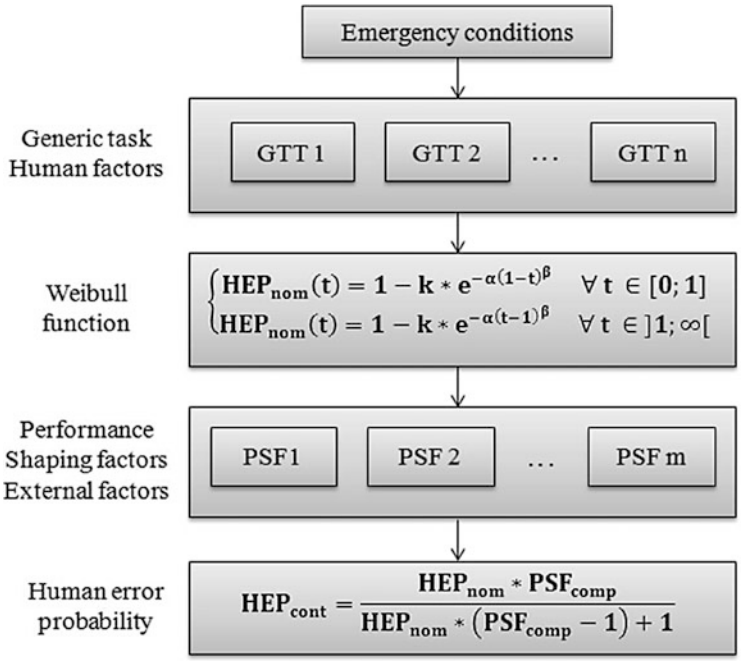


Fig. 2 Human error probability analysis

$$\begin{cases} HEP_{nom}(t) = 1 - k*e^{-\alpha(1-t)^{\beta}} & \forall t \in [0;1] \\ HEP_{nom}(t) = 1 - k*e^{-\alpha(t-1)^{\beta}} & \forall t \in]1;\infty[\end{cases} \quad (1)$$

Where:

- HEPnom: nominal human error probability depends only on human behaviour;
- t: variable which represents the working time;
- k: parameter that represents the reliability of task for each operator. This parameter is descibed in the HEART methodology (Kirwan 1996);
- β: parameter that represents the shape of reliability curve. The shape that best approximates human behaviour is a Weibull function with β=1, 5.
- α: parameter that depends on human reliability (k value). α is calculated as:

$$\alpha = \frac{-\ln[k]}{(t-1)^{\beta}} \quad (2)$$

– Performance shaping factors choice. The calculated nominal human error probability only considers internal factors, it is necessary to introduce the influence of external environmental factors. Performance shaping factors introduce in the

model the external factors influencing human reliability (Gertman et al. 2005). Each PSF assumes a defined value. The product of all PSFs defines the overall environmental value (PSFcomp);

– Human error probability. Finally the real human error probability is calculated, combining nominal error and environment influence (PSFs), with the following equation:

$$HEP_{cont} = \frac{HEP_{nom} * PSF_{comp}}{HEP_{nom} * (PSF_{comp} - 1) + 1} \quad (3)$$

Where:

- HEPcont: contextual human error probability depends on human behaviour and environment;
- HEPnom: nominal human error probability depends only on human behaviour;
- PSFcomp: parameter that describes the environment.

Step 4 In this step, decision maker has to check the error probability value and he has to compare it with an acceptable limit value. This limit varies according to the system conditions. Obviously it is strongly influenced by the possible consequences of human error. If the error probability is too high, it needs to improve the system.

Step 5 In this step a set of KPIs is identified in order to analyze the system. In particular, KPIs are to be related to external factors that influence the human error probability. PSFs represent environmental system conditions. If the influencing factors are measurable, then they can be used as KPIs, otherwise it is necessary to transform them into measurable elements.

Step 6 The sixth step improves system to decrease the human error probability. The control of KPIs is realized by a dashboard that allows to monitor KPIs value.

Step 7 The last step evaluates new human error probability and it verifies improvement.

The model is solved by evaluating the human internal behavior linked to environmental factors that affect the operator.

4 Case Study: Description of an Experimental Scenario

This section presents a model application in a petrochemical company, which regenerates waste oil to obtain lubricant bases. Problems are amplified, because the risk is defined in a confined space. For this reason it is necessary to define a specific model to quantify human errors.

Step 1 The analyzed plant is divided into different areas: deposits of waste oils, refinery department, former production departments, control room, offices and

Fig. 3 System under study (Hydrogen sulfide tank)

services. Storage of waste oils, covers an area of 3300 m^2, which are in turn occupied by tanks, machinery and other small venues for various services. Hazardous substances like: usage oil, sulphide hydrogen, natural gas, oxygen and diesel are used in the chemical plant. An average of 100 workers are present in the plant. In addition, the plant is confined to other industrial plants, supermarkets and fast foods, being in a commercial area. For these reasons, incidental conditions in the plant may have disastrous consequences on workers and the outside environment. Various types of emergency can occur in the chemical plant such as: gas leak, release of liquid hydrocarbons, fire, earthquake, flood, sabotage, pollution, etc.

The proposed research, analyzes an incidental event about the leakage of hydrogen sulfide from a tank for refining waste oils. Figure 3 shows hydrogen sulfide tank.

The event could have disastrous consequences, so decision maker has to to take the appropriate emergency measures. In this case decision maker is represented by team leader. He should activate the emergency protocol that provides:

- wear breathing apparatus;
- reaching the critical area;
- rescue any injured;
- check gas leak entities;
- investigating accident causes and eliminate them;
- end emergency.

Step 2 If human reliability is always high, the decision maker would identify the problem and activate the emergency plan. But in reality, human reliability decreases and this could create mistakes in the choices of the decision maker. It is critical to measure the human error probability, because if this value is high, it is

Table 2 Generic tasks

Generic task	Limitations of unreability	k	α	β
Shift or restore system to a new or original state	0.14–0.42	0.86	0.021	1.5

Table 3 Nominal human error probability

Generic task	HEP_{nom} (t)			
Shift or restore system to a new or original state	t = 1	0.1400	t = 5	0.274
	t = 2	0.1581	t = 6	0.322
	t = 3	0.1902	t = 7	0.370
	t = 4	0.2300	t = 8	0.420

necessary to improve the process to maintain a low level of unreliability. The case study simulates a condition where the operator is unable to identify and eliminate the causes of an accident. The consequences of the operator's unreliability can cause injuries to other operators or people outside, because the accident was not properly managed.

It is crucial to know the human error probability in order to improve human reliability. In the next steps, the human error probability of the decision maker who is found in the emergency condition described in step # 1, has been calculated.

Step 3 Generic task analyzed is shown in Table 2 with its associated reliability values. Generic tasks (GTTs) are the operation performed by the operators, they are defined by scientific literature (Kirwan 1996). Literature defines reliability values for each generic task. Reliability is represented by the three coefficients (k, α and β). In the case study it chooses the GTT that most closely approximates the operations of team leader during the described emergency. During emergency, team leader try to shift or restore system to a new or original state.

Using Eq. (1) it can calculate the nominal human error probability (HEP) by using the Weibull function. HEP is the error probability of the operator considering only internal factors (human reliability defined in the GTT). Table 3 shows the nominal human error probability for considered scenario ($1 < t < 8$).

Table 3 shows an increasing trend of unreliability. These data are in line with reality, because after several hours of work, human reliability decreases because of operator fatigue.

As already introduced, the strength of the model is the capacity to analyze internal and external factors. PSFs introduce the influences of the external environment factors into the model of human reliability. PSFcomp is the product of individual PSF and it identifies the external influence of all the environmental factors considered. Table 4 shows performance shaping factors and PSFcomp. Values in Table 4 are worse, they increase the human error probability.

Equation (3) calculates the real human error probability (HEPcont) which considers internal and external factors which influence human reliability. Figure 4 shows the real human error probability ($1 < t < 8$). It shows an increasing trend of

Table 4 Performance shaping factors

PSFs	
Choice time	1
Experience	3
Procedure	20
$PSF_{comp} = (PSF_1 * PSF_2 * PSF_3)$	60

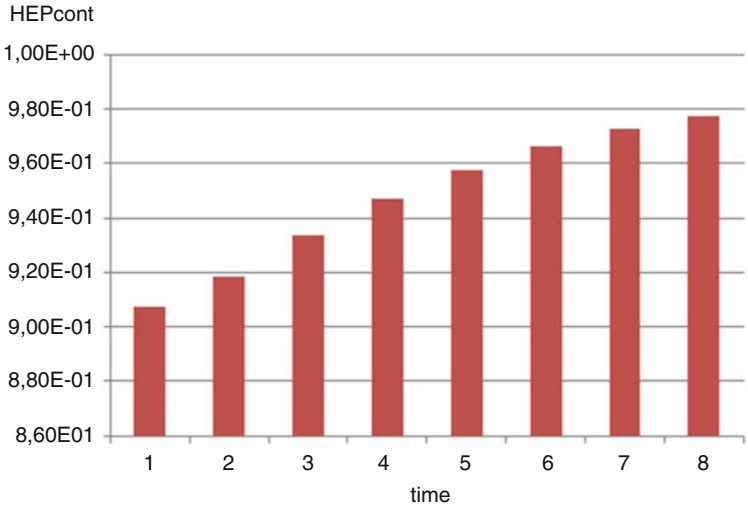


Fig. 4 Human error probability

human error probability. 8 h of work are analyzed. Under the hypothetical conditions previously described, it is evident that the human error probability is too high, so it is necessary to optimize the system.

Step 4 In the case study the limit value of the human error probability must not exceed 0.8. Fig. 4 shows that the limit value is exceeded, then it is necessary to evaluate KPIs indicator to improve the process.

Step 5 KPIs indicators are related to the performance shaping factors and they monitor environmental conditions. Three analysed PSFs are: choice time, experience and procedures. 6 operators working in the control room, are interviewed to identify factors that influence PSFs.

The interview results show that:

- choice time is influenced by non-standardization operations;
- lack of experience is due to the lack of practice during an emergency situation;
- procedures are poorly understood.

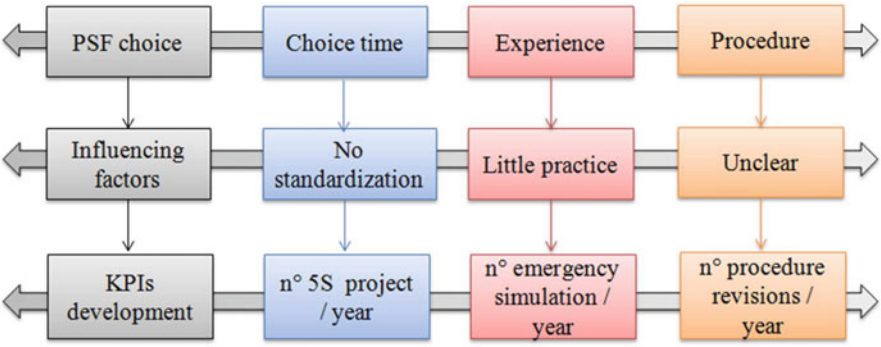


Fig. 5 KPIs development for petrochemical scenario

Table 5 KPIs value

KPIs	
n° 5S project/year	2
n° emergency simulation/year	6
n° procedure revisions/year	2
n° of internal audit/year	12
hours of training course/year	24

The identified factors are not measurable, then it is necessary to identify KPIs indicators representing them. 5s projects allow to reorder the workstation and this affects team leader's reaction rate during the emergency condition. Number of annual accident simulations is an indicator of the operator's experience level. Finally, number of annual reviews measures the difficulty to understand procedures. Figure 5 shows KPIs development for a petrochemical accident scenario.

The choice of KPIs is critical activity for the control of the achievement of the set goals. For the first annual improvement project, the goal is to implement: two 5S project, six emergency simulation, double procedures revision, an internal audit each month and 24 h of training course about the emergency procedures and safety. Table 5 shows KPIs values defined by the manager. According to continuous improvement theory, during the following years, it will be necessary to identify new KPIs to monitor more rigidly the system and to eliminate any critical issues.

Step 6 Figure 4 highlights a high error probability value. It is necessary to develop improvement programs to decrease PSFs value. The improvement process is evaluated by KPIs value.

The optimization process expected to make 12 emergency simulation every year. Emergency simulations must be random. It is necessary to review the working procedures six times a year to simplify them. Human reliability analysis shows high error probability values. Observing the values of performance shaping factors, it is

5s SAFETY AUDIT CHECKLIST - General

Mark "X" on rating column
Rate "1" = Not Acceptable
Rate "3" = Acceptable but opportunity to improve
Rate "5" = Very good

	Rate			
	N/A	1	3	5
PERSONAL PROTECTIVE EQUIPMENT				
1 Eye protection		x		
2 Hearing protection		x		
3 Face shields		x		
4 Protective clothing availability/condition			x	
5 Safety shoes, glasses, gloves				x
6 Respirators accessibility & serviceability				x
7 Safety Installations (deluge showers , eye wash stations)		x		
FIRE PROTECTION				
13 Fire equipment - serviceability				x
14 Fire equipment - adequacy				x
15 Fire equipment - accessibility				x
16 Storage of flammable materials	x			
17 Operation of fire escape facilities				x
18 Accessibility & adequacy of fire escapes				x
19 Employees aware of correct use of equipment		x		
20 Fire Warning/No smoking signs				x
21 Emergency drills - practice				x
Sub total	5	1	0	35
FIRE PROTECTION TOTAL	90.0%			

Fig. 6 5S project

evident as the complexity of the procedures negatively affects human reliability. System optimization needs to identify a model to minimize this criticality. The fundamental problem of the procedures is the lack of standardized operations. The most effective tool for standardizing processes and limiting human error is the 5S model that limits human error probability developing a clean, safety, and standardized workstation (Jiménez et al., 2015). Every year, five projects of 5s (Fig. 6) should be developed to improve working conditions.

The concept of 5s project to improve working conditions provides:

- Seiri. Identify waste;
- Seiton. Reorder workstation;
- Seiso. Clean workstation;
- Seiketsu. Standardize processes;
- Shitsuke. Continuous improvement.

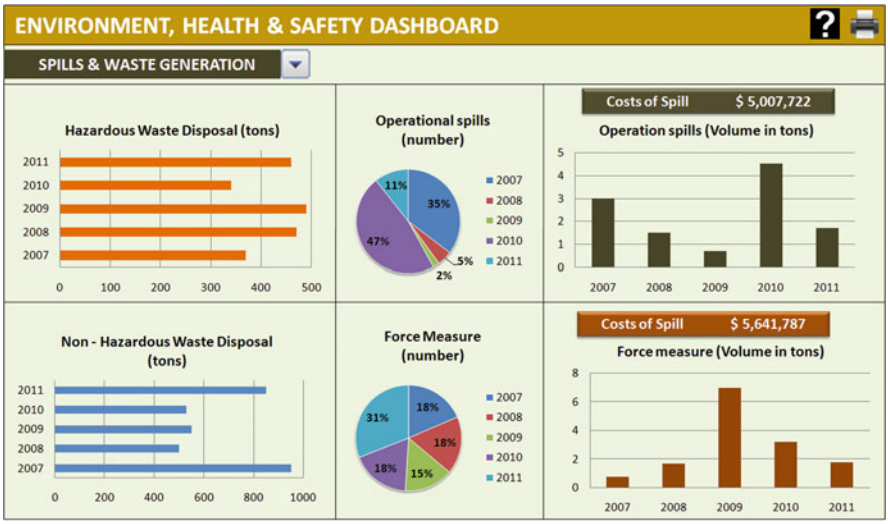


Fig. 7 KPIs monitoring

The application of 5S models reduces the value of the performance shaping factors "Procedure" and "Experience" therefore decreases the value of HEPcont. The example showed in Fig. 6 refers to a 5S safety activity, in which through the use of individual protection systems and passive fire protection, the operator protection values is 90%.

Another key element of continuous improvement processes is the continuous monitoring of data. For this reason, it is crucial to develop a dashboard to represent project progressing. In this way, stakeholders understand if the activities undertaken have improved the condition of the system or if there are still criticalities and so new corrective actions are needed. In the presented case study, the dashboard has to measure the KPI parameters defined in the first phase of the project improvement.

Figure 7 shows the control panel of KPIs value relating to the environment, health and safety in the petrochemical company. Statistics are presented in different graphs, useful for different purposes.

In addition, the dashboard allows to develop sectoral analyzes, referring to specific units of the system under analysis. Furthermore, the dashboard can be viewed on both fixed devices (computers) but also on mobile devices (tablets and smartphones).

Step 7 Optimization projects, implemented in step 6, improve PSFs value (Table 6). Only choice time remains unchanged. The development of improvement processes has reduced the performance shaping factors values, and consequently the value of HEPcont is decreased.

Table 6 New performance shaping factors

New PSFs	
Choice time	1
Experience	1
Procedure	5
$PSF_{comp} = (PSF_1 * PSF_2 * PSF_3)$	5

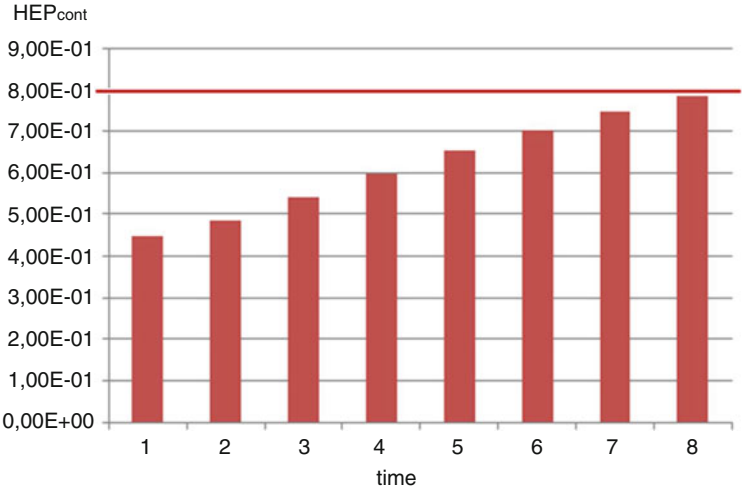


Fig. 8 New human error probability

New human error probability values are shown in Fig. 8. In this case the human error probability is below the limit value (0.8), so the value of human error probability is acceptable and the improvement interventions have been successful.

Observing Fig. 8 it is noted that the absolute value of the error probability has decreased, while the coefficient increment is higher than the initial situation. This is because the improvement intervention only influenced the "external factors" (Performance shaping factors) while the internal factors related to the GTTs remained unchanged.

To analyze and compare the results obtained before and after optimization, it is necessary to develop a sensitivity analysis. The sensitivity analysis (Fig. 9) shows with a linear diagram the results previously obtained. Sensitivity analysis confirms the previously coments. In fact, it shows that, after optimization the absolute error probability value is decreased, but the coefficient increment is higher than the initial situation. The growing trend of error probability after optimization shows that working time significantly affects human reliability. So a further improvement could be the reorganization of shift work, reducing total hours, or scheduling breaks from the fourth hour to limit the human error probability increasing.

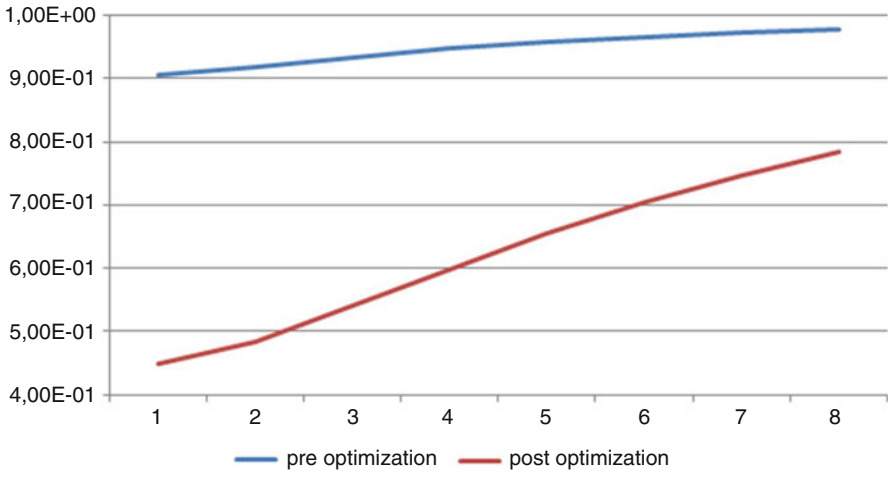


Fig. 9 Sensitivity analysis

5 Conclusions

Human behaviour, during an emergency situation, is subject to numerous studies, because a wrong decision could generate a disastrous consequences. The research presents a new hybrid model development of human error probability evaluation, depending on internal human factors and external environmental factors. Traditional HRA models, analyze separately human behavior and environment. While the presented model develops a hybrid approach that overcomes the limitations of literature. Model simulates human behavior during an emergency situation in a petrochemical company. It has also simulated the improvement of working conditions, monitoring the process through the use of specific performance indicators (KPIs). KPIs analysis allows the manager to define a continuous improvement strategies for process safety. Integrated model HRA-KPIs is advantageous, because it identifies pejorative system parameters and through improvement projects it optimizes human reliability. The model is extremely flexible, it will therefore be possible to apply it to other real case studies in different scenarios. Developed model has several limitations. In particular PSFs are independent of each other. Moreover, the system analyzes only the first 8 h of work. It is also possible extend the model to make it more complete. Future implementation will be HRA evaluation considering dependencies between PSFs and analysis after the first 8 h of work.

References

Carayon P (2006) Human factors of complex sociotechnical systems. Appl Ergon 37(4):525–535
De Felice F, Petrillo A, Zomparelli F (2016a) A hybrid model for human error probability analysis. IFAC-ChaptersOnLine 49(12):1673–1678

De Felice F, Petrillo A, Zomparelli F (2016b) Prioritising the safety management elements through ahp model and key performance indicators. 15th international conference on modeling and applied simulation, Sept 2016, Cyprus
De Koster RB, Stam D, Balk BM (2011) Accidents happen: the influence of safety-specific transformational leadership, safety consciousness, and hazard reducing systems on warehouse accidents. J Oper Manag 29(7):753–765
Del-Rey-Chamorro FM, Roy R, van Wegen B, Steele A (2003) A framework to create key performance indicators for knowledge management solutions. J Knowl Manag 7(2):46–62
DemingWE, Edwards DW (1982) Quality, productivity, and competitive position, vol 183. Massachusetts Institute of Technology, Center for advanced engineering study, Cambridge, MA
Di Pasquale V, Miranda S, Iannone R, Riemma S (2015) A simulator for human error probability analysis (SHERPA). Reliab Eng Syst Saf 139:17–32
Gertman D, Blackman H, Marble J, Byers J, Smith C (2005) The SPAR-H human reliability analysis method. US Nuclear Regulatory Commission
Grosse EH, Glock CH, Jaber MY, Neumann WP (2015) Incorporating human factors in order picking planning models: framework and research opportunities. Int J Prod Res 53(3):695–717
Imam SF, Raza J, Ratnayake RC (2013) World Class Maintenance (WCM): measurable indicators creating opportunities for the Norwegian Oil and Gas industry. In 2013 I.E. international conference on industrial engineering and engineering management, pp 1479–1483
Jiménez M, Romero L, Domínguez M, del Mar Espinosa M (2015) 5S methodology implementation in the laboratories of an industrial engineering university school. Saf Sci 78:163–172
Kim IS (2001) Human reliability analysis in the man machine interface design review. Ann Nucl Energy 28:1069–1081
Kim JW, Jung W (2003) A taxonomy of performance influencing factors for human reliability analysis of emergency tasks. J Loss Prev Process Ind 16(6):479–495
Kirwan B (1996) The validation of three Human Reliability Quantification techniques—THERP, HEART and JHEDI: part 1—technique descriptions and validation issues. Appl Ergon 27 (6):359–373
Kirwan B (1998) Human error identification techniques for risk assessment of high risk systems—part 1: review and evaluation of techniques. Appl Ergon 29(3):157–177
Konstandinidou M, Nivolianitou Z, Kiranoudis C, Markatos N (2006) A fuzzy modeling application of CREAM methodology for human reliability analysis. Reliab Eng Syst Saf 91 (6):706–716
Lo C, Pagell M, Fan D, Wiengarten F, Yeung A (2014) OHSAS 18001 certification and operating performance: the role of complexity and coupling. J Oper Manag 32:268–280
Mendonca D, Beroggi GE, Wallace WA (2001) Decision support for improvisation during emergency response operations. Int J Emerg Manag 1(1):30–38
Mosleh A, Chang YH (2004) Model-based human reliability analysis: prospects and requirements. Reliab Eng Syst Saf 83(2):241–253
Neumann WP, Village J (2012) Ergonomics action research II: a framework for integrating HF into work system design. Ergonomics 55(10):1140–1156
Trucco P, Leva MC (2007) A probabilistic cognitive simualator for HRA studies (PROCOS). Reliab Eng Syst Saf 92(8):1117–1130
Turoff M, Chumer M, Van de Walle B, Yao X (2004) The design of a dynamic emergency response management information system (DERMIS). JITTA 5(4):1
Weber A, Thomas IR (2005) Key performance indicators. Measuring and managing the maintenance function, Ivara, Burlington
Woods DD, Roth EM, People EH (1987) Cognitive environment simulation: an artificial intelligence system for human performance assessment. Technical report NUREG-CR-4862, US Regulatory Commission, Washington, DC

Fabio De Felice, PhD in Mechanical Engineering. Professor at the University of Cassino and Southern Lazio, board member of several international organizations. The scientific activity developed through studies and researches on problems concerning industrial plant engineering. Such activity ranges over all fields from improvement of quality in productive processes to the simulation of industrial plants, from support multi-criteria techniques to decisions (Analytic Hierarchy Process, Analytic Network Process), to RAMS Analysis and Human Reliability Analysis.

Antonella Petrillo, degree in Mechanical Engineering, PhD at the University of Cassino and Southern Lazio. Now Professor at University of Naples "Parthenope" (Department of Engineering) where she conducts research activities on Multi-criteria decision analysis (MCDA), Industrial Plant, Disaster Management, Logistic and Safety.

Federico Zomparelli, degree in Management Engineering at University of Cassino and Southern Lazio. Now, he is a PhD student in Mechanical Engineering at the University of Cassino and Southern Lazio. His research activity is focused on MCDA, lean management, risk analysis and industrial plant optimization.

Use of Bayesian Network for Human Reliability Modelling: Possible Benefits and an Example of Application

Maria Chiara Leva and Peter Friis Hansen

Abstract The scope of the present work is to report an action research project applied to the relationship of task and cognitive workload support on one of the most important aspects of an airport: ground handling. At the beginning of the project workload management was not in the scope of work but as the project progressed and preliminary results and feedback were gained the researcher came to realize that some form of workload management support was also achieved as a by-product. The present chapter is an attempt to account for what was achieved and how. Safe and efficient ground handling during departure and arrival of an aircraft requires coordinated responsibilities amongst qualified operators collaborating together simultaneously in a time constrained environment. The context is one of medium-high workload due to the number of activities covered in a short time, such as: passenger, baggage and cargo handling, aircraft loading, the provision and use of ground support equipment, etc. This chapter presents the introduction of a tool aimed at performance monitoring and task support and discusses how the use of it can play a key role in the adequate management of workload by operators in Ground Handling. The core elements of the tool under analysis are electronic checklist and digitized shift handover, and it aims at highlighting how they have impacted performance, reducing operational and human related issues.

M.C. Leva (✉)
Dublin Institute of Technology School of Environmental Science, Dublin, Ireland
e-mail: chiara.leva@dit.ie; chiaraleva@yahoo.it

P.F. Hansen
Det Norske Veritas, Oslo, Norway
e-mail: pfh@mek.dtu.dk

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_8

1 BBN and Human and Organizational Factors in Probabilistic Risk Analysis

Probability theory is nothing but common sense reduced to calculation. Laplace (1819)

The main issue in modelling operational risks has to do with the understanding of the functioning of a complex system. It requires the application of inductive logic for each one of the possible way in which a system operates to reach its objectives. Then it is the comparison between the hypothesis formulated in the functional analysis and the observations possible on the way the system actually function that can lead to an evolution of the knowledge regarding the system itself. This knowledge is the only credible base for the understanding and therefore a correct modelling of the system under analysis (Galvagni 1989).

Therefore, the first feature that should be evaluated in a risk model even for human reliability assessment is the functional analysis from which the modelling process stems.

The use of Bayesian Belief Networks (BBNs) in modelling operational risk provides a specific advantage when compared to many other modelling approaches since a BBN is to be structured as a knowledge representation of the problem domain, explicitly including the probabilistic dependence between the main elements of the model and their causal relationship, therefore explicating the analyst's understanding of the problem. This is a key feature for validating the behaviour of the model and its accuracy in reporting to third parties the reality under analysis (Friis-Hansen 2000). BBN are becoming more and more widely used in the current generation of Probabilistic Risk Analysis (PRA), to try and support an explicit representation of the possible impacts of organization and management processes on the safety performance of equipment and personnel (Trucco et al. 2008).

In the Bayesian statistical framework, a fully quantified BBN represents the prior knowledge for the analyst. However, as already pointed out, the model can be updated using observations (sets evidence) about certain nodes and verifying the impact on the remaining nodes in the network. By setting evidence, an analyst is proving the model with new information (e.g., recent incident events) about the state of the system. And this information can be propagated through the network to produce updated probabilities for all nodes in the model. These resulting probabilities combine both prior information and new evidence. BBNs have been recently used in traditional Probabilistic Risk Analysis by linking BBN nodes to other risk models using the so called Hybrid Causal Logic methodology (Groth et al. 2010; Wang et al. 2007), which links BBNs to Event Trees and Fault Trees. The use of HCL enables to include soft causal factors, such as human error in more deterministic models, which were more traditionally used for hardware systems.

Furthermore, current HRA methods often ignore the interdependencies and causal relationships among various Performance Shaping Factors (PSFs). While only recently BBNs have been proposed as a way of assessing the interactions among PSFs and the failure modes they are suppose to influence the present chapter report a specific application in this sense.

2 Overview of the Objective of the Case Study

The main objective of the human reliability analysis problem chosen as a case study is to analyse the role of the crew in a collision or grounding event. This was part of a EU research project Safedor whose scope was to provide integration of risk and reliability analysis methods into the design process leads to new ship design concepts. Within this framework the task in which the current work places itself aims at estimating the so-called causation factor for collision events, with due account to the integrated bridge system. The focus is on emergency response actions that is to say the ship under power is assumed to be already on a collision route (Leva et al. 2006). The links among the human element (the crew) and the other context and organizational elements (bridge equipment, operational conditions, level of fatigue etc.) has been analysed and assessed using the framework proposed by Hollnagel (1998). The model had to be integrated within the representation and assessment method chosen for the overall Probabilistic Risk Assessment evaluation, which is to say Bayesian Belief Networks (BBN). The present report describes the main elements considered in modelling the operator performance in the outlined context and the main assumptions underpinning the decisions made in modelling the nodes of the network representing the human action. Human and organizational issues are among the main causation factors for ship under power for avoiding or causing a collision and grounding events. The way the scenario is modelled in turn is a vital input to the modelling of the human actions as well. Due to these interlinks a proper inclusion of the scenario in the model is considered to be key.

3 Brief Overview of Two Approaches Available to Model the Operator

Traditionally the modelling of human actions in the PSA context and particularly in the Nuclear sector, has been carried out using THERP (Swain and Guttmann 1983).

THERP does not provide an explicit operator model, however the underlying assumptions are that the probability of error in executing a certain task can be estimated breaking down the task into observable substeps, identifying the possible related "deviations" (commission or omission errors) for each one of them and recomposing the task and its possible deviations in a binary logic using a binary tree, where the correct path and the possible "error" paths are represented. Alternatively the error path can be represented using a Fault Tree (FT) Representation to be integrated in a larger FT for the overall system reliability analysis. This is a very handy feature since Event Tree and fault Trees are the standard methodologies or PSA especially in the Nuclear Industry. To Analyse the task using THERP means to break it down to a level where the sub-steps are comparable to the elementary actions reported in the THERP Tables for which the Human Error Probability

(HEP) has been assessed using on field observations or Expert Judgments assuming a truncated lognormal distribution for each one of them.

Recent studies [2] have shown the consistency of THERP data tables with empirical observations and the possibility of using the method for contexts that differ from the Nuclear industry.

Stepping in "medias res" a possible model of the crew post initiator errors in response to a collision prone scenario can be illustrated in Annex 1.

Where the main errors considered are:

Top Event: Failure to avoid collision by one ship

1. Failure of one of the member of the crew
2. Failure of the Officer of the Watch
   (a) Failure in communication
      - Failure in communicating with the other ship
      - Miscommunication about the manoeuvre to the helmsman
      - Omit to communicate

   (b) Failure in detection
      - No visual detection of the ship on a collision route
      - No radar detection of the ship on a collision route
      - Failure to respond to one annunciator (a collision alerting system available on board)

   (c) Misinterpretation of the information detected
   (d) Failure in Planning of action
3. Helmsman error
   (a) Misunderstanding of the manoeuvring order
   (b) Error in executing the manoeuvre
4. No Recovery from the other members of the crew
5. No recovery from Vessel Traffic Service (VTS)
   (a) Vessel Traffic Service (VTS) does not see the two ship on the collision route
   (b) The VTS omit to tell

The binary logic organization of the errors is represented using AND/OR gates in the FT (Annex 1). Every single element on the tree can be detailed and discussed individually, however in the present paper the purpose of the FT outlined is just to provide an example of a possible representation of the crew action, which pays the way for the first possibility for an assessment.

Alternatives in the use of alerting systems, the role of the crew members, or possible roles of the VTS can be explored further, leading to different results and enabling a comparison among them. The analysis has to be carried out in conjunction with a more extensive analysis of the system as a whole (Ship parameters, weather conditions, traffic intensity, crew actions) (Fig. 1).

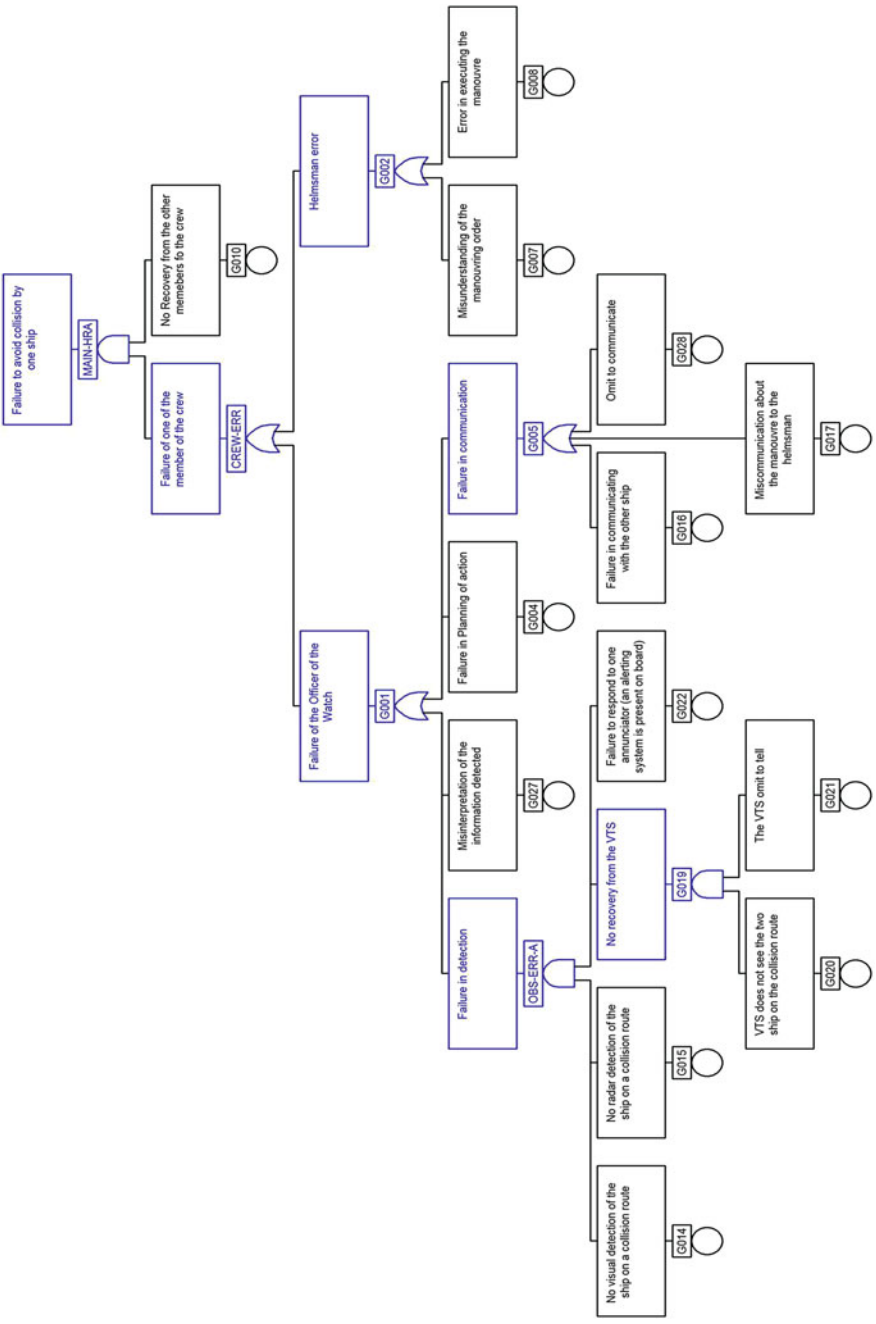


Fig. 1 Example of a possible representation of the operator model using Therp and Fault Tree analysis

However the approach encounters some significant difficulties. The Human Error Probabilities (HEP) are "insensible" to the context, that can only be taken into account through the use of multiplication factors, slightly arbitrary, that enable to take into account the effect of some of the main factors only (or nearly so). Thus no contextual factor can be actually taken into account, which is limiting the capability of a safety by design approach in respect of some of the main elements highlighted during accident analysis as contributing causation factors, or "latent causes". Examples of these factors also called Performance Shaping Factors (PSF), that include environmental and operator variables, are:

- time of the day
- stress
- fatigue
- experience of the operator
- knowledge
- Equipment usability
- Workplace conditions (noise, temperature, humidity, lighting etc.)
- Shift duration
- Weather conditions.

However the lack of data in the field most of the time, does not enable the use of a data driven model for establishing links among those factors and the human actions, and the links among themselves.

A framework that can be used in order to established a first approach to tackle the problem are the cognitive studies developed by Hollnagel (1993), where the problem is, in first approximation, dealt with considering the overall effect of the sum of factors with a positive influence and the sum of those with a negative influence in respect of the capability of a human operator to perform a given task. The PSF are actually called Common Performance Conditions (CPCs) and they can be highlighted through on field observations and direct crew-members interviews.

Essentially the way Hollnagel propose to tackle the modelling of operator in COCOM (Context and Control Model) is considering that team behaviour (i.e. a crew on a bridge) should be analysed at a macro, rather than micro, level. He proposes four principal models of team activity: strategic, tactical, opportunistic, and scrambled. These modes of team behaviour vary in terms of the degree of forward planning (highest in the strategic mode) and reactivity to the environment (highest in the scrambled mode). He further hypothesises a linear progression through the modes from strategic to tactical to opportunistic to scramble, depending upon context, and vice versa.

This modelling approach implies the use of CREAM (Hollnagel 1998) for performing the assessment of HEPs. Thus instead of considering the subtasks analysis for a comparison with the THERP Database the subtasks are analysed in terms of the Cognitive "Demand" for each of them and according to this some HEP ranges are suggested. Those ranges are then modified using multiplication factors that depend upon the control mode identified as the most probable for the situation under analysis. The framework proposed was considered, at the start, to be a

"reasonable" base in the existing literature for modelling the operator action and its underlying contextual factors within the framework of safety analysis.

4 The Contextual Control Mode

The Contextual Control Model is an extension of the Simple Model of Cognition,[1] and addresses the issues of modelling both competence and control. COCOM proposes that there are four overlapping modes of control—influenced by knowledge and skill levels—that also influence behaviour.

> It is an axiom of the study of human behaviour that everything we do is influenced-but not completely determined-by the conditions that exist at the time. (Hollnagel 1998)

Traditionally the elements highlighted as important in respect to a human performance, such as task characteristics, aspects of the physical environment, work time characteristics, etc. have been called Performance Shaping Factors. In traditional HRA approaches their influence is expressed as a numerical factor that is used to modify the basic Human Error Probability (HEP). Example of them are issues such fatigue, experience of the operator, training, tendency for risky behaviour, communication/collaboration among members of the same team, roles and responsibility distribution, pressure of schedule, equipment usability, workplace conditions (noise, temperature, humidity, lighting), shift duration, etc.

In the COCOM approach human performance is determined, largely, by the situation. The selection among the possible actions is determined by the demand characteristics of the situation. Due to the regularity of the environment there may be frequently recurring patterns or configurations of actions, but this is not evidence for procedural prototypes. A contextual control model is based on three main concepts: competence, control, and constructs (Hollnagel 1993).

[1]The Simplified Model of Cognition (SMoC) can be considered as an extension of Neisser's (1976) perceptual cycle and describes cognition in terms of four essential functions:

1. observation/identification,
2. interpretation,
3. planning/selection, and
4. action/execution.

These functions are not necessarily sequential. The small number of cognitive functions in SMoC reflects the general consensus of opinion that has developed since the 1950s on the characteristics of human cognition (Ritter et al. 2003). Those functions are in fact common to other Human Reliability Analysis (HRA) approaches as well. The fundamental features of SMoC are the distinction between what can be observed and what can be only inferred [4] (observation and execution can be observed as overt behaviour while interpretation and planning of action can only be inferred from the formers), and the cyclical nature of cognition (Neisser 1976).

– Competence represents the set of possible actions or responses that a system can apply to a situation according to the recognised needs and demands. The extent of this set depends on the level of detail of the analysis.
– Control exemplifies the way in which competence is applied. As already stated COCOM assume a set of control modes: scrambled, opportunistic, tactical, and strategic.
– Constructs refer to what can be assumed about the situation in which the action takes place. The term alludes to the fact that constructs are artificial, in the sense of being constructions or re-constructions of salient aspects of the situation, and that they are usually temporary. (Hollnagel 1993).

Each control mode can be associated with a characteristic type of performance. Although the control that a joint system can have over a situation may vary continuously, it is useful to make a distinction between the following four characteristic modes:

- Scrambled control: where the selection of the next action is unpredictable. This is the lowest level of control.
- Opportunistic control: where the selection of the next action is based on the current context without reference to the current goal of the task being performed.
- Tactical control: where performance is based on some form of planning.
- Strategic control: where performance takes full account of higher-level goals. This is the highest level of control.

Some characteristics of the four control modes might be find in reference (Hollnagel 1993) however what it is important to notice here is that the transition between control modes depends on a number of factors, particularly the amount of subjectively available time and the outcome of the previous action. These two factors are interdependent, and they also depend on aspects such as the task complexity and the current control mode.

In order to determine which control mode we have to refer to and the influence it has on the human performance from a human reliability analysis perspective we can use a different method namely CREAM. Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel 1998) has been developed from COCOM for carrying out both retrospective analysis of accidents and events, and human reliability assessment. The expected effect of each control mode on performance reliability is illustrated in Fig. 2.

The control mode most probable in a given situation in CREAM is linked to a limited set of the so called Common Performance Conditions (CPCs), which are the equivalent of Performance Shaping Factors of many other HRA approaches, therefore the elements used for characterizing the situation itself. They are:

– **Adequacy of organisation**: The quality of the roles and responsibility distribution of team members, the availability of a Safety management System, and of precise instruction and guidelines for operative conditions. In respect to safety the concept can also be linked to the safety culture of the organization itself.

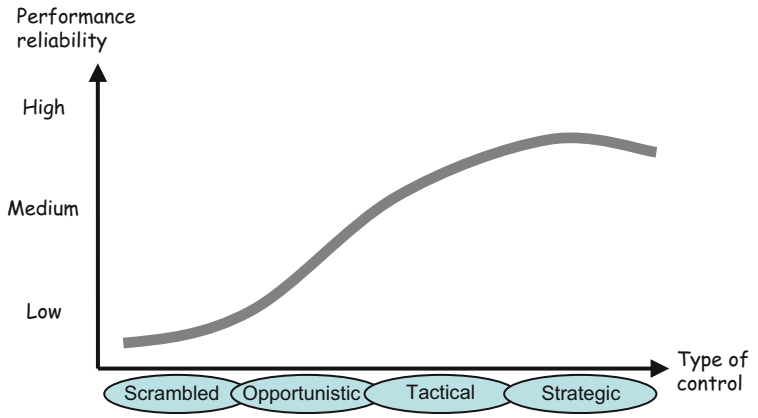


Fig. 2 Expected effect of each control mode on performance reliability adapted from Hollnagel (1993)

- **Working conditions**: The nature of the physical working environment such as noise, temperature, humidity, lighting etc.
- **Adequacy of MMI and operational support**: This CPC refers to the quality of the Man Machine Interface (MMI), which is to say the control panels or more in general the equipment the operator has to interact with for carrying out his/her tasks.
- **Availability of procedures/plans**: They include emergency plans and procedures, familiar pattern for response etc.
- **Number of simultaneous goals**: This CPC refers to the number of tasks an operator is required to perform at the same time.
- **Available Time**: Time available for carrying out the task.
- **Time of the day**: IT is well established the fact that the time of day has an effect on the quality of the work: the performance could be less effective if the normal Circadian Rhythm is not respected.
- **Adequacy of Training and experience**: Level and quality of training provided to the operators, and familiarization to the technologies adopted in the working context.
- **Crew collaboration quality**: Normally if in a crew the members work well together a task will be more easily performed efficiently. Responsibilities and working loads would be more efficiently shared.

CPCs have an effect on each other, Hollnagel identified dependencies among the above CPCs as well, and they are described in his book about CREAM. Table 1 reports the expected effect of each CPS conditions on Human Reliability.

In CREAM then the Combined CPCs score that will be considered to affect the human performance is derived by counting the number of times where a CPC is expected:

Table 1 Common performance conditions and performance reliability

CPC name	Level descriptors	Expected effect on performance reliability
Adequacy of organisation	Very efficient	Improved
	Efficient	Improved
	Inefficient	Not significant
	Deficient	Reduced
Working conditions	Advantageous	Improved
	Compatible	Not significant
	Incompatible	Reduced
Adequacy of MMI and operational support	Supportive	Improved
	Adequate	Not significant
	Tolerable	Not significant
	Inappropriate	Reduced
Availability of procedures/plan	Appropriate	Improved
	Acceptable	Not significant
	Inappropriate	Reduced
Number of simultaneous goals	Fewer than capacity	Not Significant
	Matching current capacity	Not significant
	More than capacity	Reduced
Available time	Adequate	Improved
	Temporarily inadequate	Not significant
	Continuously inadequate	Reduced
Time of the day	Day-time	Not Significant
	Night-time	Reduced
Adequacy of training and experience	Adequate, high experience	Improved
	Adequate, limited experience	Not significant
	Inadequate	Reduced
Crew collaboration quality	Very efficient	Improved
	Efficient	Not significant
	Inefficient	Not Significant
	Deficient	Reduced

1. To reduce performance reliability
2. To have no significant effect
3. To improve performance reliability.

This leads to have a triplet $[\Sigma_{reduced}, \Sigma_{not\ significant}, \Sigma_{improved}]$ constitute by summing each category without introducing any theoretical assumption in relation with the CPCs and their effect on each other.

From the above triplet it is now possible to determine the likely Control Mode.

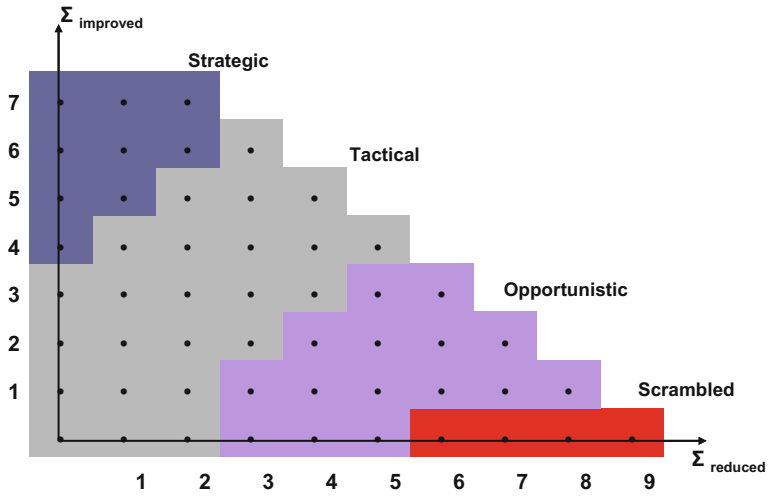


Fig. 3 Relations between the CPC score and the control modes in CREAM (adapted form Hollnagel 1993)

It is obvious that the least desiderable situation corresponds to the Scrambled control mode while the preferable situations are the ones where the operator has a strategic or a tactical control mode.

Since the number of not significant CPCs value is not very important the couple of values [$\Sigma_{reduced}$, $\Sigma_{improved}$] can be plotted and from the plot is possible to identify for each couple the most likely control mode, as shown in Fig. 3.

The steps of the analysis for establishing the CPC effect can be summarized as follow:

- Determine the CPCs that have an influence on performance
- Consider interdependencies among CPCs
- For each CPCs determine the expected level by using the descriptor of Table 2.
- Determine the expected effects on performance reliability using the outcomes listed in Table 2.
- From the Plot in Fig. 3 Determine the likely Control Mode.

The control Mode is then used in the Assessment Phase.

However its practical application in the present case study (collision or grounding events) was limited to only one case, where the use of the control mode was not considered to be acting as a black box within the Bayesian Network and it's effect was more easily traceable. Furthermore the possible relationship of dependence among contextual conditions was left to expert judgment for those elements judged to have a considerable effect on the operator ability to perform the required task (evasive manoeuvring in case of collision or grounding risk).

Table 2 Common performance conditions to be used in the model for operator performance on the bridge

CPC name	Brief description
Fatigue	Fatigue is one of the most important contextual conditions maritime operators seems to be exposed to, due to the working conditions. It depends on the shift duration and the hidden link is with the safety culture of the organization that look after the planning of the journey and the time pressure foreseen for the journey schedules
Competence	Competence is a Contextual Condition that summarise the level of experience of the operator and the level of training that enable an operator to possess the knowledge required for him in order to perform his own job
Time pressure	After a possible danger has been detected it is important to take into account the amount of time left for the operator to take action for avoiding the accident. If the time available is very short the planning phase is affected by time pressure that could influence the capacity of the operator to take decision
Time available	Time available to take action is always an important Contextual Condition, even when the operator itself is not aware of it
Weather conditions	Weather conditions affect in many ways the performance of the operator and the usability of the equipment on board (such as the radar). Can reduce visibility and affect the state of vigilance required by the operator as well
Support for planning provided by the bridge layout	The way the bridge layout is organized, and the equipment that it enables to be accessible can affect the performance of the operator both in terms of the time required for him to take action and the correctness of the action taken as well. This can be an observable data from simulators experiments and, in turn, can provide a useful mean for assessing the ergonomics of the bridge layout itself
Navigational complexity of the area	Some area regions are naturally keen to present more difficulties and hazards for the navigation. Such as straits, and channels with shallow water areas
Elements of distraction	The presence of many elements of distraction (such as phone calls, and coming off of false alarms, or tasks that are not really pertinent to the navigation itself, are to be considered important in affecting the vigilance of the operator
Vigilance	A qualitative definition of the possible degree to which an operator might be vigilance it is a useful indication for assessing the probability that he might detect a hazardous situation in time
Shift duration (working hours)	According to the European directive 1999/63/EC the hours of work and rest form maritime operators should not exceed a certain limit. If they do they expose the operator to an excessive workload and fatigue
Traffic intensity	Area with high traffic intensity such as straits, and channels are more exposed to hazards of collisions and grounding, and they are therefore more demanding for the operators in terms of effort for avoiding them

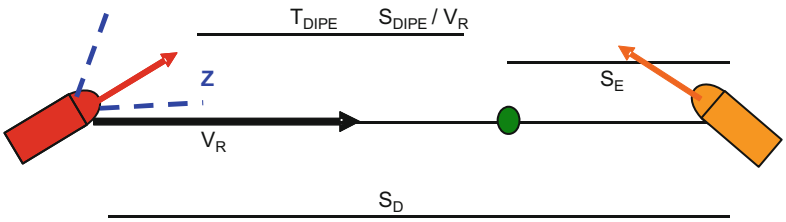
(continued)

Table 2 (continued)

CPC name	Brief description
Daylight (if it is Day or night)	The fact that is day or night affect both visibility and the capacity of the operator to keep a vigilance status (due to the circadian rhythm)
Ergonomics of the Bridge Layout	The way the bridge layout is organized, and the equipment that it enables to be accessible can affect the performance of the operator since he might be required him to go away from the optimal workstation for accessing other means, or control boards. This can be an observable data from simulators experiments and, in turn, can provide a useful mean for assessing the ergonomics of the bridge layout itself
View Zones	area from which the other ship or object is approaching: Head, Starboard, Port, Aft
Clarity of the give way situation (to be used for the collision scenario)	The Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs) provides guidance in determining safe speed, the risk of collision and the conduct of vessels operating in or near traffic separation schemes. These regulations can be applied if the situations the ship find itself in is clear (overtaking, being overtaken, etc.). When this situation is not clear the plan complexity increases
Presence of a watch alarm system	According to the RESOLUTION MSC. 128(75) "The purpose of a bridge navigational watch alarm system (BNWAS) is to monitor bridge activity and detect operator disability which could lead to marine accidents. The system monitors the awareness of the Officer of the Watch (OOW) and automatically alerts the Master or another qualified OOW if for any reason the OOW becomes incapable of performing the OOW's duties. This purpose is achieved by a series of indications and alarms to alert first the OOW and, if he is not responding, then to alert the Master or another qualified OOW. Additionally, the BNWAS may provide the OOW with a means of calling for immediate assistance if required." The alarm can be set to start at fixed intervals of time (i.e. every 8–10 min), and must be acknowledged by the OOW to prove that the OOW is able to perform the duty

5 Model of the Operator Performance: The Relevance of the Scenario

The context in which the subtask takes place is aimed at modelling the causation factors in respect to a ship under power on a collision or grounding course. The focus is on emergency response actions that is to say the ship under power is assumed to be already on a collision course with another vessel. Friis-Hansen and Terndrup Pedersen (1999) and Lützen and Friis-Hansen (2003) presented theoretical studies for modeling the causation factor. In modelling the scenario we considered those studies



$T_A = (S_D - S_E) / V_R$

IF $T_{DIPE} > T_A$ THEN COLLISION

T_{DIPE}	Time for Detect, Interpret, Plan and Execute
S_E	Minimum distance for performing the evasive manoeuvre
S_D	Distance for Detectability by device (visual, audible, radar, AIS, …)
T_A	Time available to react
V_R	Relative speed
Z	View Zone

Fig. 4 Main elements to be taken into account for the collision scenario within the model

combined with a task analysis of the operator response. Therefore there are some assumptions related to the scenario the model has to refer to.

In order to identify the main tasks to be carried out by the operator for avoiding the accident we assume as initiating event the fact that the ship is on a collision course with an another ship, or on a grounding course, and the equipment on board functions properly. Failures of some equipment can be analysed within the framework but it is not part of the operator model itself.

A simplified sketch with some of the element to be considered for the scenario in case of collision is reported in Fig. 4.

The scenario needs to set the ship type and its speed and the view zone from where the other "object" is coming and its relative speed. According to this and the visibility (weather conditions that can affect the sensorial detectability of the danger) the operator has a different time frame for taking action.

The nodes that describe the scenarios and whose input are fundamental for the nodes used for modelling the operator actions take into account a more precise description of the possible different configuration a collision or a grounding scenario might assume using geometrical descriptors such as the angle between the direction of the two ships, the relative velocity, the relative bearing angle for the direction of the approach observed by the two ships in respect to each other. Some of this elements are described in Fig. 5. They are useful also to determine contextual conditions affecting the operator performance (as for instance whether or not the situation clearly indicate who should give way according the Colreg regulation).

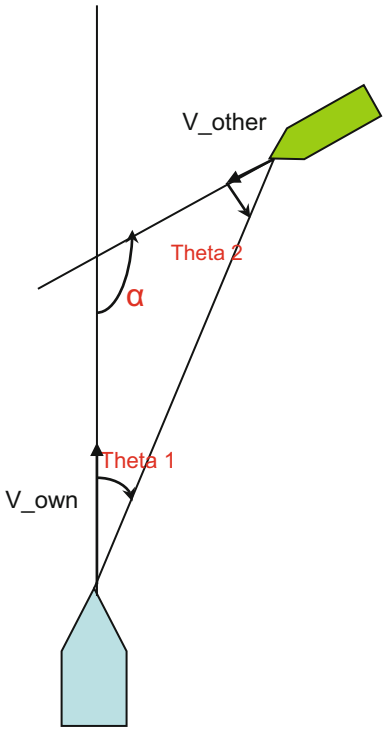


Fig. 5 BBN compact model for operator performance in collision scenario

As far as the operator model skeleton is concerned, a simplified version of the tasks to be performed in order to avoid grounding or collision is:

TASK: The Officer Of the Watch (OOW) has to detect the other ship or object on a collision route, plan a manoeuvre and execute it. The Helmsman can execute the manoeuvre if present.

The model of the operator in COCOM implies the identification of the cognitive functions involved in executing the task. The model should in fact be able to describe a set of cognitive functions that can be used to explain human correct and erroneous actions. Those functions are identified assuming the framework of the Simple Model of Cognition (SMoC) (Hollnagel and Cacciabue 1991). The Simplified Model of Cognition (SMoC) that describes cognition in terms of four essential functions:

1. observation/identification,
2. interpretation,
3. planning/selection, and
4. action/execution.

The above functions are not necessarily sequential. The small number of cognitive functions in SMoC reflects the general consensus of opinion that has developed since the 1950s on the characteristics of human cognition (Neisser 1976). Those functions are in fact common to other Human Reliability Analysis (HRA) approaches as well. The fundamental features of SMoC are the distinction between what can be observed and what can be only inferred (Hollnagel 1998) (observation and execution can be observed as overt behaviour while interpretation and planning of action can only be inferred from the formers), and the cyclical nature of cognition (Neisser 1976).

Referring to the above framework the cognitive functions identified as important in carrying out the task of the operator for avoiding a collision are;

1. Detection-Interpretation
2. Interpretation-Planning
3. Execution of the actual manoeuvre (which also imply a possible process of communication between the operator (Officer of the Watch) and the actual executor of the manoeuvre which could be the Helmsman.

6 The Contextual Conditions for the Operator Model

The Common Performance Conditions highlighted in the case under analyses are reported in Table 3. A more detailed description of them will follow in the paragraph that relates to the nodes that need to be included in the final Causation factor model for collision and grounding events. The Contextual Performance Conditions are obviously related to each other the links among them are at two levels: they may be connected to each other and they may be connected to the same specific human action. The connections with the human actions are reported in Table 3, while the connections among themselves in Table 4. They were identified using expert judgment. The use of the control mode according to the COCOM model is present only on the planning phase where the "control mode" node can be used to summarize the impact on the operator of the following external conditions: time pressure, competence of the operator and plan complexity.

The above tables (Table 2, Table 3 and Table 4) provide the Common Performance Conditions and their connections with the task to be analysed for the operator model. This according to the theoretical method chosen (COCOM-CREAM) is one of the basic elements to base the development of the model. It helps therefore in representing the role played by the operator on the bridge in the framework of the collision and grounding scenarios. The connection could be revised or updated as the modelling of the overall causation factor progresses.

Table 3 Common performance conditions affecting operator functions

	Function	Details about breakdown of the function	Common performance conditions affecting the function
Officer of the watch	Detection	Looking frequency for radar or AIS Looking frequency for outside Respond to annunciators (if alarm is present on board)	• Fatigue • Weather conditions • Day light • Vigilance • Elements of distraction • Area complexity • Ergonomics • Shift durations • Traffic intensity • Time available for detection • Availability of Radar or AIS • View zone • Presence of a watch alarm system
	Planning of the manoeuvre	The manoeuvre could be decided with wrong timing or the planning can be wrong even if made in perfect timing. Both possibilities are taken into account	• Competence • Clarity of the give way situation (for collision scenarios) • Traffic intensity • Navigational complexity of the area • Support for planning coming from the Bridge • Layout (availability of ECDIS etc.) • Time available for planning
	Execution of the manoeuvre		• Competence • Time available for manoeuvring • Ergonomics of the bridge layout • Communication with the helmsman (if present) • Steering mode

7 Model of the Operator: Why Choosing Bayesian Belief Networks

The data problem for safety assessment in the maritime domain can be referred to other causation factors (not only the human and organizational ones). Therefore the use of a methodology such that of Event Tree and Fault Tree would not be advisable for helping the analyst in the difficult issue of the data gathering, especially because some of the data would be collected through the use of Expert Judgment. A more suitable method for implementing the main structure of Safety Assessment as far as

Table 4 Main dependencies identified among CPC through Expert Judgment

Elements that have an influence	Element that is influenced
Shift duration	Fatigue
Fatigue	Vigilance
Traffic intensity	
Day or night	
Weather	
Navigational complexity of the area	
Elements of distractions	
Support provided by the bridge layout	Plan complexity
Competence	
Traffic intensity	
Clarity of the give way situation	
Time pressure	
Vigilance	Frequency with which the Operator look outside or to the radar/AIS
View zones	
Presence of a watch alarm system	
Ergonomics	

the causation factors for the collision and grounding events are concern are Bayesian Belief Networks (BBN). They are a widely used method for representing uncertain knowledge. The BBN approach stems from conditional independence assumptions and strongly relies on graphical representations. Therefore it makes it easy to display how the model of a complex system works and its dependences and causal structures (Cowell et al. 1999).

Briefly a BBN consists of:

- A directed acyclic graph (DAG) with nodes V in D and edges representing the causal probabilistic relationship among the nodes;
- A set of random variables:

$$X = (X_v)_{v \in V} \tag{1}$$

- a probability distribution on X given by the joint density:

$$p(x) = \prod_{v \in V} p\left(x_v | x_{pa(v)}\right) \tag{2}$$

where $pa(v)$ denotes the set of parents of v in D and $x_A = (x_v)_{v \in A}$ for any subset A of D.

The conditional property applies when A and B have the same parent C. For each node it is possible to consider a conditional probability table for the conditional

probabilities with respect to all possible combinations of values in the parent nodes. A marginal distribution is specified for the root nodes, i.e. those without parents, and joint probabilities can be computed in cascade using the chain rule.

The probabilities of a generic BBN are updateable given a set of evidences collected from the field, therefore a BBN model of organisational factors involved in accident scenarios might be updateable over time exploiting information contained in accident/incident reporting systems, or coming from simulation experiments. The BBN that refer to the crew action developed within Safedor in the initial stage was mostly filled using Expert Estimates however some of them are "mathematical nodes" for which specific mathematical formulation can be assumed. As far as the operator model is concern in fact there are some node for which a specific distribution has been assumed and the related mean and variance has been the assessed using Expert judgment. The node labelled as "control mode" for instance influences is decided using Expert judgement for assessing how much the mean value for the distribution of the Probability of error in planning or the time needed for the planning phase is shifted from the nominal conditions giving a certain control mode for the operator. The study aims at outlining a first network whose results and whose robustness will be tested in the validation phase of the project. If the tool provides reasonable results all the assumptions can be explored and some sensitivity analysis can be directed towards the evaluation of different approaches for linking Human Actions to Influencing factors.

8 The operator Model Nodes

A Bayesian Belief Network will be used for representing the causation factors for ship under power in collision and grounding scenario. The causation model is broken down into objects for the scope of clarity, each object is a Bayesian Network representing part of the bigger picture (Scenario, Detection, Planning of action etc.) connected to each other through the input-output nodes.

Some of the nodes that might be used or connected to the modelling of operator actions and that will be connected within the overall framework for the causation factors are reported in Table 9. They might be modified if the progresses in the definition of the overall picture require doing so.

The first simplifying assumption we encountered on the model is considering only one OOW, The "solo watch" assumption is considered justifiable by the fact that a solo watch situation is actually more critical than the traditional one, where the OOW task is supported by additional crewmen (Fig. 6).

Considering the scenarios the model aims at approaching (which assumes as initiating event the fact that the ship is on a collision course with another ship, or on a grounding course, and the equipment on board functions properly) the first action

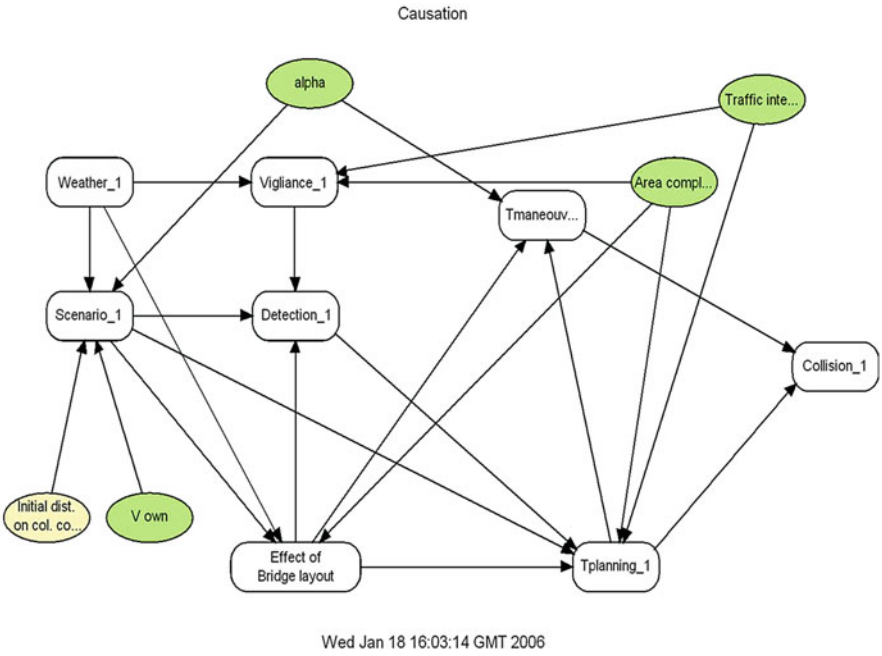


Fig. 6 **B**BN related to detection. The network is part of the object named TDetection in Annex III

the OOW should perform in order to take action is the detection. The model that covers the issue of visual detection in the network is reported in Fig. 7.

The OOW can detect the danger by two means: looking outside from the bridge, or checking the radar/AIS. The frequency with which the OOW perform a look out check and the one with which he check the radar are interdependent. In the model we assume a lognormal distribution for the mean time between two successive look out scan and a lognormal distribution for the mean time between two successive radar/AIS scan. Both distributions depend from the same two parents nodes: the node "World, Radar, Other" and the node "BNWS" (Bridge Navigational Watch alarms system). The node "World, Radar, Other" is used to describe how the OOW distribute its time among different tasks: looking outside, looking at the radar, doing other things. The assessment of its related conditional probability table depends on Vigilance, and the Ergonomic of the Bridge Layout. Looking at Tables 5 and 6 we can clarify the process by which the values have been assigned: the assessment starts with expert judgment on the node where the ergonomic does not contribute (Table 5), and then it take into account the contribution of the ergonomic quality of the bridge (the probability table for the node where the ergonomics has an effect are reported in Table 6). It reduce the no surveillance probability by the percentage given by the status (value x), and increase the value of World by P(w)/[P(w) + P(r)] of this value x and Radar by P(r)/[P(w) + P(r)] of the same value x.

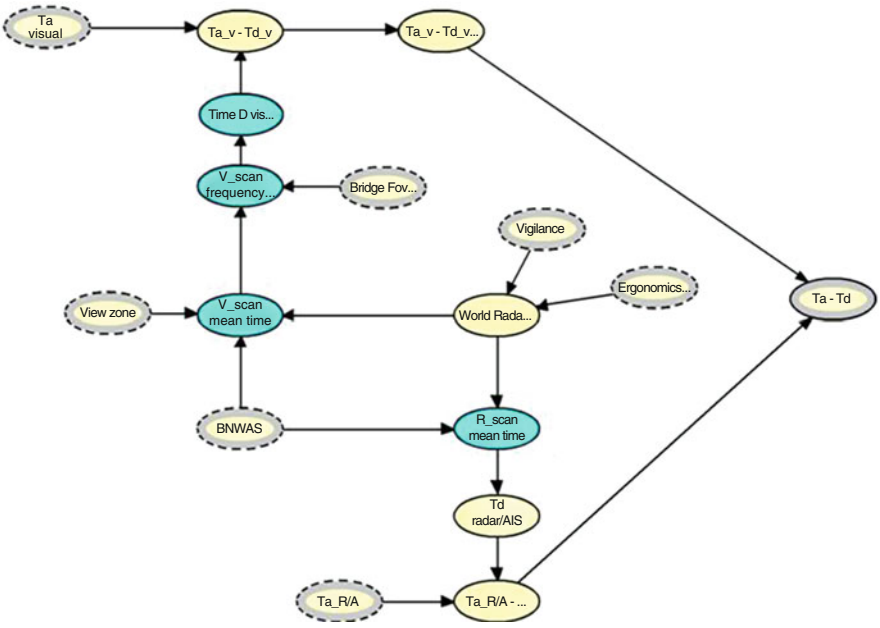


Fig. 7 BBN related to planning. The network is part of the object named TPlanning in Annex III

Table 5 Example of a conditional probability table for the node "World, Radar, Other" where ergonomics has no impact

Vigilance	Low	Medium	High
Visual/audible	65	70	75
Radar/AIS	10	10	15
No surveillance	25	20	10

Table 6 First six columns of the probability table for the node "World, Radar, Other"

Ergnomics	0–0.05	0–0.05	0–0.05	0.05–0.1	0.05–0.1	0.05–0.1
Vigilance	Low	Medium	High	Low	Medium	High
Visual/audible	65.541	70.437	75.441	66.625	71.312	76.323
Radar/AIS	10.083	10.06	15.041	10.250	10.187	15.125
No surveillance	24.375	19.500	9.7500	23.125	18.500	9.2500

Therefore according to the fact that the state of the node "World Radar, Other" is in the state "Visual/audible" "radar/AIS" or "no surveillance" the mean of the lognormal distribution for the looking frequency and the radar checking frequency assume a different value.

Table 7 First six columns of the conditional probability table for the node "Mean time between two successive scan"

BNWAS	6 min	6 min	6 min
World/Radar/Other	Visual/audible	Radar/AIS	No surveillance
0.001–0.25	0.0051	0.6614	0.0000
0.25–0.625	0.0660	0.2740	0.0000
0.625–1.25	0.1916	0.0553	0.0000
1.25–2	0.2092	0.0076	0.0000
2–3	0.1896	0.0014	0.0000
3–4	0.1155	0.0002	0.0008
4–6	0.1172	0.0001	0.5243
6–8	0.0504	0.0000	0.4652
8–10	0.0242	0.0000	0.0096
10–12	0.0126	0.0000	0.0000
12–16	0.0111	0.0000	0.0000
16–inf	0.0076	0.0000	0.0000

The time is measured in minutes

The effect of the node "BNWAS" is to truncate the distribution so that if a Bridge Navigational Watch Alarm System is present on board, and it is set on a certain time interval the probability that one look out scan or one radar check happened before the BNWAS time interval is 95%. An example of this is reported in Table 7; where the state of the BNWAS is assumed to be set on to 6 min.

Furthermore the mean time between two successive look visual scan is affected specifically also by the node that take into account the Bridge Field of Vision "Bridge FOV".

The probability that the detection either by looking outside or by checking the radar/AIS is given according to an exponential distribution.

$$P(t) = \int_0^t \lambda e^{-\lambda x} dx \tag{3}$$

Therefore Eq. (3) represents the distribution of the probability of detection from 0 to the time t. the parameter λ is the looking frequency, which is to say the inverse of the mean interval of time between two successive scans.

Finally given the time available for visual or radar detection from the nodes of the scenario object, the total time available after detection is evaluated as maximum value between the two nodes "Ta_R/A–Td_R/A" and "Ta_v–Td_v".

After modelling the step of detecting the danger it is necessary to model the planning phase where the OOW plans what type of manoeuvre he wants to execute in order to avoid the collision. In this phase we make used of the concept introduced

Table 8 First six columns of the conditional probability table for the node "Control mode"

Support for planning	0–0.05					
Competence	Medium			High		
Time pressure	Very high	High	Normal	Very high	High	Normal
Tactical	0.01	0.12	0.18	0.02	0.15	0.23
Opportunistic	0.14	0.49	0.72	0.16	0.61	0.90
Scrambled	0.70	0.39	0.20	0.44	0.24	0.12

by Hollnagel (1998) of the control mode. The node called "control Mode" is used to summarize the impact on the operator of the following conditions: time pressure, competence of the operator and the support for planning provided by the bridge layout. The node presents three possible states:

- Scrambled control: where the selection of the next action is unpredictable. This is the lowest level of control.
- Opportunistic control: where the selection of the next action is based on the current context without reference to the current goal of the task being performed.
- Tactical control: where performance is based on some form of planning.

The strategic control mode in fact, given the type of scenario considered, is not a likely control mode for our cases. The conditional probability table of the node is assessed with a method similar to the one followed for assessing the node "World, Radar, Other" (Table 8).

Another node is then used for summarizing the impact of other contextual conditions. This node is called "Complexity of the plan to be developed", while the contextual condition of which it is made are: "clear give way", "area complexity", "traffic intensity".

The node "clear give way situation" is an input coming from the object scenario. This node in fact serves to indicate if, according to the geometrical configuration of the collision course, the situation that the operator has to face is ambiguous or unclear. The main rules in a comparison with which the ambiguity is considered are the one stated in the Colreg 1972 "Convention On The International Regulations For Preventing Collisions At Sea". Unclear give way situations are considered to be the following:

- Head on (alpha from 175 to 185)
- Being overtaken (alpha smaller than 180 and theta 1 from 107.5 to 117.5)
- Overtaking (alpha greater than 180 and theta 2 from 107.5 to 117.5). Where alpha and theta are described in Fig. 8.

Where alpha is the angle between the object speed vector and the own ship's speed vector: alpha is 0 when the two ships are sailing in the same direction while it is 180 when the two ships are head on. Theta 1 is the relative bearing of the other

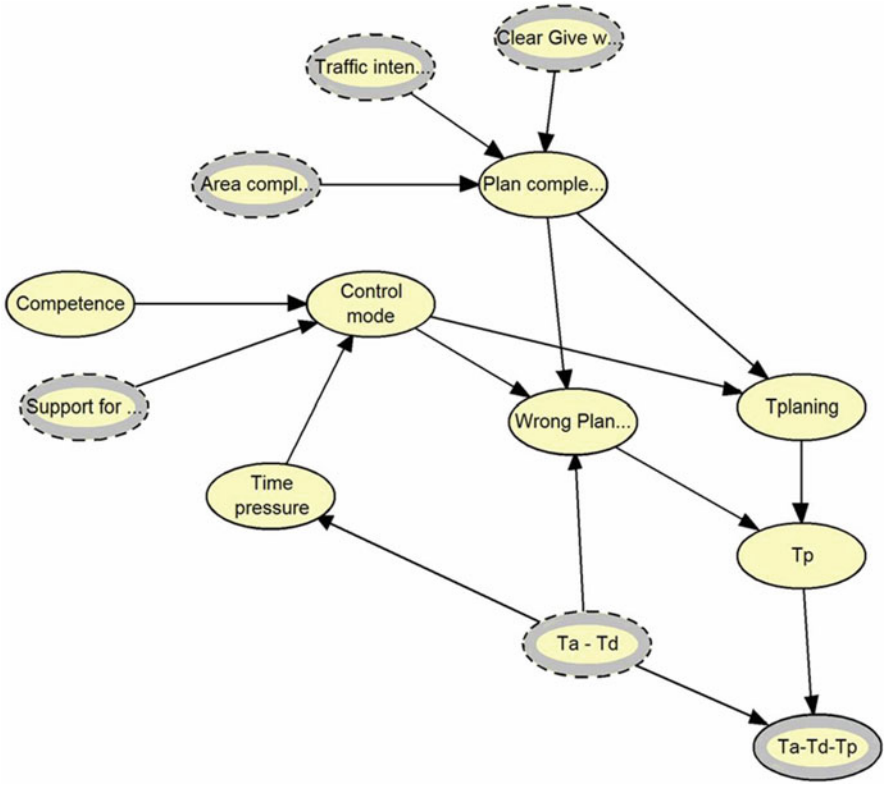


Fig. 8 Geometrical representation of a possible collision scenario

object in relation to own vessel, while theta 2 is the relative bearing of own vessel in relation to the object on collision course.

The intensity of traffic in the area and the navigational complexity of the area are node whose states are decided by the users. They are user input nodes.

According to the control mode the operator is considered to be in and on the complexity of the planning, it is then possible to attribute some values for the probability that the operator perform a wrong plan or on the time likely to be used by the OOW for deciding the action to be taken.

The probability that the operator either takes no decision or takes the wrong decision is assigned according to a logit distribution whose formula is

$$HEP(t) = 1 - \frac{e^{\frac{(t-\mu)}{\sigma}}}{1 + e^{\frac{(t-\mu)}{\sigma}}} \tag{4}$$

Where the mean (μ) and the standard deviation (σ) of the logit are calibrated using two pair of points (T, HEP), where T is a given interval of time available to perform a

decision and HEP is the Human Error Probability of failing the planning. These two pairs are dependent on the given "Control Mode" state and the "Plan Complexity" state. And they are on this first release of the model based on expert judgment. The pairs of value for the calibration will be in the future substitute by two possible couple coming from observational data (simulator training experiments).

It is worth noting that

$$\sigma = k\left(1 - e^{\left(\frac{\mu - g}{a}\right)^b}\right) \tag{5}$$

The Eq. (5) is obtained by fitting to the fitted pair of μ and σ, and thus obtaining the best fitted value for the parameters g, k, a, b. The least square method is used for all fitting of parameters.

The HEP is obtained as function of the interval states of the node "Ta-Td" using the integral in expression (6).

$$[HEP]_{t1}^{t2} = \int_{t1}^{t2} 1 - \frac{e^{\frac{(x-\mu)}{\sigma}}}{1 + e^{\frac{(x-\mu)}{\sigma}}} dx = \frac{1}{t2 - t1}\left[t - \sigma \ln\left(1 + e^{\frac{(x-\mu)}{\sigma}}\right)\right]_{t1}^{t2} \tag{6}$$

On the other hand the probability distribution for the time used by the operator to take a decision is expressed using a lognormal distribution. The mean and variance of the distribution depends on the control mode and on the complexity of the decision to be taken. This is expressed in the node called "Tplanning". Finally the node "Tp" which present as possible states the same interval of times presented by "Tplanning" assume the same value presented by "Tplanning" if no decision error occurred, otherwise it assume the last possible value presented by the list, therefore collision occurs.

The last phase of the operator task considered by the model is the execution of the manoeuvre. In this last phase the main criticality is the technical time used by the ship in order to perform the manoeuvre. The time used by the operator to manoeuvre the ship present a conditional probability table where the probability is distributed according to a lognormal distribution whose mean and standard deviation depend on the control mode. The distribution however is assumed to go no further than 3–4 min. It takes in fact into account the possible changing to manual mode if the autopilot is on, and then used the manual steering mode to give the manoeuvre rudder angle desired, or use the autopilot for getting the same aim). The ship response time is not taken into account in this node but in a different node where all the technical element contributing to varying the ship response time are considered (rudder angle needed for the manoeuvre given the situation, manoeuvrability of the ship etc.). The probability that the operator performs a wrong execution even if he made a right plan is also taken into account. It is a so called "skill based error". The error is assumed to be recoverable. The final effect of the error therefore is a delay in the T-Manoeuvring.

All the other assumptions and assessment are reported in Table 9.

Table 9 Description of the nodes involved in the operator modelling for the Bayesian Belief Network that describes collision and grounding scenarios

Object	Name	Description	Assessment	Note
Vigilance	Vigilance	This node can serve to identify the level of vigilance of the operator given certain situational conditions, a certain level of fatigue, if it is day or night and if there are elements of distraction	Expert judgment	
	Situational conditions	This node can be used to summarize the impact on the operator of the external conditions: Weather, Traffic Intensity, Area complexity	Expert judgment	
	Fatigue	The level of fatigue depends on the shift duration	Expert judgment	
	Shift duration	It can have two states and it can be used to take into account the fact that the operator may be subjected to "too" long working hours	It can be assessed in accordance with the European directive 1999/63/EC A ship that is on the register of two Member States is deemed to be registered in the State whose flag it flies. Hours of work * and rest * are laid down as follows: Either the maximum hours of work which must not exceed: – 14 h in any 24-h period – 72 h in any seven-day period The minimum hours of rest which must not be less than: – 10 h in any 24-h period – 77 h in any 7-day period	
	distraction	This node may serve to represent if there are many or few elements of distractions (phone calls etc.)	Input from outside (depends on the scenario we want to assess)	

	Traffic intensity	Traffic intensity of the area	Input from outside	
	Weather	Weather conditions can be: Good Storm Rain Heavy rain Fog	Input	
	Area complexity	Navigational complexity of the Area (high medium or low)	Input	
	Daylight	This is a Boolean node, the two possible states being Day or Night	Input	
Detection	Ergonomics	This node can be used to summarize how a certain set of elements on the bridge affect the performance	This node can be an input from the object bridge layout. It is an interval node. The intervals are the percentage by which the no surveillance probability should be decreased assigning then the value from which the no surveillance is decreased to the other two states of the node "World radar other" according to the proportion they affect the overall state already example shown in notes	The assessment starts with expert judgment on the node where the ergonomic does not contribute, and then it take into account the contribution of the ergonomic quality of the bridge. (it reduce the no surveillance probability by the percentage given by the status(value x), and increase the value of World by P(w)/[P(w)+P(r)] of this value x and Radar by P(r)/[P(w)+P(r)] of the same value x (see Fig. 7)

Table 1

Ergonomics	0 - .05	0 - .05	0 - .05
Vigilance	Low	Medium	High
Visual/audible	65	70	75
Radar/AIS	10	10	15
No surveliance	25	20	10

Table 2

Ergonomics	0 - .05	0 - .05	0 - .05
Vigilance	Low	Medium	High
Visual/audible	65.54167	70.4375	75.44118
Radar/AIS	10.08333	10.0625	15.04167
No surveliance	24.375	19.5	9.75

No surveillance in Table 2 is 25*(1-0.025)
Visual/audible in Table 2 is 65*(1+ 25*0.025/ (65+10))
Radar/AIS in Table 2 is 10*(1+ 25*0.025/ (65+10))

Calculation for the effects of ergonomics on the node World radar other

(continued)

Table 9 (continued)

Object	Name	Description	Assessment	Note
	V_scan frequency	Is the frequency with which the operator may be scanning the surface of the sea	Can be assessed assuming a normal distribution, whose mean depends on the state of the nodes: World Radar/ Other, BNWAS, View Zone	
	Time D visual	Time for visual detection used by the OOW	Every state of this node has a probability that can be evaluated assuming the exponential distribution like λe^ (−λt)(where λ is the looking frequency)	
	Ta AIS	Time available for the AIS to display the risk	Input form object scenario	
	Ta radar	Time available for the radar to display the risk	Input form object scenario	
	Ta visual	Time available for the visual detection of the risk it depends on the visibility and on the distance between the two vessels	Input form object scenario	
	view zone	There are four view zones Head, Aft, Starboard and Port. Forward is the more supervised of the four	Input from other object	
	World Radar Other	This node is used to describe how the OOW distribute its time among different tasks (looking outside, looking at the radar, doing other things)	The assessment starts with expert judgment on the node where the ergonomic does not contribute, and then it take into account the contribution of the ergonomic quality of the bridge. (it reduce the no surveillance probability by the percentage given by the status(value x), and increase the value of World by P(w)/[P(w)+P(r)] of this value x and Radar by P(r)/[P(w)+P(r)] of the same value x.	

	R_scan frequency	Scan frequency at which the operator looks a the AIS	It can be evaluated assuming a normal distribution, whose mean depends on the node World/Radar/other. The truncation of the distribution may depend on the value of the node Bridge Navigational Watch alarm system (BNWAS) thata states the maximum interval of time at the end of which the operator has to be "present and vigilant"	
	Td radar/ AIS	Time for detection using the radar or the AIS	every state of this node has a probability evaluated like $\lambda e^{\wedge}(-\lambda t)$ (λ is radar checking frequency)	
	Ta_R/A-Td_R/A	Time available for the Radar detection-Time used for detection by the operator through the Radar	the probability of each state can be given by an " if then/" comparison of the states of the two nodes Ta_r and Td_r. If the two time as are both >0 then we consider the value of the difference between the two nodes and if the difference is negative we assume a value of −0.5 which means no detection through radar/AIS)	
	Ta_v-Td_v	Time available for the visual detection-Time used for detection by the operator visually	the probability of each state can be given by an " if then" comparison of the states of the two nodes Ta_v and Td_v (same as above)	
	Ta-Td	Time available-time for detection (it will be assumed selecting the maximum time available between Ta_v-Td_v, Ta_r-Td_r Ta_A-Td_A since they are weighted by the percentage of time spent by the operator in checking outside or looking at the radar-AIS)	Maximum value between the two nodes "Ta_R/A − Td_R/A" and "Ta_v − Td_v"	

(continued)

Table 9 (continued)

Object	Name	Description	Assessment	Note
Tplanning	Mean	Mean of the distribution for T planning (normal_)	Normal distribution based on expert judgment depends on plan complexity, Control Mode. . .in the future it can be derived from experimental data	
	Variance	Variance for the distribution of T planning	Normal distribution based on expert judgment depends on plan complexity, Control Mode. . .in the future it can be derived from experimental data	
	Tplaning	Time for planning	Lognormal distribution mean and variance are given by the nodes	$\mu\ln = \log(\mu x) - 0.5\sigma^2 \ln$ $\sigma^2\ln = \log(1 + \sigma^2 x/\mu^2 x)$
	Plan complexity	Complexity of the plan to be developed it summarize some other nodes(clear give way, area complexity, traffic intensity)	Expert judgment	
	Traffic intensity	Traffic intensity of the area	Input	
	Area complexity	Navigational complexity of the Area (high medium or low)	Input	
	Clear give way situations	Unclear give way situations: Head on (alpha from 175 to 185) Being overtaken (alpha smaller than 180 and theta 1 from 107.5 to 117.5) Overtaking (alpha greater than 180 theta from 107.5 to 117.5). Where alpha and theta are described in Fig. 8	Input from the object "Scenario"	This node affect the probability of performing a wrong planning and the time used for planning
	Competence	Competence of the operator (unique indicator for year of experience and training)	Input	
	Control Mode	This node can be used to summarize the impact on the operator of the external conditions: time pressure, competence of the operator and plan complexity	Expert judgment	

	Ta-Td	Time available—time for detection (it will be assumed selecting the maximum time available between Ta_v-Td_v, Ta_r-Td_r Ta_A-Td_A since they are weighted by the percentage of time spent by the operator in checking outside or looking at the radar-AIS)	Input from other object (Detection)	
	Support for Planning	This node was intended to be used for summarizing all the quality of a bridge layout useful for supporting planning activities	Input from other object (Bridge layout)	
	Time pressure	It depends on the time value of Ta-Td it has an influence on the control mode	Derived from Ta-Td. It is used to give a qualitative indication of the presence of time pressure and how relevant it might be.	
	Wrong Planning	Probability that the operator either take no decision or take the wrong decision	It is a logit distribution (type logit) whose formula is $1 - \exp((t - \mu)/sn)/(1 + e^{((t - \mu)/sn)})$. The μ and the sigma of the logit are calibrated based on two pair of points (T, HEP). These two pairs are dependent on the given control mode state and a Plan Complexity state. $sn = -k(1 - \exp[-[(\mu - g)/a]^b)$. The formula is obtained by fitting to the fitted pair of μ and sn, and thus obtaining the best fitted value for the parameters g, k, a, b. The least square method is used for all fitting of parameters.	The pairs of (T, HEP) are currently based on Expert Judgment on all the possible combination of control mode states and Plan complexity states (9 in total)

(continued)

Table 9 (continued)

Object	Name	Description	Assessment	Note
			The HEP is obtained as function of the interval states of the node "Ta – Td" using the integral of the expression $1 - \exp((t - \mu)/sn)/(1 + e^{\wedge}((t - \mu)/sn))$, in its integrated form [HEP] $t_1 - t_2 = 1/(t2 - t1)$ [t-snln(1+exp[(t−μ)/sn]]$t_1 - t_2$	
	Tp	Time used for planning	equal to Tplanning if no wrong planning occurs otherwise it assume the last value of the time interval available (therefore collision occurs)	
	Ta-Td-Tp	Time available-time for detection-time for planning	Obtained through a comparison of the value of the difference of the values of the parent nodes	
T_manoeuvring	Operator Execution time	Time used by the operator to manoeuvre the ship (changing to manual mode if the autopilot is on, and then used the manual steering mode to give the manoeuvre rudder angle desired, or use the autopilot for getting the same aim). The ship response time is not taken into account in this node but in a different node where all the technical element contributing to varying the ship response time are considered (rudder angle needed for the manoeuvre given the situation, manoeuvrability of the ship etc.)	The time used for executing the manoeuvre is a lognormal distribution whose mean and standard deviation depend on the control mode. The distribution however is assumed to go no further than 3–4 min	
	Execution error	Probability that the operator performs a wrong execution even if he made a right plan. It is a so called "skill based error". The error is assumed to be	The node has two states only (Error or correct). The probability of an execution error is distributed according to a lognormal	

		recoverable. The final effect of the error therefore is a delay in the T-Manoeuvring	whose mean depends on the control mode. The starting value for the mean is assumed to be the one reported in the Hollnagel description of CREAM as the basic value for the execution error named "action of wrong type": 3.0 E-03	
	Operator Execution time (2)	equal to operator execution time if no execution error occurs otherwise it assume the last value of the time interval available (3–4 min)		

9 Conclusions and Way Forward

The model presented in this example tries to take into account the main elements affecting human performance in a solo watch situation considering those features that are also observable during a normal training session with the use of a bridge simulator. Thus the time to detect a ship, the time used for planning an action, the probability of taking the wrong decision the probability of performing the wrong execution of a maneuver (even if the right plan has been made) and the time for maneuvering the ship have been considered as main focuses of the operator performance in the model. The above elements are also performance indicators that are collectable from observations, as, for instance, training sessions. In this early stage the model mostly rely on the use of the Expert Judgment for identifying the main elements of performance in relation to collision scenarios, and assessing their impact. However the assessment is tailored in such a way that it would be possible in a further validation phase to incorporate real observational data. This will provide a key input for the model for evaluating in a more realistic way, the impact of different bridge layout and situations on this specific field of human performance The Model can be validated in fact by performing some experiments in a simulated training environment for different bridge layout, and assuming the availability of different equipment and different conditions, so as to observe the influence they have on the time used for detection and planning for different operators. This in turn can provide a benchmark for testing how well these factors are represented in the model. The interesting aspect here is the capacity of the model to update when new empirical data become available which is a desirable feature to allow better accuracy for human reliability analysis.

References

Colreg (1972) Convention on the international regulations for preventing collisions at sea

Cowell RG, Dawid AP, Lauritzen SL, Spiegelhalter DJ (1999) Probabilistic networks and expert systems. Springer, New York

Friis-Hansen A (2000) Bayesian networks as a decision support tool in marine applications. PhD thesis. Department of Naval Architecture and Offshore Engineering, Technical University of Denmark, December

Friis-Hansen P, Terndrup Pedersen P (1999) Risk analysis of conventional and solo watch keeping. Department of Naval Architecture and Offshore Engineering, 65 p. www.mek.dtu.dk

Galvagni R, Clementel S (1989) Risk analysis as an instrument of design. In: Cumo M, Naviglio A (eds) Safety design criteria for industrial plant. CRC Press, Boca Raton

Groth K, Wang C, Mosleh A (2010) Hybrid causal methodology and software platform for probabilistic risk assessment and safety monitoring of socio-technical systems. Reliab Eng Syst Saf 95:1276–1285

Hollnagel E, Cacciabue C (1991) Modeling cognition and erroneous actions in system simulation contexts. Paper presented at 3rd European meeting on 'Cognitive science approaches to process control,' Cardiff, 2nd–6th September

Hollnagel E (1993) Human reliability analysis: context and control. Academic, London

Hollnagel E (1998) Cognitive reliability and error analysis method CREAM. Elsevier, Oxford
Laplace PS (1819) A philosophical essay on probabilities. Wiley
Leva MC, Hansen PF, Sonne Ravn E, Lepsøe A (2006) SAFEDOR: a practical approach to model the action of an officer of the watch in collision scenarios. In: Proceedings of ESREL Conference, Estoril Portugal, Taylor & Francis Group
Lützen M, Friis-Hansen P (2003) Risk reducing effect of AIS implementation on collision risk. In: Proceedings of world maritime technology conference, 17–20 Oct 2003, San Francisco
Neisser U (1976) Cognition and reality: principles and implications of cognitive psychology. Freeman, New York
Ritter F, Shadbolt N, Elliman D, Young R, Gobet F, Baxter G (2003) Techniques for modeling human performance in synthetic environments: a supplementary review. Human Systems Information Analysis Center, Wright-Patterson Air Force Base, Dayton, OH
Swain AD, Guttmann HE (1983) Handbook on human reliability analysis with emphasis on nuclear power plant application. NUREG/CR-1278, SAND 08-0200 R X, AN
Trucco P, Cagno E, Ruggeri F, Grande O (2008) A Bayesian belief network modelling of organisational factors in risk analysis: a case study in maritime transportation. Reliab Eng Syst Saf 93(6):845–856
Wang Q, Garrity GM, Tiedje JM, Cole JR (2007) Naive bayesian classifier for rapid assignment of rRNA sequences into the new bacterial taxonomy. Appl Environ Microbiol 73:5261–5267

Maria Chiara Leva, is a Lecturer in Dublin Institute of Technology in the College of Environmental Health, she is also a visiting research Fellow in the Centre for Innovative Human systems in Trinity College Dublin. Her area of Expertise is Human factors and Safety Management Systems. Chiara holds a PhD in Human factors conferred by the Polytechnic of Milano Department of Industrial Engineering. Her PhD focused on Human and Organizational factors in Safety Critical System in Transport Sector. She has been chair of The Irish Ergonomics Society and has been working in Ergonomics and Risk Assessment as a consultant since 2008. More than 56 publications on Human Factors, Operational Risk Assessment and Safety Management in Science and Engineering Journals. Researchgate profile: http://www.researchgate.net/profile/Maria_LevaGoogle Scholar: http://scholar.google.com/citations?user=tTUXwI8AAAAJ&hl=en

Peter Friis Hensen, works at Det Norske Veritas in Oslo. He was Associate Professor, Department of Naval Architecture and Offshore Engineering of Technical University of Denmark. He contributed to several project such as "Risk Management of Climate Extremes in an Urban Environment". His research interests include risk analysis, reliability and safety.

A Methodology to Support Decision Making and Effective Human Reliability Methods in Aviation Safety

Pietro Carlo Cacciabue and Italo Oddone

Abstract This Chapter shows firstly a practical way to support Risk Informed Decision Making processes. The approach, discussed only in abstract and theoretical terms, shows that it is possible to develop practical instruments supporting the safety analysts in presenting overall results of the risk analysis process to the decision makers in a way highlights the effectiveness of safety measures and their efficiency with respect to cost benefit. The second part of this Chapter evaluates four different and well established Human Reliability methods, with the aim to assess their differences and ability to cope with aviation procedures. The comparison of results of applying the methods to two aviation case studies shows advantages and drawbacks in the implementation of each method. It has not been possible to come to a conclusive assessment of the ability of the methods to cope with aviation issues, as a much more extensive process is necessary to carry out an accurate revision of existing data.

Keywords Aviation safety • Safety management system • Risk analysis • Management of change

1 Introduction

Risk Analysis (RA) and Human Reliability (HR) are recognised as the most important and variable contributor to safety assessment of modern technological systems. The normative requirement, in many different domains and in particular in Aviation (FAA 2010; EC 2012; EASA 2012), to implement Safety Management Systems (Stolzer et al. 2010; ICAO 2012) based on RA and HR has led to the necessity of many organisations to apply techniques enabling the evaluation of probability of hazards and assessment of the associated consequences in a fast and consistent manner.

P.C. Cacciabue (✉)
Faculty of Science, Engineering and Computing, Kingston University, London, UK
e-mail: P.Cacciabue@kingston.ac.uk

I. Oddone
Dipartimento di Ingegneria Aerospaziale, Politecnico Milano, Milano, Italy
e-mail: italo.oddone@polimi.it

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_9

This is necessary for both types of analysis that sustain a SMS, namely:

(a) Prospective approaches, for the predictive evaluation of risks that may be encountered when new developments are planned or when changes occur in an organisation; or
(b) Retrospective analyses, for the evaluation of the root causes of actually encountered occurrences and for assessing, on a risk base, whether an organisation can still operate within acceptable safety margins.

Although the two types of assessments, i.e., prospective and retrospective studies, aim at different goals, the methods that are utilised must be strictly correlated in order to ensure appropriate and logical data transfer and sharing of results from one approach to the other. What changes is only the way in which the methods are applied and the outcomes are utilised and filtered for safety analysis.

With respect to RA methods and techniques, the implementation of classical and standardised approaches, such as Fault Trees (FTs) and Event Trees (ETs) remains the most valuable way to assess risk (Roland and Moriarty 1990); Andrews and Moss 1993). However, the complexity and time necessary to implement a combined FT/ET methodology and the difficulty to identify adequate data for their implementation has favoured the application of much more agile and fast approaches essentially based on Expert Judgement (EJ). The Bow-Tie methodology (Bow-Tie 2013) has emerged as the most popular and utilised approach. The Bow-Tie approach, based on the Cause Consequence Analysis approach developed in the 1970s (Nielsen 1971), enables the user, i.e., the safety analyst, to apply the most appropriate method for the safety case under study. Consequently, the various steps of the Bow-Tie are not necessarily associated to EJ evaluations but can be carried out using whichever model or technique assumed appropriate by the user. Therefore, within a Bow-Tie analysis, it is possible to consider different and detailed methods, such as FTs and EVs, as well as more direct approaches like EJ. In the Aviation domain, the methodology that is strictly related to the Bow-Tie is ARMS (ARMS 2011), which enables the performance of both prospective and retrospective approaches with two different methods, namely SIRA (Safety Issue Risk Assessment) for prospective analysis, and ERC (Event Risk Classification) for retrospective analysis. ARMS is strictly based on only the use of the safety annalist's EJ.

An issue that remains open is the way to present integrated results of the complex and vast RA process to the decision makers, so as to enable the selection of measures and safeguards that are manageable and sustainable for the organisation. This chapter aims primarily at tackling this open issue with respect to RA and Safety Management System.

With respect to HR, the complexity of systems and the extensive use of automation have been the major contributors to enhance the relevance of human error to incidents and accidents in almost all technologically advanced domains. Because of this aspect and the need to perform safety studies in relation to SMS and design of new technologies, the key issue emerged in research in the years 1980s and 1990s has been the need to develop methods and techniques enabling (Humphreys 1988):

(a) To assess in quantitative terms the probability of errors for prospective studies associated to Probabilistic Risk and Safety Assessment (PRA, PSA); and
(b) To describe, in a formal and structured way the causes and interplay of human activity with the overall environment for retrospective analysis.

The HR area has evolved and generated a vast variety of methods, similarly and even more extensively than the domain of RA, aimed at supporting the assessment of probability and the identification of the causes of human error. The use of EJ has been utilised in many methods, especially in the domain of Nuclear Energy and Petrochemical production, based on a large resources of data and incident analysis (Lyons et al. 2005; Bell and Holroyd 2009). More complex and articulated method, based on theoretical approaches such as Task Analysis (TA) and Cognitive Models (CMs) have been developed (Kirwan 1994; Hollnagel 1998; Cacciabue 2004; Salvendy 2006). As in the case of RA also for HR the use of articulated methods is difficult and time consuming, whereas the methods based on EJ are rapid and relatively simply to utilise.

The alternative implementation of complex and detailed methods for RA and HR or of rapid and simple approaches based on EJ is govern by the resources available to the safety team performing the study. This is primarily associated to the availability of a good body of data and of a consolidated knowledge of the selected methods.

Obviously, the methods based on EJ are faster and simpler to apply than complex methods. On the other side, complex and articulated methods enable the detailed structuring of tasks and processes to be analysed and the selection of the specific steps that require in-depth analysis. However, the reliability and quality of the results of the safety analysis is not necessarily better when complex methods are utilised, as data and inadequate knowledge may strongly affect the overall analysis. Simple methods present the enormous advantage of being fast and enable a rapid assessment of the impact on safety of the hazards and human errors that are analysed. Recently, the most commonly utilised methods have been studied and compared in order to evaluate their capability to cope with modern issues, such as security (Kierzkowski and Kisiel 2015; Castiglia et al. 2015).

The second main goal of this chapter is associated to supporting the analyst in the identification and selection of the most appropriate HR method to implement for the safety case at hand.

In general, for both RA and HR, the following set of rules can be implemented for maintaining a conservative perspective and according to a "safety first principle":

1. If a rich and validated body of data and information are available about the system, HMI and safety case under development, then the use of simple methods may be the best way forward for an initial assessment of safety.
2. This first step is considered sufficient in many cases, also in relation to the other safety cases and area of analysis associated to a Safety Management System.
3. On the other hand, when a simple method shows obvious inconstancies or when a more precise analysis is deemed necessary, then a second iteration of the safety study can be performed, primarily on the tasks and processes that are deemed more relevant for the whole safety case.

This chapter will initially discuss a practical implementation of the Bow-Tie methodology called RAMCOP (Risk Assessment Methodology for Company Operational Processes). In particular, the way to present the overall results to the decision makers for the final selection of what should or should not be implemented is discussed. Then, focusing on HR, a number of well known simple methods based on EJ is revised for implementation in the domain of Aviation. In particular, some safety cases are discussed with the goal of evaluating the applicability of the methods to the domain of Aviation, especially for what concerns the empirical parameters utilised to evaluate the probability of errors of operators. In this way the need for more data analysis and improvement of the databased of the simple methods is assessed and discussed.

2 An Integrated Safety Methodology for Decision Making

2.1 The Role of Risk Informed Decision Making

The safety process of complex systems is governed by risk analysis and the decision making of top management is associated to what is nowadays called Risk Informed Decision Making (RIDM) (Ersdal and Aven 2008). The RIDM process has been proposed primarily in the domain of Nuclear Energy production at the end of the 1990s in the US (NRC 1995, 1998, 2002, 2003, 2009) and more recently at International level (IAEA 2005, 2011). In more recent years, NASA proposed the RIDM approach in a very extensive and detailed handbook (NASA 2010) comprehensive of all methods and techniques that can be utilised to carry out a risk based safety assessment at different level of accuracy and depth.

The RIDM must be based on a body of information and results obtained by what is usually implemented in a Safety Management System (SMS). SMS characterises the stages prior the starting of operations, i.e., at design and implementation of a systems, as well as the processes associated to the entire life of an organisation. In general, a SMS implies the performance of *prospective* and *retrospective* analyses when changes occur, as the organisation evolves in time, and when unexpected and unwanted events occur during operational processes. Moreover, a SMS covers the routine implementation of *safety audits* and the plans for managing *emergencies* and *security*.

The SMS enables the "living" appraisal of the safety state of an organisation and is applied very frequently and repeatedly with different perspectives. Consequently, it must be "agile", so as to adapt easily and rapidly to the specific goals of the intended analysis, and very "user friendly", so as to be applied by the safety analyst with simple and rapid steps.

The principal "actor" of a SMS is the safety manager of an organisation, supported by the safety team. The prime "recipient" of an SMS is the CEO and top management of an organisation expected to make the final decision about which measure should be implemented in order to preserve safe, effective and efficient operations. The analyses performed at Risk Assessment level aim at identifying the safety state of an

organisation with respect to various hazards and associated barriers and safeguards that can be put into operations in order to minimise and contain the risks derived from the encounter of the hazards or undesired operational states. The process of risk informed decision making follows the risk assessment and aims at selecting the actual implementation of barriers on a cost/benefit principle.

Various methodologies exist to formalise a risk informed decision making and risk assessment process. The Bow-Tie and ARMS are two well-known and established methodologies usually proposed for the implementation of SMS in the aviation domain. The Bow-Tie is easy to understand and enables a rapid development of a risk assessment, at qualitative level. The idea is to combine causes and consequences associated to an initiating event, which is similar to the Event Tree (ET) process. The quantification process requires the implementation of techniques that consider data and possibly fault assessment processes such as Fault Trees (FTs). The Bow-Tie Methodology can be considered an evolutionary step of the Cause-Consequences diagrams (Nielsen 1971). The use of Expert Judgement (EJ) can be exploited as part of the methodology for the systematic identification of threats, hazards and recovery measures.

ARMS (Aviation Risk Management Solutions) is a much more recent methodology (ARMS 2011) that tackles both retrospective and prospective operational risk assessment by means of the "Event Risk Classification" (ERC) and the "Safety Issue Risk Assessment" (SIRA). ARMS is only based on Expert Judgement and requires a vast experience in order to consistently evaluate risk and acceptability level.

Both methodologies, Bow-Tie and ARMS, enable the assessment of risk, but do not offer guidance for the decision making process. In other words, they are only appropriate and supportive for the first part of the RIDM process described above.

The RAMCOP (Risk Analysis Methodology for Company Operational Processes) is a methodological approach that aims at supporting the RIDM process and the implementation of different methods and models according to the need (Cacciabue et al. 2015). The outcome of applying RAMCOP can be summarised in a specific table, called Overall Risk Assessment Table (ORAT), that offers and overview of all risks associated to the hazards selected for safety study. The ORAT table can be further elaborated combining risk and cost benefit analyses for the ultimate selection of the decision makers into what may be Risk Informed Decision Making Table (RIDMT). The following sections of this chapter will discuss the process of implementation of the RAMCOP methodology and the generation of the associated ORAT and RIDMT tables.

2.2 Short Description of RAMCOP-ORAT

2.2.1 The Risk Analysis Methodology for Company Operational Processes

The RAMCOP methodology consists of a simple and straightforward approach for implementing the prerequisites of safety management systems and overall risk assessment of a plant or organisation.

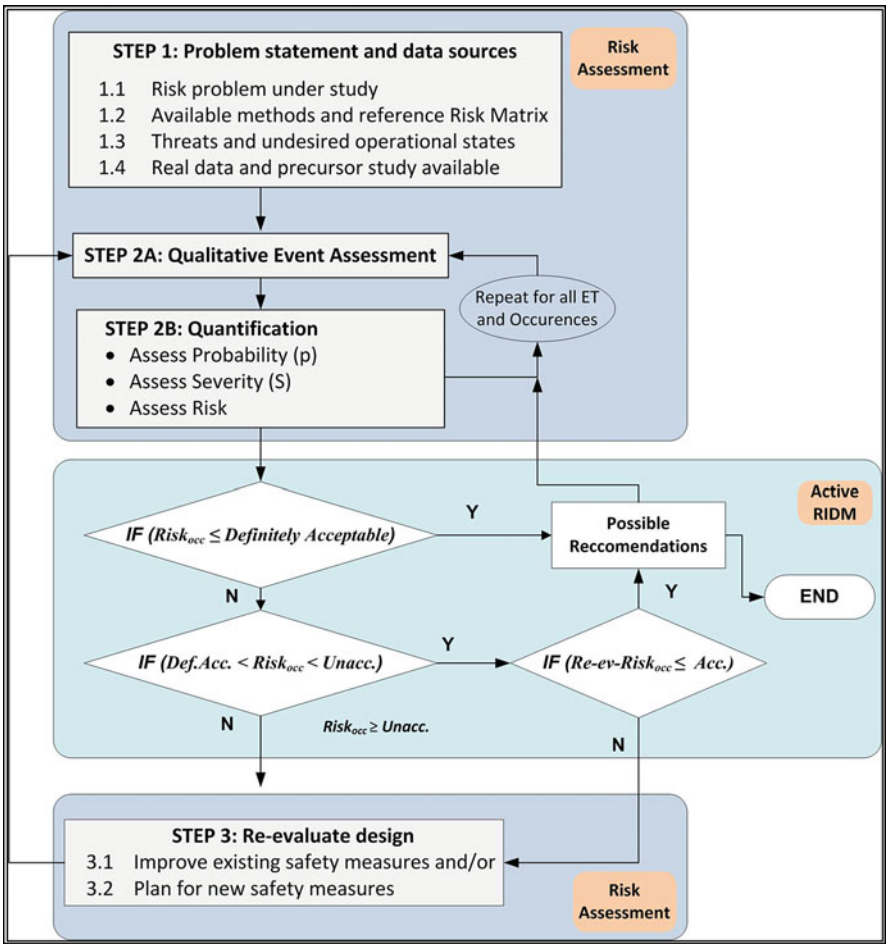


Fig. 1 Risk Assessment Methodology for Company Operational Processes—flow chart adapted from Cacciabue et al. (2015)

The methodology, initially developed as research approach (De Grandis et al. 2012) has been further formalised to support an organisation to respond to the needs of developing and maintain appropriate safety standard especially when changes occur within the organisation (Cacciabue et al. 2015) (Fig. 1). It contains three steps of Risk Assessment (RA) and a phase of Risk Informed Decision Making (RIDM). The three steps of RA are:

1. Develop the case with reference to knowledge and data;
2. Conduct a complete qualitative and quantitative Risk Assessment;
3. Revise design and revaluate safety.

The RIDM is the formal process that leads decision makers to select the most appropriate and acceptable actions and safety measure to implement.

In essence, Step 1, "Problem statement and data sources" implies the preparation and search for all necessary information, data and material that can support the analysis. In particular, the selection of available methods and models and the definition of the reference risk matrix are essential. Also the documentation and practical information about tasks and performances expected by the human operators involved needs to be known. Finally, the documentation and databases relative to past events and occurrences are necessary.

In Step 2, the detailed process of risk assessment is carried out by analysing each hazards, selected in Step 1, from a qualitative and quantitative perspective. This process, of risk analysis can be done utilising the methods and approaches selected according to the accuracy that the safety analyst considers necessary. This implies that different methods can be selected and applied, from simple Expert Judgement to a more complete combinations of Event Tree—Fault Tree.

Step 3 is implemented only when the Risk Informed Decision Making process ends with the need to revise the design and to implement relevant changes that expand the safeguards and barriers against the consequences of hazards. This implies that a further risk assessment process is carried out.

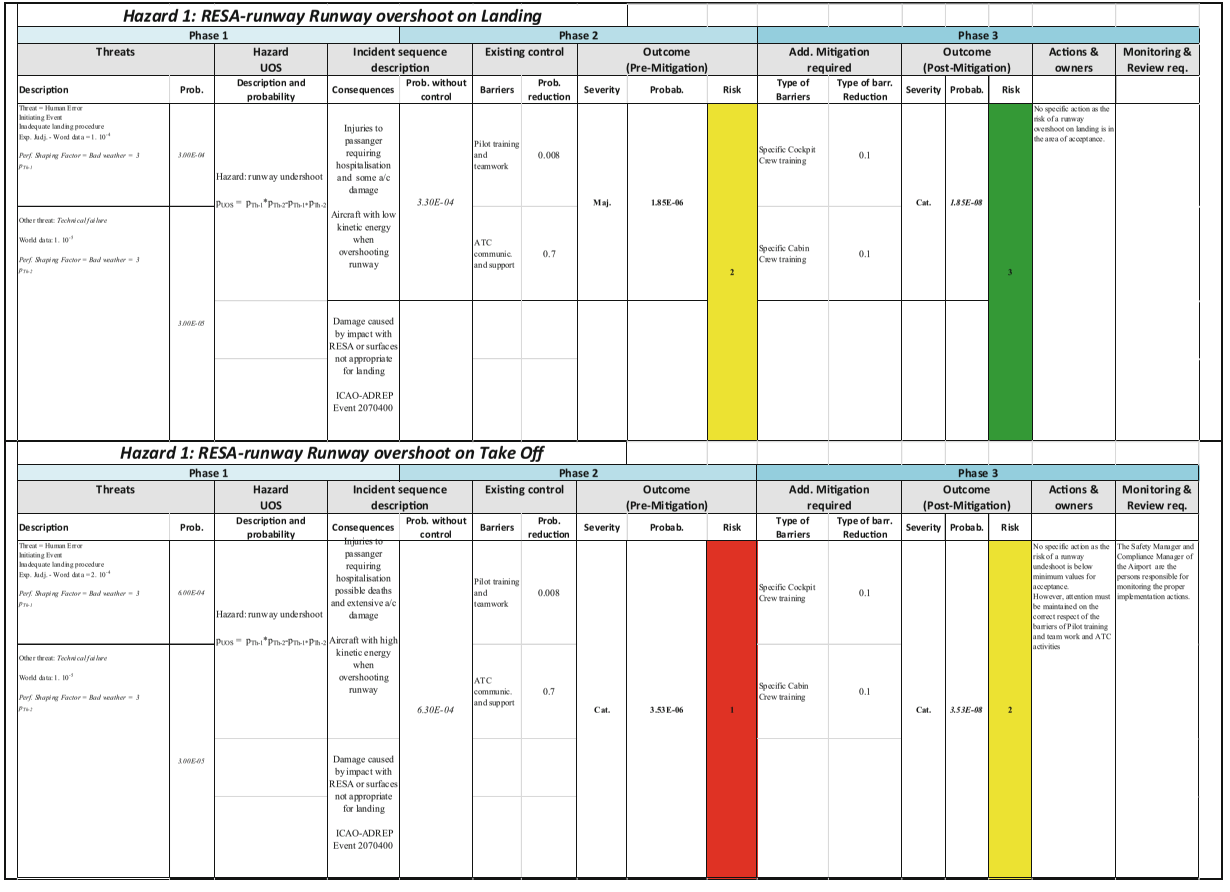
The RIDM process implies that:

1. When all risks are acceptable ($Risk_{occ} \leq Acceptable$), the risk analysis is completed. Recommendations are developed as final stage.
   Before reaching this final stage,
2. It is necessary to deal with the unacceptable risks ($Risk_{occ} \geq Unacceptable$), by re-evaluating design and safety measures and introducing new barriers in order to further reduce risks and reach the acceptable levels of risk.
3. The most important step of RIDM occurs when risks reside between the totally unacceptable and acceptable level ($Acceptable < Risk_{occ} < Unacceptable$). This intermediate area requires the decision of whether or not to accept the assessed risks of occurrence.

2.2.2 Overall Risk Assessment Table

During the implementation of the RAMCOP approach in relation to a multiple hazards analysis, a variety of risks evaluations are carried out associated to the different hazards being analysed. In practice, it is possible to gradually fill an *Overall Risk Assessment Table* (ORAT) that contains the key elements of the analysis and represents the practical implementation of the methods and models implemented in order to carry out each specific risk analysis.

The ORAT table enables the safety analyst to obtain an overview of the entire set of hazards and barriers analysed during the RAMCOP process (Fig. 2).



Hazard 1: RESA-runway Runway overshoot on Landing

Phase 1				Phase 2					Phase 3						
Threats		Hazard UOS	Incident sequence description	Existing control		Outcome (Pre-Mitigation)			Add. Mitigation required		Outcome (Post-Mitigation)			Actions & owners	Monitoring & Review req.
Description	Prob.	Description and probability	Consequences	Prob. without control	Barriers	Prob. reduction	Severity	Probab.	Risk	Type of Barriers	Type of barr. Reduction	Severity	Probab.	Risk		
Threat = Human Error Initiating Event Inadequate landing procedure Esp. Judg. - Word data = 1. 10^{-4} *Perf. Shaping Factor = Bad weather = 3* P_{Th-1}	3.00E-04	Hazard: runway undershoot $P_{UOS} = P_{Th-1} * P_{Th-2} * P_{Th-1} * P_{Th-2}$	Injuries to passanger requiring hospitalisation and some a/c damage Aircraft with low kinetic energy when overshooting runway	*3.30E-04*	Pilot training and teamwork	0.008	**Maj.**	**1.85E-06**	2	Specific Cockpit Crew training	0.1	**Cat.**	***1.85E-08***	3	No specific action as the risk of a runway overshoot on landing is in the area of acceptance.	
Other threat: *Technical failure* World data: 1. 10^{-3} *Perf. Shaping Factor = Bad weather = 3* P_{Th-1}					ATC communic. and support	0.7				Specific Cabin Crew training	0.1					
	3.00E-05		Damage caused by impact with RESA or surfaces not appropriate for landing ICAO-ADREP Event 2070400													

Hazard 1: RESA-runway Runway overshoot on Take Off

Phase 1				Phase 2					Phase 3						
Threats		Hazard UOS	Incident sequence description	Existing control		Outcome (Pre-Mitigation)			Add. Mitigation required		Outcome (Post-Mitigation)			Actions & owners	Monitoring & Review req.
Description	Prob.	Description and probability	Consequences	Prob. without control	Barriers	Prob. reduction	Severity	Probab.	Risk	Type of Barriers	Type of barr. Reduction	Severity	Probab.	Risk		
Threat = Human Error Initiating Event Inadequate landing procedure Esp. Judg. - Word data = 2. 10^{-4} *Perf. Shaping Factor = Bad weather = 3* P_{Th-1}	6.00E-04	Hazard: runway undershoot $P_{UOS} = P_{Th-1} * P_{Th-2} * P_{Th-1} * P_{Th-2}$	Injuries to passanger requiring hospitalisation possible deaths and extensive a/c damage Aircraft with high kinetic energy when overshooting runway	*6.30E-04*	Pilot training and teamwork	0.008	**Cat.**	**3.53E-06**	1	Specific Cockpit Crew training	0.1	**Cat.**	***3.53E-08***	2	No specific action as the risk of a runway undeshoot is below minimum values for acceptance. However, attention must be maintained on the correct respect of the barriers of Pilot training and team work and ATC activities	The Safety Manager and Compliance Manager of the Airport are the person responsible for monitoring the proper implementation actions.
Other threat: *Technical failure* World data: 1. 10^{-3} *Perf. Shaping Factor = Bad weather = 3* P_{Th-1}					ATC communic. and support	0.7				Specific Cabin Crew training	0.1					
	3.00E-05		Damage caused by impact with RESA or surfaces not appropriate for landing ICAO-ADREP Event 2070400													

Fig. 2 The Overall Risk Assessment Table (ORAT)

2.3 Integrated Risk Analysis Results for Risk Based Decision Making

The implementation of a risk analysis process is usually associated to the overall design of a system/plant or to important changes planned for improving or modifying an organisation. In these cases, the Rias Analysis covers a variety of hazards defined and selected at qualitative level and then calculated according to a process such as RAMCOP.

In many circumstances, new barriers and safeguards are defined and selected to ensure acceptance of the risks associated to hazards and consequences. Barriers are of different nature, as they can represent a physical or a functional obstacle to the evolution of the sequences, or aim at improving behaviours, regulations and standards for limiting the possibility of incidental evolution. Moreover, barriers can be developed simply aimed at improving the general safety culture of an organisation (Hollnagel 2004).

From the decision-making perspective, it is essential to present a general picture to the highest level of management of an organisation to enable a choice of improvements and barriers that enhance the impact of the barriers on safety while fitting within a cost-benefit acceptance process. It is important to present the overall integrated effect of all barriers defined before selection. A typical example of the goal that can be achieved in this process is to enable the evaluation of the effective protection offered by a specific barriers that may affect different hazards, thus reducing the overall cost benefit perspective of that specific barrier.

In order to enable a RIDM process the ORAT table needs a further step of development. In particular, it is necessary that all assessed hazards and associated barriers are presented in a single frame that offers an overall picture of the impact of each barrier and of the relevant cost/benefit ratio.

Figure 3 shows a generic Risk Informed Decision Making Table (RIDMT) that summarises the results of the RAMCOP-ORAT analysis. It includes a number of results and data that support the selection of which barrier implement, namely:

1. The pre-mitigation information with likelihood and risk level.
2. The barriers that can be implemented and the severity achieved after implementation. It is noticeable that, as most barriers are of "causal" nature, i.e. they aim at reducing the probability of occurrence as opposed to "consequential" nature aiming at reducing the severity, the overall reduction is on the likelihood rather than the severity.
3. The resulting risk level after the implementation of the barrier.
4. The actual cost of implementation of the barriers.

Figure 4 shows an hypothetical example of a further step of combination of results. In particular, in the left end side of the figure enables to evaluate the effect that can be obtained by combining different barriers and their associated cost. In this case, the minimum cost of implementation, barriers B2, B3 and B4, leads to all

Pre-mitigation					Post-mitigation				
Hazard	Severity	Barrier	Like.	Risk level	Barrier	Severity	Lakelihood	Risk level	Cost K$
H1	High - 4/5	Existing Barriers	p_{H1}	RED	B2	High	$p_{H1,B2}$	RED	10
					B3	High	$p_{H1,B3}$	YELLOW	30
					B2, B3	High	$p_{H1,B2,B3}$	YELLOW	40
					B4	High	$p_{H1,B4}$	YELLOW	50
					B2, B3, B4	High	$p_{H1,B2,B3,B4}$	GREEN	90
					B3, B4	High	$p_{H1,B3,B4}$	YELLOW	80
					....	.....	.....	....	...
H2	Catastr. - 5/5	Existing Barriers	p_{H2}	RED	B5	Catastr.	$p_{H2,B6}$	YELLOW	100
					B6	Catastr.	$p_{H2,B6}$	YELLOW	70
					B4	Catastr.	$p_{H2,B4}$	YELLOW	50
					B6, B4	Very High	$p_{H2,B4,B6}$	GREEN	120
					....	.....	.....	....	.....
H3	Major	Existing Barriers	p_{H3}	YELLOW	B5	Major	$p_{H3,B5}$	GREEN	100
					B3, B2	Major	$p_{H3,B3}$	YELLOW	40
					B6, B4	Major	$p_{H3,B4,B6}$	GREEN	120
					....	.....	.....	....	

Fig. 3 Generic form of a Risk Informed Decision Making Table

Means to reduce all Hazards		H1	H2	H3		φ of barriers		K$	
Barrires	Cost					Barrier	N. of app.	Cost	Cost/ Benefit
B2, B3, B4	90	YELLOW	YELLOW	YELLOW		B2	4	10	2.50
B2, B3, B6	110	YELLOW	YELLOW	YELLOW		B3	5	30	6.00
B5, B3	130	YELLOW	YELLOW	GREEN		B4	6	50	8.33
B4, B6	150	YELLOW	GREEN	GREEN		B5	2	100	50.00
B2, B3, B4, B6	160	GREEN	GREEN	GREEN		B6	3	70	23.33

Fig. 4 Combination of barriers for RIDM

Hazards being controlled with consequences in the "yellow" area of the risk, i.e., risk that can be accepted after consideration of acceptance. The highest cost and safety level is obtained when combining barriers B2, B3, B4 and B6, with the overall result leading to all sequences being in the "green" area of the Risk matrix, i.e., acceptable. Other intermediate levels of safety levels and cost can be identified when different combination of barriers are considered.

The right end side of the figure shows a very simple cost benefit analysis based on the frequency of encounter of the barriers with respect to the hazards being analysed.

3 Human Reliability Methods for Aviation Safety Analysis

The assessment and contribution of human factors (HF) to risk analysis is one of the most important issues to be resolved when performing a risk analysis.

The variety of existing models and taxonomies used to carry out Human Reliability Analysis (HRA) and human error does not represent a favourable condition, as the user needs to select the most appropriate technique for the case under consideration. A variety of methods are recognised and identified by the safety authorities as valuable and usable for HRA. Most of these are based on Exert Judgement. The aim of this section is to revise the effectiveness of some of these methods to describe and calculate probabilities of erroneous performances and execution of activities and tasks, including those strongly associated to cognitive aspects. This aspect is particularly important given the major role of automation and human decision making with respect to execution of actions.

In next section, four existing methods recognised by the Civil Aviation Authorities, including the European Aviation Safety Agency and the US-Federal Aviation Administration will be studied in detail and their detailed structures and process of implementation will be assessed. In particular, as these methods have been developed primarily with respect to domains such as process plants, nuclear energy production and petrochemical plants, the ability of these models to account for the human error probabilities in the domain of aviation will be assessed.

The methods that will be evaluated are: THERP, HEART, TESEO and HCR (Swain and Guttmann 1983; Williams 1988; Bello and Colombari 1980; Spurgin 2010). Each method will be briefly described and then they will be compared in terms of user-friendliness and accuracy in the implementation of a real case study. For a more accurate description of the models and their actual implementation and correlations, the literature is very rich of fully developed and accurate description (NEA-CSNI 1998).

3.1 Description of THERP TESEO, HEART, and HCR and Issues for Aviation

3.1.1 Technique for Human Error Rate Prediction: THERP

The THERP model and technique is the first and most utilised approach to tackle human factors form a risk analysis perspective (Swain and Guttmann 1983).

It is based on the concepts of task performance according to procedures and human error types of commission, essentially errors made due to lack of knowledge and understanding of the systems/environment, and errors of omission, i.e., typical jumps of specific actions in the procedural process of task implementation.

The method is structured according to the construction of the procedure under study according to an "event-tree-like" process. In other words, assuming that every action associated of the procedure can be performed in a binary way, either successfully or erroneously, a human error tree is built that accounts for the sequence of successfully and/or erroneously performed actions.

The result is a combination that may lead to success or failure of the entire process.

The probability of performing erroneously each action is assessed, considering the "Nominal Human Error Probability—NHEP" and the boundary conditions of environmental affects ("Performance Shaping Factors—PSF") and the dependencies between actions. Consequently, due to the assumption of binary alternative between success and failure, the probability of performing each action successfully is also known.

The NHEP and the correlations that account for the PSF and dependencies are also defined in the THERP manual. This enables the user to carry out a complete analysis of HRA once the tasks are well defined and studied by the analyst.

In particular, the database associated to NHEP represents a very rich set of data that are focused on the authors' experience in the domain of nuclear energy production. In essence, THERP is a combination of a structured approached for representing a task in a procedure like sequence and a set of data based on expert judgement and field observations.

3.1.2 Human Cognitive Reliability: HCR

The HCR method has been developed in the 1980s (Hannaman et al. 1984; Spurgin 2010) in order to account for the models of cognition that were becoming popular in those days. These models were focused on the mental processes leading to the actual behaviour of human beings and their most known approach was the so called SRK model (Rasmussen 1983). This model assumed that human behavioural performance was the result of a process and interaction between different human cognitive functions, such as perception, interpretation planning. This cognitive process can be performed at "Skill" based level, i.e., when actions are carried out as an automatic response to certain stimuli, at "Rule" based level, when actions are the results of the implementation of well-known rules and regulations, or at "Knowledge" based level, when actions are the results of an elaborated cognitive process of reasoning on the perceived stimuli and basic knowledge about the system under control.

The HRC model is based on the assumption that human performance is the result of a typical SRK based behaviour. The authors collected an enormous amount of data, mainly in the domain of nuclear energy production, about task performance of power plant operators of different level of experience and expertise and then studied the results dividing behaviour of the operators in the three categories of S-R-K behaviour. The results were then fitted with a specific correlation that enabled to associate human reliability, or the probability of failing to perform correctly a certain task, with the time available, normalised with respect to the standard expected performance, vs. the type of behaviour, either Skill, Rule or Knowledge of the operators under assessment.

In more recent time (Sun et al. 2011) the HRC model has been applied to aviation domain.

The HRC model is then fully based on empirical data, derived primarily from the nuclear energy production and expert judgement.

3.1.3 Human Error Assessment and Reduction Technique: HEART

HEART is a method used to evaluate the probability of human errors happening during the accomplishment of a particular task. The method is based on Expert Judgment and the user is guided to select the most appropriate coefficients to evaluate the probability of failing to perform an action as well as an entire task.

HEART was initially introduced in the 1980s (Williams 1985, 1988), whilst he was employed by the Central Electricity Generating Board. The method is designed to be a swift and straightforward technique, based on human performance literature, that is suited to any circumstance or industry where human reliability is significant. HEART is currently being utilised in the chemical industry.

The first step is to categorise the task, in terms of its generic human unreliability, into one of the eight generic HEART task types, known as the Generic Task Unreliability. Next, the Error Producing Conditions (EPC) appropriate to the situation under analysis is identified, which may negatively affect performance. Each EPC has a corresponding multiplier, which will result in the maximum predicted nominal amount by which unreliability may increase. The next step is to approximate the influence of each EPC on the task, based on judgement. This will give the proportion of effect, which is a value between 0 and 1. The subsequent step is to work out the assessed impact value, by calculating the assessed impact for each EPC. The final step is to determine the total probability of failure of the work, by multiplying the EPC for all Assessed impacts.

3.1.4 Tecnica Empirica Stima Errori Operatori: TESEO

TESEO, developed in the 1980s (Bello and Colombari 1980) is a HRA method that assesses the likelihood of human error happening during the whole of the fulfilment of a particular task. Thee TESEO technique is currently utilised in the petrochemical industry.

Measures can be taken from such analysis to reduce the probability of an error happening within a system, which consequently leads to an advancement in the general safety levels. TESEO predicts the human reliability values using five main factors, which are:

K1—The type of task executed;
K2—The time available to the operator to complete the task;
K3—The operator's level of experience/characteristics;
K4—The operator's state of mind;
K5—The environmental and ergonomic conditions prevalent.

The general human error probability (HEP) may be computed by using these figures with this formula:

$$\mathrm{HEP} = \mathrm{K1} \times \mathrm{K2} \times \mathrm{K3} \times \mathrm{K4} \times \mathrm{K5}$$

Specific values of all the functions above have been published in a set tables that take account for the process by which the HEP is derived.

3.1.5 HRA Approaches and Aviation

The domain of aviation, in simple terms, is a very highly proceduralised environment with a strong interaction amongst humans, i.e., pilots, crew members, air traffic control etc. and between pilots and automation according to a complex and very important interaction.

The cognitive aspect of human behaviour are absolutely important and can not be neglected, especially because the mental and decision making process leading to the selection of certain procedures, carried out by the automation, is the primary source of errors and hazard generation.

Another essential element of the human-machine interaction in aviation is the time response. The time intervals are much longer than those for example of the automotive environment especially when the cockpit is involved. As an example the time response in terms of "time to collision" in the case of the Traffic Collision Avoidance System are of the order of 10s of seconds, whereas in the automotive environment these are of one order of magnitude smaller. Moreover, when the airport environment is involved the timing of operations is extremely distributed, from few seconds, as in the case of runway crossing, to several minutes when airport operations are involved, such as runway change.

Certainly, the issues of cognitive aspects and time intervals affecting behaviour are essential in the assessment of human errors and HRA. The selection of the four methods for the evaluation of Human Reliability comparison exercise that follows is based on their peculiarities of attention of the two issues of cognitive behaviour and time related activities.

The fact that aviation presents important cognitive issues and is very dependent on the time response, as discussed above, has lead to the selection of these models as the most appropriate ones for implementing HRA in the aviation domain, as they are focused on the same aspects.

On the other side, the domains of application that are typical for these models and their databases are quite different than the aviation domain and consequently it is important to assess whether the databases and their empirical correlations and coefficients are still valid in the aviation domain.

The comparison and extension of these models has been performed by several authors, mainly with the aim of exploring the implementation of specific techniques, such as fuzzy set theory, to expand their validity and their databases (Dhillon 2014). In this paper the models and their databases are applied according to the formal procedure and correlation. No extension are introduced, as the goal of the comparison is to assess whether the methods are able to cope with the domain of aviation or if they need some form of update and expansion, primarily with respect to their databases, that enables them to be applied to aviation.

4 Case Studies

The selected methods have been applied to two different case studies associated to the aviation domain. The goal of the comparison is to consider two types of tasks, i.e., a short and rapidly performed task in response to an alarm requiring immediate response and a longer and more complex task requiring the namely:

1. The response of the pilots to the alarms generated by the Enhanced Ground Proximity Warning System (EGPWS). This is a single or at least a simple sequence of actions in response to an important alarm generated by the on-board protection system, requiring immediate actions of flight management.
2. The Runway change procedure operated by airport staff when the orientation of the runway in use is inverted for meteorological or traffic management reasons. This is an articulated process composed of several steps and completed in a period of time of a certain length, much longer than the case of the EGPWS.

The two systems and tasks/procedures involved are firstly described and then the three human reliability methods are applied separately and compared.

4.1 Case Study 1: Enhanced Ground Proximity Warning System

The Enhanced Ground Proximity Warning System (EGPWS) is a system developed in order to warn pilots when their aircraft may be in urgent danger of crashing into the ground, or flying into an obstacle.

The system uses a radar altimeter to check the clearance above terrain and rate of descent information. These readings are then monitored by a system showing trends, which will indicate to the flight crew via visual and audio signals when the aircraft is in certain defined flying modes. In general, an EGPWS system has usually seven modes:

Mode 1. "Excessive Descent Rate" alerts the flight crew of an excessive descent rate, when the aircraft is near the ground. The EGPWS firstly monitors the flight profile when the aircraft is $<$2000 feet above the ground. Should an excessive rate of descent be recorded, a warning light would flash on combined by a voice warning "Sinkrate". If the rate of descent doesn't stop, or gets worse, when the aircraft's altitude becomes within 1000 feet of terrain, a continuous "Pull Up" voice alert would be announced.

Mode 2. "Excessive Terrain Closure" alerts the crew when excessive terrain closure rates are recorded. This mode uses radar altitude, airspeed, and the rate of descent. The EGPWS compares the ground below the aircraft to the flight path. If ground rises substantially within 2000 feet of the aircraft and a risk of excessive closure rate is evaluated, a warning light and a voice warning "Terrain

Mode	Action	*Calls*	Hight/dist. Ft	Standard avail. t. Sec
1	Excess. Desc. Rate	*Sinkrate*	2,000	60
2	Excess. Terrain Closure	*Pull Up*	1,000	30
		Terrain Terrain	2,000	60
		Pull up	1,000	30
3	Unsafe terr. Clearence	*Too Low Terrain*	1,000	86
		Too Low Gear	500	42

Fig. 5 EGPWS modes studied in this chapter

Terrain" are firstly generated. If the closure rate doesn't stop, or gets worse, when terrain closure reaches 1000 feet, the voice alert will alter changes to a continuous "Pull Up" call until the ground is further away.

Mode 3. "Altitude loss after take-off" provides a warning to the flight crew of inadvertent descents, or during any missed approaches.

Mode 4. "Unsafe Terrain Clearance" provides minimum terrain clearance protection in all stages of the flight. The EGPWS warns the crew regarding insufficient ground clearance based on aircraft configuration, altitude, airspeed, and rate of descent. If the aircraft breaches a floor of 1000 feet above ground the flight, the EGPWS warning light and voice warning "Too Low Terrain" are firstly produced. Then, should the landing gear is not be extended and locked at 500 feet above terrain, the EGPWS warning light would light up and the voice warning "Too Low Gear" sound.

Mode 5. "Excessive Deviation below Glideslope" provides defence from inadvertent descent below a glide slope when on an ILS approach.

Mode 6. "Bank Angle" contains voice warnings for altitude and bank angle.

Mode 7. "Windshear" provides detection and alerts for incidents of wind shear.

Only three modes are examined in this chapter, namely Mode 1, 2 and 4, as they present well defined time sequences and are based on two possible sequential and correlated interventions by the crew (Fig. 5).

This is a typical two steps series activities, anyone step being performed correctly, leads to the success of the task (Fig. 6). The calculation of the probability of failure of the sequence of activities accounts for the fact that:

(a) The activities are in series and only one of them may be performed successfully to grant success of the task; and
(b) The two activities may not be dependent and the appropriate probability need sto be accounted for.

Consequently, the success, $p_s(task)$, and failure, $p_f(task)$, probabilities of the task are expressed as follows:

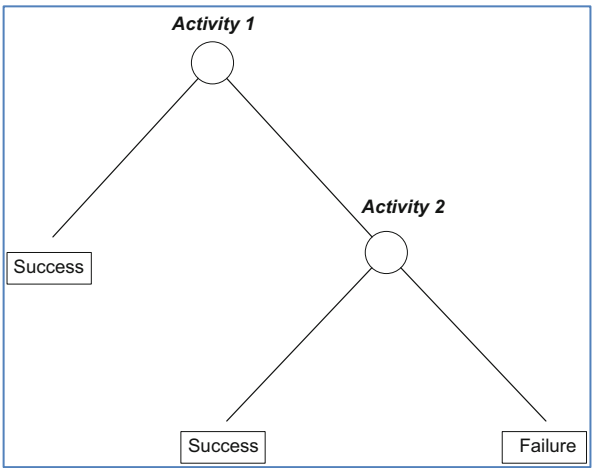


Fig. 6 Task performance of EGPWS sequence of two activities

$$p_s(task) = p_{s-ac1} + p_{f-ac1} * p_{s-ac2/f-ac1}$$

$$p_f(task) = p_{f-ac1} * p_{f-ac2/f-ac1}$$

as $p_{s-ac1} + p_{f-ac1} = 1$ *and* $p_{s-ac2/f-ac1} + p_{f-ac2/f-ac1} = 1$:

$$p_s(task) + p_f(task) = p_{s-ac1} + p_{f-ac1} * p_{s-ac2/f-ac1} + p_{f-ac1} * p_{f-ac2/f-ac1} = 1$$

4.2 Case Study 2: Runway Change Procedure

4.2.1 The Runway Change Procedure

The runway change procedure is a task often carried out in airports with unpredictable windy conditions, or even in airports with more than one runway to share the burden and to give the residents periods of relief from aircraft noise. It is assumed that the Runway change concerns and typical Runway 04R/22L turned around to 04L/22R.

For the Case Study 2, the procedure had been simplified and organised in six steps which need to be performed by three different teams of airport staff with different roles and competence. Fig. 7 shows, the actual task to be performed in each step, the teams involved, identified by team-number, and the time allowed to complete each task.

The overall runway change procedure is considered successfully completed when the tasks are carried successfully or errors are recovered according to the combinations of the different tasks:

Step 1. The first step of the procedure is performed by airport ground staff (Team 1) and implies to place a fence barrier of the inner perimeter road. Ten minutes are allowed to carry out this step.

Step	Action	Team	duration min
1	Place fence barrier of the inner perimeter road	1	10
2	Alight Approach Lights 04L. ILS 04R Off Aeronautical Ground Lighting (AGL) 04R/22L off Aeronautical Ground Lighting (AGL) 04L/22R * Switch frm blue to white side RW 04L/22R * Centre-line taxiway off	2	0.5
3	Visual check glide slope and AGL	3	15
4	Close Taxi way L, Y, JA e JB aeronautical barrier Close Taxi way R, P, N and W by stop bars	1 1	3
5	Visual inspection RW 04L/22R	3	15
6	Close RW 04R/22L by Marking RW	1	2

Fig. 7 Generic runway change procedure

Step 2. The next step is performed by Team 2 to intervene on the Aeronautical Ground Lighting (AGL) system by adapting the lights and colour to the requested standard and by turning the Instrumented Landing System (ILS) for 04R off. This step is carried out in 30 s.

Step 3. Step 3 is a visual check of the glide slope and aeronautical ground lighting. This is performed by Team 3, and it is a typical activity of check and verification of the previously perform3ed tasks. It is assumed that it takes 15 min to complete.

Step 4. Step 4, carried out by Team 1, implies the adjustment of the taxiways to the new configuration of the runway in use, by closing and opening the ways according to a well established procedure. Step 4 is divided into two subsequent activities and lasts about 3 min.

Step 5. Step 5 is performed by Team 3 as it implies the same kind of verification and check activity of a visual inspection of the runway 04L/22R becoming operative. Step 5 takes 15 min to carry out.

It important to note that, it is assumed that the visual inspection associated to *Step 5* enables to correct possible errors made at the level of taxiways ri-configuration, while it is not affecting the operations carried out in Steps 1–3.

Step 6. The final step is to close runway 04R/22L, by marking the runway. This activity is a very simple routine action of imposing "physical barriers" on the closed runways and it is carried out by Team 1 and in about 2 min.

4.2.2 Fault Tree Approach to Assess Failure of Runway Change Procedure

The whole procedure is carried out by different teams and tasks in temporal sequence. Therefore, it can structured in three phases: phase A, phase B and

phase C. This enables to make use of a Fault Tree (FT) to assess the overall final probability of error, which results from a combination of errors made during the performance of certain tasks and the possible recoveries resulting from the visual inspections. In particular:

- Phase A covers Steps 1, 2 and 3;
- Phase 2 contains Steps 4 and 5; and
- Phase 3 is associated to Step 6.

The fault tree of the operation in the runway change procedure be seen in Fig. 8.

In Phase A, either Step 1, i.e., the positioning of the fence barrier of the inner perimeter road, or Step 2, i.e., the operations on the AGL and ILS, can fail. However, errors made in Step 1 and 2 can be recovered in Step 3, i.e., the visual check. Therefore, Phase A fails if Step 1 OR Step 2 AND Step 3 fail. Similarly, for phase B to fail, Step 4 AND Step 5, i.e., operations on the taxiways and the visual inspection, need to fail. Finally, phase C is the closing of the runway. So if phase C fails, the whole procedure fails.

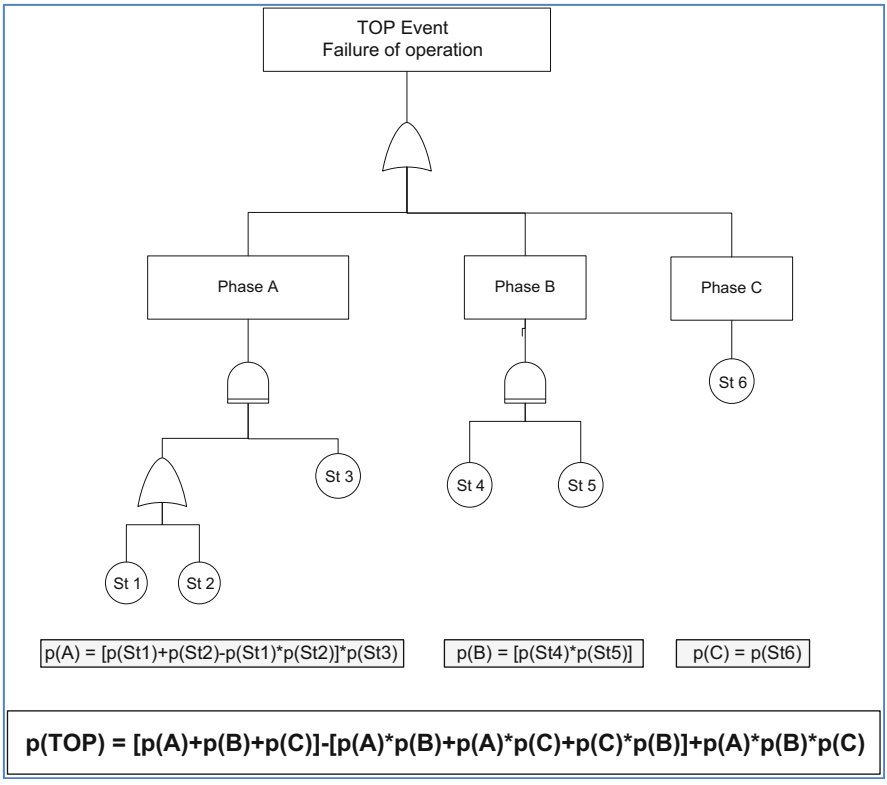


Fig. 8 Fault Tree for the assessment of failure of the Runway Change procedure

Fig. 8 shows also the probability calculation associated to the TOP Event, i.e., the failure of the task of runway change.

4.2.3 THERP Methodology Approach to Assess Failure of Runway Change Procedure

A THERP tree, resulting from a qualitative analysis of the whole procedure, can be developed in alternative to the FT method to describe the procedure under study (Fig. 9).

In this case, all steps of the procedure are considered as a single element of a "THERP Tree" and each step is represented as the binary alternative of success or failure. The sequence of successes and failures for all steps are combined to formalise the THERP tree. In particular, the visual tasks (Step 3 and 5) dedicated to checking and verifying the correct execution of earlier tasks, enable the "recovery" of previously made errors, when they are performed successfully. The success of the procedure is obtained when all steps are carried out correctly in relation to their specific goals and interactions, as described above, and in consideration for the recovery process.

It is noticeable how the two visual inspections of Sep 3 and Step 5 are able to correct previously performed errors only in relation to their associated specific activities, namely: Steps 1 and 2 associated to visual inspection Step 3 and Steps 4 associated to visual inspection Step 5. Moreover, errors made during the visual

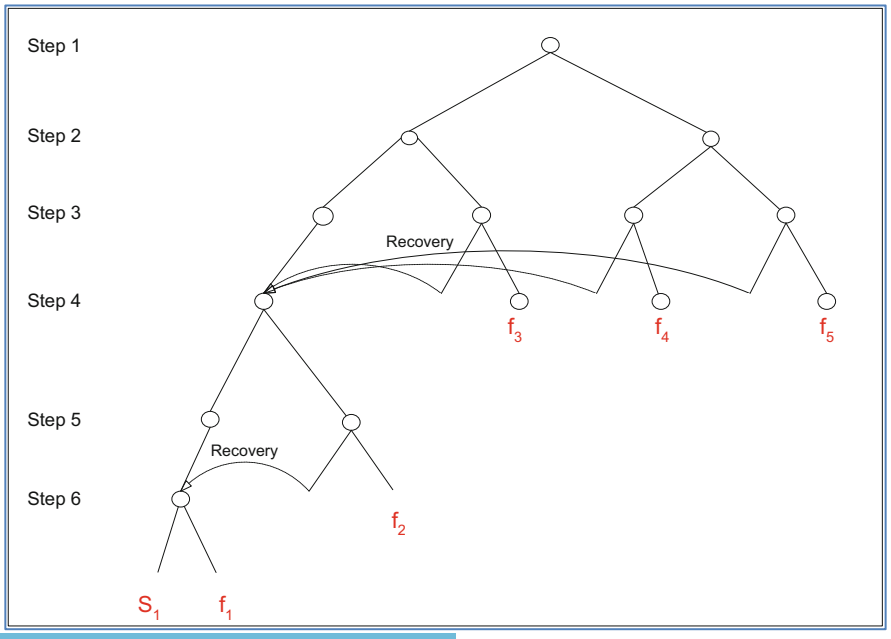


Fig. 9 THERP tree for the assessment of failure of the Runway Change procedure

inspections, when the previous actions, to which they refer, are performed correctly, are not accounted.

The success of the procedure is represented by a single branch of the THERP tree, whereas five possible sequences of failures can be envisaged. The probability calculation requires the combination of the various failures, recoveries and successes that combine to represent the whole process.

The calculations of Human Error probabilities of failing to carry out correctly the procedures involved in Case Study 1 and 2 are discussed in the following sections, for the four selected methods.

4.3 Human Error Assessment for Case Study 1: EGPWS

4.3.1 THERP: EGPWS Human Error Assessment

The THERP assessment of Human Error probability to respond to the alarms of the three cases of EGPWS for the three Alert modes selected are performed in consideration of the dependency between the two actions involved in each task.

The three modes of response to the EGPWS are: Mode 1, "Excessive Descent Rate"; Mode 2, "Excessive Terrain Closure"; and Mode 3, "Unsafe Terrain Clearance". As all three Modes of interaction between the automated alarm system and the pilots are essentially associated to the response of the crew to an alarm demanding immediate action, the estimated HEPs for multiple annunciators are found in Tables 20–23 of the THERP handbook. Moreover, it has been assumed that there is a "low" dependency between the failure to respond to the second alarm with respect to the failure to respond to the first alarm, for all three Alert modes. No Performance Shaping Factors effects have been considered (PSD = 1)

The overall result is shown in Fig. 10 that contains the probability of failing each single response action, given the hypotheses of Nominal Human Error Probability, dependencies and factors affecting performance.

Mode	Action	*Calls*	Hight/dist. Ft	Standard avail. t. Sec		THERP	NHEP	PSF	Dependcy	EP
1	Excess. Desc. Rate	*Sinkrate*	2,000	60		20-23	6.00E-04	1.00E+00	-	6.00E-04
		Pull Up	1,000	30		20-23	6.00E-04	1.00E+00	Low	5.06E-02
2	Excess. Terrain Closure	*Terrain Terrain*	2,000	60		20-23	6.00E-04	1.00E+00	-	6.00E-04
		Pull up	1,000	30		20-23	6.00E-04	1.00E+00	Low	5.06E-02
3	Unsafe terr. Clearence	*Too Low Terrain*	1,000	86		20-23	6.00E-04	1.00E+00	-	6.00E-04
		Too Low Gear	500	42		20-23	6.00E-04	1.00E+00	Low	5.06E-02

Fig. 10 THERP: EGPWS Human Error Assessment

Mode	Action	*Calls*	Hight/dist. Ft	Standard avail. t. Sec		HCR - t = 20 s HE	S-based t/T_{05}
1	Excess. Desc. Rate	*Sinkrate*	2,000	60		*3.39E-04*	3.00
		Pull Up	1,000	30		*1.05E-01*	1.50
2	Excess. Terrain Closure	*Terrain Terrain*	2,000	60		*3.39E-04*	3.00
		Pull up	1,000	30		*1.05E-01*	1.50
3	Unsafe terr. Clearence	*Too Low Terrain*	1,000	86		*1.15E-06*	4.29
		Too Low Gear	500	42		*1.22E-02*	2.10

Fig. 11 HCR: EGPWS Human Error Assessment

4.3.2 HCR: EGPWS Human Error Assessment

In the case of applying the HRC model, the average time available for responding to each alarm is associated to the actual EGPWS activated operational modes (Fig. 5). The time available for performing all actions has been assumed equal to 20 s.

Moreover, as the pilots are considered experts and well trained in their tasks, and the EGPWS is a serious alarm system that demands immediate action, it has been assumed that the pilots respond at level of "Skilled Based Behaviour".

According to the correlations utilised for the evaluation of the HE probability (Sun et al. 2011), the overall probabilities associated to each single action are shown in Fig. 11.

4.3.3 HEART: EGPWS Human Error Assessment

The implementation of the HEART model requires that each action or task is evaluated in consideration of the tables of "Generic Task Unreliability" (GTU) and "Error Producing Conditions" (RPCs).

In the case of the EGPWS, it has been assumed that the actions involved in each operation Mode of the EGPWS are all associated to a response of the pilots to an "automated supervisory system". However, the EPCs for the two specific response actions associated to the first or second call of the EGPWS are different.

As all three modes of operation of the EGPWS are dealt with the same types of activity, the assessment of HE for failing to respond to the alarms are shown in Fig. 12.

4.3.4 TESEO: EGPWS Human Error Assessment

In the case of TESEO, as in the case of THERP and HEART application, it has been assumed that the responses to the different EGPWS modes are essentially similar and therefore the same correlations apply for reach sequence of responses to first and second "call" of the alarm system.

In TESEO it has been assumed that response to the GWPS call, for both levels of call, implies a a "non routine activity", carried out by "carefully selected, expert,

p_1 = Probability of pilot errorat 1 st EGPWS call						p_2 =Probability of pilot errorat 2 nd EGPWS call					
GTU H	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP	GTU H	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP
2.00E-05	2	11	0.7	8	7.20E-04	2.00E-05	2	11	0.7	8	5.81E-03
6.0E-6 - 9.0E-5	8	6	0.7	4.5		6.0E-6 - 9.0E-5	8	6	0.7	4.5	
6.00E-06					2.16E-04	6.00E-06	3	10	0.7	7.3	1.74E-03
9.00E-05					3.24E-03	9.00E-05	33	1.15	0.7	1.105	2.61E-02

Fig. 12 HEART: EGPWS Human Error Assessment

Mode	Action	*Calls*	Standard avail. t. Sec	TESEO
1	Excess. Desc. Rate	*Sinkrate*	60	*7.00E-03*
		Pull Up	30	*7.00E-02*
2	Excess. Terrain Closure	*Terrain Terrain*	60	*7.00E-03*
		Pull up	30	*7.00E-02*
3	Unsafe terr. Clearence	*Too Low Terrain*	86	*7.00E-03*
		Too Low Gear	42	*2.10E-02*

Fig. 13 TESEO: EGPWS Human Error Assessment

well trained" pilots and represents a "situation of potential emergency". The working environment has been assumed to be "Excellent microclimat, excellent interface with plant".

The probabilities of HE in carrying out the two actions of response depend primarily on the time available for reacting to the EGPWS call (Fig. 13).

4.4 Human Error Assessment for Case Study 2: Runway Change Procedure

4.4.1 THERP: Runway Change Procedure Human Error Assessment

The THERP assessment of Human Error probability to carry out the procedure as described earlier, can be calculated applying the FT (Fig. 8) or the THERP three (Fig. 9) that consider the interactions between each action.

The assessment of the HE probability for each action of the procedure is evaluated applying different THERP Tables (Fig. 14), assuming that no dependencies exist between actions and that no effects on the performances due to environmental nor social conditions exist. In other words, it has been assumed that the procedure takes place in a non-stressful condition with time and support systems available.

Step	Action	Team	duration min		THERP	NHEP	PSF	EP
1	Place fence barrier of the inner perimeter road	1	10		20-7	1.00E-03	1.00E+00	1.00E-03
2	Alight Approach Lights 04L. ILS 04R Off Aeronautical Ground Lighting (AGL) 04R/22L off Aeronautical Ground Lighting (AGL) 04L/22R * Switch frm blue to white side RW 04L/22R * Centre-line taxiway off	2	0.5		20-6	3.00E-03	1.00E+00	3.00E-03
3	Visual check glide slope and AGL	3	15		20-22	1.00E-03	1.00E+00	1.00E-03
4	Close Taxi way L, Y, JA e JB aeronautical barrier	1	3		20-7	1.00E-03	1.00E+00	1.00E-03
	Close Taxi way R, P, N and W by stop bars	1						
5	Visual inspection RW 04L/22R	3	15		20-22	1.00E-03	1.00E+00	1.00E-03
6	Close RW 04R/22L by Marking RW	1	2		20-12	1.00E-03	1.00E+00	1.00E-03

Fig.14 THERP: Runway Change Procedure Human Error Assessment

Step	Action	Team	T_{05} = time necessary	t = duration min	HRC Mode	HCR HE prob	t/T_{05}
1	Place fence barrier of the inner perimeter road	1	5	10	RBB	1.18E-01	2
2	Alight Approach Lights 04L. ILS 04R Off Aeronautical Ground Lighting (AGL) 04R/22L off Aeronautical Ground Lighting (AGL) 04L/22R * Switch frm blue to white side RW 04L/22R * Centre-line taxiway off	2	0.2	0.5	SBB	2.60E-03	2.5
3	Visual check glide slope and AGL	3	5	15	SBB	3.39E-04	3
4	Close Taxi way L, Y, JA e JB aeronautical barrier	1	2	3	RBB	2.37E-01	1.5
	Close Taxi way R, P, N and W by stop bars						
5	Visual inspection RW 04L/22R	3	5	15	SBB	3.39E-04	3
6	Close RW 04R/22L by Marking RW	1	0.5	2	RBB	8.59E-03	4

Fig. 15 HCR: Runway Change Procedure Human Error Assessment

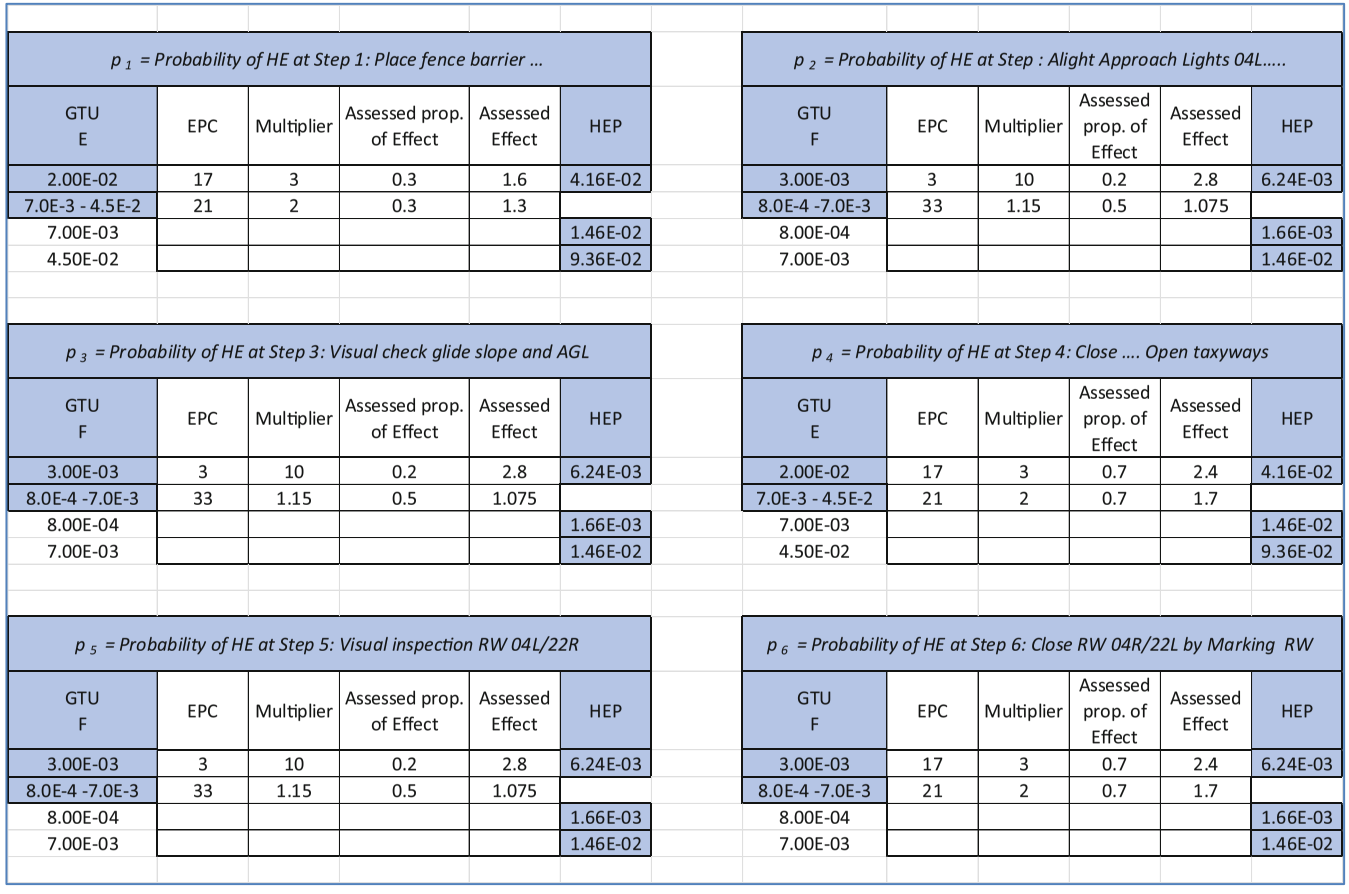
4.4.2 HCR: Runway Change Procedure Human Error Assessment

The implementation of the HCR model requires the association of the time available for performing each activity of the task and the average time normally assumed necessary. The airport personnel utilised to carry out the activity is either considered experts and well trained in at level of "Skilled Based Behaviour" or operating at "Rule Based Behaviour".

According to the correlations utilised for the evaluation of the HE probability (Sun et al. 2011), the overall probabilities associated to each single action are shown in Fig. 15.

4.4.3 HEART: Runway Change Procedure Human Error Assessment

The implementation of HEART and the consideration of the tables of GTU and RPCs have generated the results shown in Fig. 16.



p_1 = Probability of HE at Step 1: Place fence barrier ...

GTU E	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP
2.00E-02	17	3	0.3	1.6	4.16E-02
7.0E-3 - 4.5E-2	21	2	0.3	1.3	
7.00E-03					1.46E-02
4.50E-02					9.36E-02

p_2 = Probability of HE at Step : Alight Approach Lights 04L.....

GTU F	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP
3.00E-03	3	10	0.2	2.8	6.24E-03
8.0E-4 -7.0E-3	33	1.15	0.5	1.075	
8.00E-04					1.66E-03
7.00E-03					1.46E-02

p_3 = Probability of HE at Step 3: Visual check glide slope and AGL

GTU F	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP
3.00E-03	3	10	0.2	2.8	6.24E-03
8.0E-4 -7.0E-3	33	1.15	0.5	1.075	
8.00E-04					1.66E-03
7.00E-03					1.46E-02

p_4 = Probability of HE at Step 4: Close .... Open taxyways

GTU E	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP
2.00E-02	17	3	0.7	2.4	4.16E-02
7.0E-3 - 4.5E-2	21	2	0.7	1.7	
7.00E-03					1.46E-02
4.50E-02					9.36E-02

p_5 = Probability of HE at Step 5: Visual inspection RW 04L/22R

GTU F	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP
3.00E-03	3	10	0.2	2.8	6.24E-03
8.0E-4 -7.0E-3	33	1.15	0.5	1.075	
8.00E-04					1.66E-03
7.00E-03					1.46E-02

p_6 = Probability of HE at Step 6: Close RW 04R/22L by Marking RW

GTU F	EPC	Multiplier	Assessed prop. of Effect	Assessed Effect	HEP
3.00E-03	17	3	0.7	2.4	6.24E-03
8.0E-4 -7.0E-3	21	2	0.7	1.7	
8.00E-04					1.66E-03
7.00E-03					1.46E-02

Fig.16 HEART: Runway Change Procedure Human Error Assessment

The following conditions for each step of the procedure apply:

- Steps 1 and 4 are activity type E, namely "routine highly practised (during training) rapid task involving relatively low level skill". They are affected by little independent checking (EPC 17) and sometimes are implemented without following the procedure (EPC 21) for various reasons, such as simplicity of the activity, experience etc.
- Steps 2, 3, 5 and 6 are activity type F, namely "shifting a system to a new state following procedures". However, Steps 2, 3 and 5, which are essentially carried out by airport personnel knowledgeable in the runway control system, are affected by EPC 3 (Low signal-to-noise ratio) to account for the need to verify the electronic system performance and EPC 33("poor hostile environment") to consider the presence of traffic and a variety of environmental conditions. Affecting the performance. Step 6, instead, is affected by the same EPCs of Steps 1 and 4 as it is essentially the implementation of a task on the runways, which is however carried out with attention for the procedure.

4.4.4 TESEO: Runway Change Procedure Human Error Assessment

In the case of TESEO, Fig.17 shows the assessment of HE in performing the runway change procedure.

The combination and assumptions about the various aspects of the activities performed by the airport personnel take into consideration the environmental conditions.

Step	Action	Team	duration min	TESEO	TESEO coefficients
1	Place fence barrier of the inner perimeter road	1	10	7.00E-04	Rout. req. att.; Caref. sel. staff; Pot. em.; Exc. Micr.
2	Alight Approach Lights 04L. ILS 04R Off Aeronautical Ground Lighting (AGL) 04R/22L off Aeronautical Ground Lighting (AGL) 04L/22R * Switch frm blue to white side RW 04L/22R * Centre-line taxiway off	2	0.5	7.00E-03	Rout. req. att.; Caref. sel. staff; Pot. em.; Exc. Micr.
3	Visual check glide slope and AGL	3	15	1.00E-03	Rout. req. att.; Caref. sel. staff; Pot. em.; Good Micr.
4	Close Taxi way L, Y, JA e JB aeronautical barrier Close Taxi way R, P, N and W by stop bars	1	3	1.00E-03	Rout. req. att.; Caref. sel. staff; Pot. em.; Good Micr.
5	Visual inspection RW 04L/22R	3	15	1.00E-03	Rout. req. att.; Caref. sel. staff; Pot. em.; Good Micr.
6	Close RW 04R/22L by Marking RW	1	2	7.00E-04	Rout. req. att.; Caref. sel. staff; Pot. em.; Exc. Micr.

Fig. 17 TESEO: Runway Change Procedure Human Error Assessment

5 Comparison of Results and Discussion

5.1 Comparison of Results for Case Study 1: EGPRS

The overall results obtained applying the four different methods to the case study EGPWS are shown in Fig. 18.

The left hand side of the figure shows the three modes of operation of the EGPWS studied and the expected responses and timing available for implementation by the pilots. Each operational mode is divided into two subsequent "calls" and types of reaction and each one of them enables to resolve the hazardous condition.

The incident can be considered avoided if at least one of the two responses to the alert is actually implemented. In other words, both actions must fail for the incident to occur. In probability terms, assuming that the two actions are independent:

$$p_{inc} = p_{fail\ action\ 1} * p_{fail\ action\ 2}$$

The right hand side of Fig. 18 shows firstly the probability calculated with the different methods of failing each action and then the overall probability of failing the combined actions, i.e., failing to respond to the specific EGPWS specific alert.

Comparing the probabilities, a number of comments and remarks can be made:

1. The results presented by HEART and THERP are reasonably similar for all types of actions and consequently for their combination, as overall result. In particular, they show values of probability of failing to respond to the second call higher than the probabilities to respond to the first call. This is logical and expected also for common sense reason, as the pilots are facing a reduced-to-collision time.
2. The results of TESEO and specially HCR are more distributed in terms of probability of failure of action, as they are very sensitive to the time availability for response.

   a. HCR, being particularly sensitive to the time available parameter, evaluates a very low probability of failing to responds to the "Unsafe terrain clearance" alert as the time available is substantially longer that the average time required to respond. The probability of failing to respond to the calls of the other modes of alert are similar to the values calculated by HEART and THERP for the first call and much higher for the second call, being very small the available reaction time.

Mode	Action	*Calls*	Hight/dist. Ft	Standard avail. t. Sec		THERP	HEART	HCR	TESEO		THERP	HEART	HRC	TESEO
1	Excess. Desc. Rate	*Sinkrate*	2,000	60		6.00E-04	7.20E-04	*3.39E-04*	*7.00E-03*		3.03E-05	4.18E-06	3.57E-05	4.90E-04
		Pull Up	1,000	30		5.06E-02	5.81E-03	*1.05E-01*	*7.00E-02*					
2	Excess. Terrain Closure	*Terrain Terrain*	2,000	60		6.00E-04	7.20E-04	*3.39E-04*	*7.00E-03*		3.03E-05	4.18E-06	3.57E-05	4.90E-04
		Pull up	1,000	30		5.06E-02	5.81E-03	*1.05E-01*	*7.00E-02*					
3	Unsafe terr. Clearence	*Too Low Terrain*	1,000	86		6.00E-04	7.20E-04	*1.15E-06*	*7.00E-03*		3.03E-05	4.18E-06	1.40E-08	1.47E-04
		Too Low Gear	500	42		5.06E-02	5.81E-03	*1.22E-02*	*2.10E-02*					

Fig. 18 Results of Case Study 1: EGPWS

b. TESEO shows similar probabilities to HCR, especially in relation to the error to miss the second call of the alarm mode "Unsafe terrain clearance" and, in more general terms, in relation to the second "call" of all alarm modes. Whereas, the probability to failing to respond adequately to the first call differs substantially from all other results and is the most conservative value, i.e., shows the heights probability of error.

3. When comparing the overall probability of failing to respond to the combined calls for each alarm mode, on the far left hand side of Fig. 18, HCR shows a very low probability of failing to the "Unsafe terrain clearance", of about four orders of magnitude with respect to TESEO and two and three with respect to HEART and THERP respectively. The other probabilities are less distributed, with TESEO being the most conservative method, showing the highest error probabilities, approximately one or two orders of magnitude higher than the other methods.

5.2 Comparison of Results for Case Study 2: Runway Change Procedure

The comparison of results for the case study of the runway change procedure lead to similar conclusions as for the case of the EGPWS.

The evaluation of the probabilities of failing each single action or step in the procedure are strongly affected by the time available, especially in the case of the HCR method. The dependency of HCR on "time availability" results in probabilities values of two to three orders of magnitude greater than those obtained using the other methods, especially for Steps 1 and 4. For the other Steps HCR is more aligned with the results of the other methods.

HEART, TESEO and THERP show results of very similar order of magnitude for each Step of the procedure.

The overall probability of failing to perform the procedure correctly is strongly affected by the combination of the errors of performance of single actions and the recoveries due to the Steps 3 and 5 of visual check and verification of the previous activities. This has been represented by the Fault Tree (Fig. 8) or the application of the THERP tree (Fig. 9).

In this case, the failure of the final Step 6 is governing the whole procedure, as it represent a single failure affecting the entire procedure. Consequently, as the probabilities of failing Step 6 for all four methods lead to similar values, ranging from 7.0×10^{-4} to 8.59×10^{-3}, the overall probability of failing the procedure, p (TOP), are within comparable values (Fig. 19).

Step	Action	Team	duration min	Severity	TESEO	HEART	HCR	THERP
1	Place fence barrier of the inner perimeter road	1	10	Med	7.00E-04	4.16E-02	1.18E-01	1.00E-03
2	Alight Approach Lights 04L. ILS 04R Off Aeronautical Ground Lighting (AGL) 04R/22L off Aeronautical Ground Lighting (AGL) 04L/22R * Switch frm blue to white side RW 04L/22R * Centre-line taxiway off	2	0.5	High	7.00E-03	6.24E-03	2.60E-03	3.00E-03
3	Visual check glide slope and AGL	3	15	Med	1.00E-03	6.24E-03	3.39E-04	1.00E-03
4	Close Taxi way L, Y, JA e JB aeronautical barrier Close Taxi way R, P, N and W by stop bars	1	3	High	1.00E-03	4.16E-02	2.37E-01	1.00E-03
5	Visual inspection RW 04L/22R	3	15	High	1.00E-03	6.24E-03	3.39E-04	1.00E-03
6	Close RW 04R/22L by Marking RW	1	2	High	7.00E-04	6.24E-03	8.59E-03	1.00E-03
				p(TOP) =	7.09E-04	6.80E-03	8.71E-03	1.00E-03

Fig. 19 Comparison of results for Case Study 2: Runway Change Procedure

6 Discussion

The comparison exercise developed in the second part of this Chapter aimed at evaluating and ascertaining two aspects of existing and well-known human reliability methods, namely:

1. Firstly, the capability of each method and the differences of results in the evaluation of the human error probability in performing certain activities, with specific reference to the domain of aviation;
2. Secondly, given that these methods have been developed with reference to different domains than aviation, the validity of each method with respect to the range of parameters and constant values proposed to represent human error probabilities for the domain of aviation.

6.1 Comparison of Results in Assessing Human Error Probability

The two case studies refer to two different procedures frequently encountered in the domain of aviation, namely the response to an alarm and request to perform rapid and evasive manoeuvres and the sequence of activities carried out on a regular basis, usually with a reasonable amount of time availability. The reason for selecting these two procedures is associated to the time-to-response dimension, which is crucial and very short for the first case study. Whereas, in the second case study, "time" is a less relevant parameter than aspects such as accuracy and respect of the actual steps in performing each task.

In both case studies, the results of THERP and HEART, and partly TESEO, show similar evaluation of human error probabilities, even if the values vary in some cases of more than one order of magnitude. TESEO in particular, being more affected by the available time and the criticality of certain activities, generates very

conservative human error probabilities when the time constraint is relatively small, such as in the first case study of the EGPWS. Whereas it produces smaller error probabilities than THERP and HEART, when the activities are less constrained by the time aspect, i.e., in the second case study of runway change procedure.

The HCR method is very sensitive to the time availability aspect and therefore it generates human error probabilities that, in certain cases, differ substantially from the results of the other methods. As an example, in assessing the human error probability to respond to the "unsafe terrain clearance" calls, HCR generated failure probabilities of four orders of magnitude smaller than TESEO and almost three orders of magnitude than THERP and HEART.

A first result of this comparison can therefore be associated to the selection of the method that needs to be very carefully adapted to the variable of time availability to perform the tasks of the procedures under assessment.

6.2 Comparison of Processes in Applying the Methods

Another aspect that is relevant is associated with the process of assessment of the different boundary and environmental conditions affecting human error probability. THERP and HEART require a similar process leading the error probability. Firstly, the type of human error and relative probability are identified, called "Nominal Human Error Probability" (NHEP) in THERP and "Generic Task Unreliability" (GTU) in HEART. Then a very accurate and detailed process of evaluation of the factors affecting human error is carried out. This implies that the socio-technical conditions of task performance are evaluated, via the "Error Producing Conditions" in HEART and the "Performance Shaping Factors" in THERP. Moreover, the dependencies are also evaluated in both methods, using a specify correlations.

This relatively lengthy and accurate process enables the safety analyst to consider a great variety of factors that are associated to the performance of tasks, including the time availability and the working contexts.

TESEO also considers the time and socio-technical aspects in each of the five parameters that combine in the evaluation of human error probability. However, the variety of conditions that can be accounted for is much smaller and limited than HERATH and THERP. On the other side TESEO is much easier and rapid to apply.

HCR is also rapid and can be easily applied as the correlation that generates human error probability is developed and applied on the basis of few parameters. However, the relevance of the time available to perform the task and, to a lower level, the experience and expertise of the persons involved are predominant with respect to other aspects. In certain cases, this aspect affects strongly the overall human error probability.

Another aspect that is relevant with respect to the process of overall human error assessment is the uncertainty associated to the probability of error. In the case of THERP and HEART, the uncertainty is coupled to the initial values of the NHEPs, via the "Error Factors" (EF) in THERP, and GTUs, via the 5th and 95th percentiles

in HEART. The user can therefore assess the overall uncertainty bounds associated to the error probability of each action or task by propagating the initial uncertainty via a simple process or, in the most complex approaches, by means of a Montecarlo simulation.

6.3 Comparison in Aptness to the Domain of Aviation

The results in applying the four methods to specific procedures and tasks in the domain of aviation was unable to demonstrate clearly the aptness of the methods to assess human error probabilities.

The fact that the various parameters and coefficients have been developed in different domains than aviation, primarily chemical and nuclear environment, favours the expectation that a set of specific values should be developed for aviation. This can be done by analysing the extensive and accurate data collection of exiting events reported by the various organisations to the authorities as well as to their own safety departments. On the other hand, the results of applying the methods, as they are at present, has shown the relevance of certain aspects, such as the time availability, that may predominate with respect to the accuracy of certain basic factors and coefficients.

The overall results obtained in the two case studies seem to be "reasonable" in terms of expected human error probability. Moreover, the uncertainty that is associated to the mean value is a means to account for the possible imprecision associated to the coefficients. The implementation of larger uncertainty bounds, in addition to the standard uncertainty that is typical of risk analysis processes, could be a way to account for this aspect.

7 Conclusions

This Chapter aimed at discussing firstly a practical way to support Risk Informed Decision Making processes. The proposed approach, although discussed only in abstract and theoretical terms, has shown that it is possible to develop practical instruments supporting the safety analysts and safety managers in presenting overall results of the risk analysis process to the decision makers in a way that is condense and enables to visualize the relevance of different measures with respect to safety. The generic form of a Risk Informed Decision Making Table is an instrument that support the selection of the most relevant barriers with respect to safety and their distributed cost in a shared form. The Safety Managers can demonstrate the importance of the barriers and safeguards that have been identified, both in terms of effectiveness with respect to safety and efficiency with respect to cost benefit.

The second and more detailed content of this Chapter was the evaluation of four different and well established Human Reliability methods to cope with aviation procedures. In particular, two procedures were selected with very different characteristics. Time and criticality aspects were the relevant factors affecting the tasks. The goals of the comparison was to evaluate the capability of these methods, and their differences, in the evaluation of the human error probability in performing aviation activities.

The comparison of results has shown that two of the methods namely THERP and HEART, are more accurate and enable to consider several different contributing factors. In particular, they can account for dependencies and socio-technical aspects in addition to time and criticality of tasks. Moreover, they uncertainty bounds is included in the error assessment process in all steps of the methods.

TESEO and HCR are mush rapid and easier methods to apply. However, they are strongly affected by the few coefficients and parameters that support the methods. The time availability, especially in the case of HCR is extremely predominant on all other factors affecting human performance.

Finally, it has not been possible to come to a conclusive assessment of the ability of the methods, as they are at present, to cope with aviation issues, as a much more extensive process of existing data collection and analysis would be needed to carry out an accurate revision.

References

Andrews JD, Moss TR (1993) Reliability and risk assessment. Logman Scientific & Technical, Harlow

ARMS (2011) The arms methodology for operational risk assessment in aviation Organisations. http://www.easa.eu.int/essi/documents/Methodology.pdf visited 2011.12.28

Bell J, Holroyd J (2009) Review of human reliability assessment methods. Health and Safety Executive (HSE). Research Report—RR679

Bello GC, Colombari C (1980) The human factors in risk analyses of process plants: the control room operator model, TESEO. Reliab Eng Syst Saf 1:3–14

BowTie (2013) The Bowtie methodology. Online: www.bowtiepro.com. Visited 12/06/2013

Cacciabue PC (2004) Human error risk management for engineering systems: a methodology for design, safety assessment, accident investigation and training. Special issue on HRA data issues and errors of commission. Reliab Eng Syst Saf 83:229–240

Cacciabue PC, Cassani M, Licata V, Oddone I, Ottomaniello A (2015) A practical approach to assess risk in aviation domains for safety management systems. Cog Tech Work 17:249–267

Castiglia F, Giardina M, Tomarchio E (2015) THERP and HEART integrated methodology for human error assessment. Radiat Phys Chem 116:262–266

De Grandis E, Oddone I, Ottomaniello A, Cacciabue PC (2012) Managing risk in real contexts with scarcity of data and high potential hazards: the case of flights in airspace contaminated by volcanic ash. Proceedings of PSAM-11—ESREL 2012, Helsinki, June 25–29.

Dhillon BS (2014) Human reliability, error, and human factors in power generation. Springer, Cham, ISBN 978-3-319-04019-6

EASA—European Aviation Safety Agency (2012) European Aviation Safety Plan 2012–2015. Final Report

EC—European Commission (2012) Commission Regulation (EU) No 965/2012

Ersdal G, Aven T (2008) Risk informed decision-making and its ethical basis. Reliab Eng Syst Saf 93:197–205
FAA (2010) SMS Notice of Proposed Rulemaking (NPRM) for 14 CFR Part 121 Certificate Holders. SMS NRPM for 14 CFR Part 121
Hannaman GW, Spurgin AJ, Lukic YD (1984) Human cognitive reliability model for PRA analysis. NUS-4531, NUS Corporation, San Diego, CA
Hollnagel E (1998) Cognitive reliability and error analysis method. Elsevier, London
Hollnagel E (2004) Barriers and accident prevention. Ashgate, Aldershot
Humphreys P (ed) (1988) Human reliability assessors guide. United Kingdom Atomic Energy Authority, RTS88/95Q
IAEA—International Atomic Energy Agency (2005) Risk informed regulation of nuclear facilities: overview of the current status IAEA-TECDOC-1436. Vienna
IAEA—International Atomic Energy Agency (2011) A framework for an integrated risk informed decision making process INSAG-25. Vienna
ICAO—International Civil Aviation Organisation (2012) Safety management manual, 3rd edn. Doc 9859 AN/474. Montreal
Kierzkowski A, Kisiel T (2015) Airport security screeners' reliability analysis. Proceedings of 2015 I.E. International Conference on Industrial Engineering and Engineering Management (IEEM 2015). Singapore, 6–9 December 2015, pp 1158–1163
Kirwan B (1994) A guide to practical human reliability assessment. Taylor & Francis, London
Lyons M, Woloshynowych M, Adams S, Vincent C (2005) Error Reduction in Medicine. Final Report to the Nuffield Trust
NASA (2010) NASA risk informed decision making handbook. NASA/SP-2010-576 (Vol 1)
NEA-CSNI (1998) Critical operator actions: human reliability modelling and data issues. Principal Working Group No. 5—Task 94-1. NEA/CSNI/R(98)1
Nielsen DS (1971) The cause/consequence diagram method as a basis for quantitative accident analysis. Danish Atomic Energy Commission RISO-M-1374
NRC—US Nuclear Regulatory Commission (1995) Final policy statement 'Use of Probabilistic Risk Assessment (PRA) Methods in Nuclear Regulatory Activities'. Washington, DC
NRC—US Nuclear Regulatory Commission (1998) An approach for plant-specific, risk-informed decision making: technical specifications. RG 1.177. Washington, DC
NRC—US Nuclear Regulatory Commission (2002) An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. RG 1.174. Washington, DC
NRC—US Nuclear Regulatory Commission (2003). Fleming KN. Issues and recommendations for advancement of PRA technology in risk-informed decision making. NUREG 6813
NRC—US Nuclear Regulatory Commission (2009). Drouin M, Parry G, Lehner J, Martinez-Guridi G, LaChance J, Wheeler T. Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making. NUREG 1855. Vol 1
Rasmussen J (1983) Skills, rules and knowledge: signals, signs and symbols; and other distinctions in human performance model. IEEE-SMC 13-3:257–267
Roland HE, Moriarty B (1990) System safety engineering and management. Wiley, New York
Salvendy G (2006) Handbook of human factors and ergonomics. Wiley, Hoboken
Spurgin AJ (2010) Human Reliability Assessment. Theory and practice. CRC Press, Taylor & Francis Group, New York
Stolzer AJ, Halford CJ, Goglia JJ (2010) Safety management systems in aviation. Ashgate, London
Sun R, Chen Y, Liu X, Peng T, Liu L (2011) A method of analysis integrating HCR and ETA modeling for determining risks associated with inadequate flight separation events. J Aviat Technol Eng 1(1):19–27
Swain AD, Guttmann HE (1983) Handbook of reliability analysis with emphasis on nuclear plant applications. Nuclear Regulatory Commission NUREG/CR-1278 Washington, DC

Williams JC (1985) 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 (SaRS). NEC, Birmingham.

Williams JC (1988) A data-based method for assessing and reducing human error to improve operational performance, 4th IEEE conference on Human factors in Nuclear Power Plants, Monterey, California, pp. 436–450, 6–9 June 1988

Pietro Carlo Cacciabue is currently a Lecturer at Kingston University (London), Faculty of Science, Engineering and Computing. In the period 2008–2016 he was Professor at the Politecnico of Milan, Dpt. of Aerospace Engineering. He is a retired senior scientist of the European Commission-Joint Research Centre (EC-JRC). He is following and has contributed to various Projects associated to safety and risk management. In particular he is the reference figure and principal consultant for a UK based Small and Medium Enterprise active in the domain of Aviation and Railway Safety in favour of institutional and private parties. He acts as consultant on aviation safety and safety management for the Italian Flight Safety Committee (IFSC), Rome, Italy, and for other bodies and academies at national and international level. In the period 2009–2016, he has supervised and collaborated to various competitive projects in Aviation, Health Safety, Rail and Automotive Transport. In the position of senior scientist of the EC-JRC, he has managed several projects. In detail, in the years 2000–2007. He was responsible for competitive and institutional actions in Transport, Petrochemical Industries, and in Health and Safety Environment. In the years 1980 up to 2000, he contributed to research activities in Nuclear Reactor Safety-Probabilistic Studies, Working Environment, and Environment-Risk Assessment.

Italo Oddone is currently professor at the Politecnico of Milan. Department of Aerospace Engineering and president of the Italian Flight Safety Committee. He is retired as captain of Airdolomiti, a Lufthansa company in 2016. He act as captain in several airline since 1996 as safety, security and crisis manager. He graduated in the Italian Airforce Academy and has served as a military pilot from 1976 to 1996. He is tutor of basic and advanced SMS / Investigation Courses c/o IFSC. He has acted as Advisor in the A-PiMod project "Applying Pilot Models for Safety" of the Seventh Framework Program of the European Commission and was in charge of Airdolomiti within the "Managing System Change in Aviation" of the Seventh Framework Program of the European Commission. He is an accident investigator, instructor pilot and auditor for airlines. He is qualified Short Field landings, Unprepared runways and snowy slope, Parachute Drops and Aerobatic Flying with over 14,000 flight hours on multiple airplanes.