System Safety Analysis of a Brake Press Using Fuzzy Methodology

by

Antonio VENDITTI

THESIS PRESENTED TO ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
IN PARTIAL FULFILLMENT FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
Ph.D.

MONTREAL, NOVEMBER 30, 2020

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

BOARD OF EXAMINERS

THIS THESIS HAS BEEN EVALUATED

BY THE FOLLOWING BOARD OF EXAMINERS

Mr. Anh Dung Ngô, Thesis Supervisor
Department of mechanical engineering at École de technologie supérieure

Mr. Tony Wong, President of the Board of Examiners
Department of systems engineering at École de technologie supérieure

Mr. Thien My Dao, Member of the jury
Department of mechanical engineering at École de technologie supérieure

Mr. François Gauthier, External evaluator
School of Engineering, UQTR

THIS THESIS WAS PRENSENTED AND DEFENDED

IN THE PRESENCE OF A BOARD OF EXAMINERS AND PUBLIC

OCTOBER 16, 2020

AT ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

ACKNOWLEDGMENT

I would like to express my gratitude to my Professor Anh Dung Ngô for his support and great patience. His experience and quick grasp of the key elements of a research project were invaluable. I would like to express also my deepest gratitude to Dr. Nguyen Duy Phuong Tran of Ho-Chi-Minh University of Vietnam. He collaborated on this research and provided me with precious advice on mathematical modelling and Matlab programming in particular.

I would like to thank my dear wife Marina. She had to endure long years of wondering when was this all going to finish. To my daughters Sarah and Jessica, I want to express my love and my thanks for being the wonderful persons they've grown up to become during these years.

System Safety Analysis of a Brake Press Using Fuzzy Methodology

Tony VENDITTI

RÉSUMÉ

Les presses plieuses sont des machines largement répandues dans l'industrie manufacturière. Elles permettent de plier des feuilles et plaques de métal de multiples manières afin de façonner des pièces variées. Le principe de fonctionnement même de ces machines crée une zone de coincement et d'écrasement pour les opérateurs notamment au niveau des mains et des doigts. Des normes de sécurité se sont développées au cours des années qui prescrivent des moyens techniques de protection de la zone d'opération ainsi que les autres moyens de contrôle des autres risques générés par l'opération de ces machines.

Toute machine industrielle telle qu'une presse plieuse doit faire l'objet d'une analyse des risques systématique permettant de tenir compte de tous les éléments physiques et humains qui peuvent interagir menant ainsi à des accidents possibles. Au cours des années, des méthodes ont notamment été élaborées visant à estimer la probabilité d'occurrence d'un accident à partir de l'identification des facteurs de risques contributifs. Dans le cas des machines industrielles telles que les presses plieuses, ces méthodes font rarement appel à des données historiques sur les accidents ayant eu lieu à cause de la relative rareté de ces données. Le jugement des intervenants participant à ces analyses est alors utilisé. Bien que le résultat de ces analyses aide à élaborer les stratégies de contrôle des risques, leur caractère subjectif continue de poser problème.

Cette thèse aborde la question de l'estimation de la probabilité d'occurrence d'accident pouvant survenir sur une machine industrielle telle qu'une presse plieuse dans l'optique de rendre cette analyse plus quantitative mais dans un contexte où les données historiques sur les accidents ou techniques sur les facteurs contributifs aux accidents sont limitées. Pour ce faire, cette thèse utilise le concept de logique floue ainsi que la technique structurée de la sollicitation d'expert pour quantifier des jugements sur les probabilités estimées.

Dns cette thèse, une presse plieuse est analysée en tenant compte de deux types de défaillances pouvant affecter son fonctionnement soit celles que peut subir les systèmes de protection de la zone dangereuse de la machine ainsi que celles constituées par les gestes accomplis par les opérateurs.

Les facteurs contributifs menant aux accidents considérés sont analysés en utilisant les arbres de fautes. Le caractère dynamique, séquentiel de la genèse d'un accident sur une machine est tenu aussi en compte par cette technique dans ce travail.

La probabilité d'accident ainsi estimée pour le système industriel est alors utilisé par la suite dans cette thèse pour optimiser le coût associé.

Cette thèse est constituée d’analyses de complexité croissante de situations de travail centrées sur une presse plieuse hydraulique. Dans un premier temps, la probabilité d’occurrence d’un accident subi par l’opérateur est estimée en considérant la défaillance du dispositif de protection et la défaillance de l’opérateur. Puis, cette même situation est considérée en incorporant le taux de réparation des modes de défaillance technique et humain. Finalement, des éléments de redondance tant au niveau technique qu’humain sont ajoutés au modèle. Cette thèse démontre que la méthode d’analyse mathématique développée permet une estimation plus quantitative de la probabilité associée au risque étudié et d’optimiser le coût associé à l’atteinte d’un niveau de sécurité visé.

Cette thèse présente une méthode qui augmente la validité des jugements de probabilité d’occurrence d’évènements contribuant à des accidents industriels mais ceux-ci demeurent dépendant des jugements exprimés en premier lieu par les intervenants impliqués. Nous envisageons des travaux ultérieurs qui raffineront la méthode de sollicitation d’experts dans un contexte d’analyse de risques de machines industrielles. De plus, les modèles exprimant le coût relié au maintien d’un niveau de sécurité donné devront être également perfectionnés. Les modèles décrivant des situations menant à des accidents reliés à des machines incorporeront dans l’avenir d’autres complexités telles que des taux de défaillance non constants.

Mots-clés: logique floue, nombre flou, analyse des risques, Chaîne de Markov, fonction de coût, arbre des fautes dynamique, sollicitation d’experts, facteurs humains.

System Safety Analysis of a Brake Press Using Fuzzy Methodology

Tony VENDITTI

ABSTRACT

Brake presses are machines which are widely found in the manufacturing industry. They enable metal sheets and plates to be bent in multiple ways so as to shape a wide variety of parts. The very principle by which these machines function creates a pinch and crushing zone for operators notably as far as their hands and fingers are concerned. Safety norms have been developed in the course of the years which prescribe technical protective means of the operating point as well as other means of controlling the other risks generated by the operation of these machines.

Any industrial machine such as a brake press must be the subjected to a systematic risk analysis which take into account all the physical and human elements which can interact thus leading to possible accidents. Over the years, methods have been devised aiming to to estimate the probability of occurrence of an accident starting from the identification of the contributing risk factors. In the case of industrial machines such as brake presses, these methods rarely refer to historical data regarding accidents because of the scarcity of these data. The judgement of participants in these analyses is then utilized. Although the results of these analyses help in elaborating risk control strategies, their subjective character continue to pose problems.

This thesis tackles the question of the estimation of the probability of occurrence of an accident which can arise on an industrial machine such as a brake press with a view towards making this analysis more quantitative but in a context where the historical data on accidents or knowledge on the factors contributing to accidents are limited. Towards that end, this thesis uses the concept of fuzzy logic as well as the structured technique of expert elicitation to quantify the judgements on the estimated probabilities.

In this thesis, a brake press is analyzed taking into account to types of failures which can affect its functioning namely those that can impact the protective systems which guard the point of operation of the machine as well as those failures which arise from the actions of the operators.

The contributing factors leading to accidents considered are analyzed using fault trees and Markov diagrams. The dynamic, sequential character of the genesis of an accident on a machine is also accounted for with this technique in this thesis.

The probability of accident thus estimated for the industrial system is then used furthermore in this thesis to optimize the cost associated with a given level of safety achieved.

This thesis is constituted of analyses of increasing complexity of work situations centered on a hydraulic brake pres. Firstly, the probability of occurrence of an accident suffered by an operator is estimated considering the failure of the protective device and the failure (error) of the operator. Then, this same situation is considered by incorporating rate of repair of the technical and human failure modes. Finally, elements of redundancy both technical and human are added to the model. This thesis show that the mathematical analysis method developed allows a more quantitative estimation of the probability associated with the risk being studied as well as an optimization of the cost associated with the achievement of a given targeted level of safety.

This thesis presents a method which increases the validity of the judgement of the probability of occurrence of events contributing to industrial accidents but these remain dependent on the judgements expressed by the participants in the analysis. We plan further research works which will refine the expert solicitation method in the context of industrial machine safety. Furthermore, the models expressing the cost related to maintaining a given level of safety will also be perfected. The models describing situations leading to accidents involving industrial machines will incorporate in future works other complexities such as non-constant failure rates.

Keywords: fuzzy logic, fuzzy numbers, risk analysis, Markov Chains, cost function, dynamic fault tree, expert elicitation, human factors.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF SYMBOLS AND UNITS OF MEASUREMENT

A	Availablity, unitless
c_{pc_i}	coefficient related to the cost of prevention for each component i, unitless
c_{fc_i}	coefficient related to the cost incurred due to failure of component i, unitless
c_{mc_i}	coefficient related to the maintainability of component i, unitless
h	Lagrange multiplier constraint function, unitless
kp_i	power of the i terms in cost function relating to prevention, unitless
kf_i	power of i terms in cost function relating to failure, unitless
km_i	power of i terms in cost function relating to maintainability, unitless
F	Unreliability, unitless
M	maintainability, unitless
P	probability vector in a Markov equation, unitless
Q	transition matrix in a Markov equation, unitless
R	Reliability, unitless

Greek letters

μ_X	a fuzzy number relating to quantity X, unit depending on context
$\mu_{\lambda_{d_i}}$	failure rate of protective device i , a fuzzy number in units of per h
$\mu_{\mu_{d_i}}$	repair rate of protective device i , a fuzzy number in units of per h
$\mu_{\lambda_{h_i}}$	failure rate of operator i, a fuzzy number in units of per h
$\mu_{\mu_{h_i}}$	repair rate of error by operaror i, a fuzzy number in u nits of per h
$\mu_{p_{\lambda_{d_i}}}$	probability of failure of protective device i, a fuzzy number, unitless

$\mu_{p_{\lambda_{h_i}}}$	probability of failure of operator i, a fuzzy number, unitless
$\mu_{p_{\mu_{d_i}}}$	probability of repair of protective device i, a fuzzy number, unitless
$\mu_{p_{\mu_{h_i}}}$	probability of repair of human error by operator i, a fuzzy number, unitless

LIST OF ABREVIATIONS AND ACRONYMS

FFTA	Fuzzy Fault Tree Analysis
FSFT	Fuzzy Static Fault Tree
FFMEA	Fuzzy Failure Mode and Effects Analysis
MTTF	Mean Time to Failure
MTBR	Mean Time between Repair
MTTR	Mean Time to Repair
RCA	Root Cause Analysis

INTRODUCTION

Brake presses are widely used in industry, especially in small and medium sized establishments because of their relative affordability and flexibility. They enable the production of a wide variety of sheet metal parts of various sizes and shapes.

The operation of brake presses, involves various important risks for the operators, as studies by Ngô et al. (1994), Venditti (2005) and Tran (2009) have investigated. Brake press operations most often contain an important human-machine interaction. In most press work stations, the operator manually feeds, holds and retrieves the part from the machine. The operator holds the piece-part and actuates the closing motion with a foot pedal, in most applications. An hazardous situation is thus created from the proximity of the workers hands to the press closing motion. A possible accident in such a situation is then that the worker gets his hands caught between the closing dies.

Safety regulations and standards therefore require that machines such as brake presses be equipped with protective devices which either prevent entry of the operator in the hazardous zone or stop the hazardous motion when parts of the workers body are in the hazardous zone. However, before implementing an effective safeguarding device, an effective risk assessment methodology is in order. The motivation for such an approach can easily be found in legislations, regulations and safety standards around the world. For example, in Québec, the *Act respecting occupational health and safety at work* requires that employers must take the necessary measures to protect the health, safety and physical integrity of the workers. Commonly used approaches to risk assessment rely on subjective perceptions. A quantitative approach provides more objective results. In this thesis, fault tree methodology will be used.

0.1 Fuzzy numbers in Risk assessment and fault tree analysis

In traditional fault tree analysis precisely. probability values are not always known. There is always uncertainty surrounding them. It has been pointed out, in many papers , see for instance Kabir (2018), that the probabilities associated with the events making up the tree are seldom known with precision and gathering the required information has proved to be very difficult. To remedy this difficulty, fuzzy logic concepts have proved useful. Fuzzy set theory first proposed by Zadeh (1965), has proven to be a useful methodology to cope with these cases where uncertainty and scarcity of data are important features.

So, fuzzy numbers can help in handling uncertainty about data. But the question remains, how to obtain the necessary data in the first place? The fuzzy logic approach can use the opinion of field experts to extract the probabilities or failure rates required in a fault tree analysis. This could be done informally, but in this thesis, this process will be done following guidelines enunciated in the literature under the denomination Expert Elicitation. These expert opinions take the form of qualitative linguistic estimates of the elicited probabilities. For example, the answers given can be expressed as ‘’the probability is low’’ or ‘’ It is very low’’. Fuzzy methodology is then utilized to convert these linguistic estimates into a quantitative expression.

In the literature the exact solicitation process is rarely detailed. In this thesis, however, brake press operators, supervisors and safety coordinators from three manufacturing companies were solicited and a questionnaire containing brief instructions and was used to gather the probability estimates necessary for this work.

0.2.1 Static forward problem

In this study, a «static» fuzzy fault tree analysis is performed on a metal brake press. The term «static» refers to the fact that the order in which events leading to a undesirable event (an accident) happens is not taken into account (as opposed to a dynamic view, which will be taken up later). The term «forward» refers to the process of evaluating the top event of a fault tree starting from the bottom events, with everything being done in terms of fuzzy numbers. In the static case, the probabilities of the basic events that lead to the undesirable event are assumed to remain constant during the time frame.

0.2.2 Dynamic forward problem

The analysis described so far takes a static view of the system; that is, the sequence in which the events leading to the undesirable event happens is not considered. A dynamic fault tree is one which takes into account the sequential nature of events which are related to the system under consideration.

0.3 Inverse problem

Fault trees can thus serve to identify the sequence and combination of basic events which lead to an undesirable event. But they can also be used to identify the most important basic events in terms of highest probability of occurrence or because these events can directly lead, by themselves, to the undesirable events. The «inverse» problem is thus tackled in this thesis, whereby one starts from the top event of a fault tree and deduces the probabilities of the bottom events which satisfy certain requirements.

0.4 Inverse problem. Optimization

The fault tree analysis described so far yields two valuable outputs: an estimate of the probability of occurrence of the top event (the accident being analyzed) and the sequence and combination of contributing basic events that may lead to the accident. From this, it might be asked: what basic event probabilities could lead to an accident probability within the acceptable limit set by regulation or by recognized safety standards at the lowest monetary cost possible? This could achieve the primary goal to protect workers but at the same time, optimize the resources of the enterprise. To this end, a cost function will be defined which will consider the costs incurred in maintaining a certain level of reliability, the costs necessary to properly maintain the machines and the costs of failures when they do occur.

0.5 Objectives of thesis

The general objective of this thesis is to develop a methodology for estimating the probability of occurrence of a given identified accident on an industrial brake press using the concepts and techniques of Fault tree analysis, Fuzzy numbers and logic, Expert Elicitation and Risk Management.

This thesis pursues also two specific objectives:

a. Apply the methodology to a so-named static case where the occurrence of an accident does not depend on the sequence of events. Both forward and inverse problems will be solved.

b. Apply the methodology to so-named dynamic cases where the sequence of events leading to an accident is important. Markov Diagram technique will be used in the forward problem. Both forward and inverse will be solved.

The methodology will include:

i. Consideration of human failure and repair rates
ii. Consideration of human redundancy

0.6 Organization of the thesis

The rest of the thesis is divided into seven chapters as follows:

Chapter 1 discusses the various definitions of risk. The probability aspect of risk, central to this thesis, is also presented in the various ways in which it appears in the literature. The risk analysis process is described. The various risk analysis techniques are reviewed. Chapter 2 presents the literature review showing the needs to develop a methodology for risk estimating quantitatively and safety cost optimization (Rapport technique DGA1031). The four following chapters, presented as articles published in Conferences, consist of study cases of increasing complexity. Every one of these chapters contains the pertaining Literature review, Methodology[1]. Chapter 3 (FSDM 2018) presents the static case with both the forward and the inverse problem. Chapter 4 (AFHE 2017) presents the forward problem for a dynamic situation with Markov diagram analysis. The inverse problem for this situation is similar to the one for

[1] The original papers contained the references. However, in order to comply with ÉTS standards, references have been keyed according to authors, instead of in the original numbering scheme, and have been all collected in the thesis Bibliography.

the static case and thus is not presented in the remainder of this work. Chapter 5 (AFHE 2018) describes the Expert Elicitation process used to extract data from field experts. Chapter 6 (AFHE 2020) presents the dynamic case using Markov Reliability Diagram including machine and human failure and repair. More complex situation where Human failure and redundancy are considered and is presented in chapter 7, which is in the form of a paper to be published. This chapter contains the inverse problem for both the dynamic case with repair and the dynamic case with repair and redundancy.

Finally, chapter 8 contains the integration of relevant conclusions from the chapters and provides also the recommendation for further study.

CHAPTER 1

LITERATURE REVIEW

1.1 Introduction

As a way to introduce the literature on risk analysis methods, let us introduce a colourful and original example taken from Winnick (1997), which, ironically, is a reference not on the subject of safety or risk but rather a textbook on chemical engineering thermodynamics. The author introduces a chapter on the thermodynamics of internal combustion engines with the following example (page 223):

«Imagine, if you will, the chances under today's regulatory climate, of introducing a new transportation mode to the nation where previously had existed only, say, electric cars with a top speed of 35 mph:

A new automobile is to be introduced in the U.S. market. It will have a top speed of 120 mph, powered by an engine fuelled by a highly volatile liquid composed of refined petroleum distillates. Each unit will have a capacity to carry about 25 gal, or enough to create an explosion and fire equivalent to 500 lbs of TNT. In addition, this fuel is toxic and carcinogenic if inhaled and harmful to the skin if handled without proper clothing. If accidentally leaked from a storage tank, of which there must be several thousand, it will pose a severe threat to ground and surface water supplies. The combustion products will contain incompletely burned polycyclic hydrocarbons and carbon monoxide, likely to be toxic to all plant and animal life, and nitrogen oxides, known to enter into photochemical reactions that will produce an intense, coloured haze in most urban areas.

The new automobile is to be made available to all segments of the market: from teenagers to the retired. It is anticipated that 100 millions of these vehicles will soon be flooding our highways and streets, day and night and in all weather conditions. Operators will have to pass a minimal skills test and eye test and have some knowledge of the rules of the road. Operation under the influence of mind-altering substances such as alcohol is discouraged, but because of the large number of vehicles anticipated it is unlikely that enforcement will be effective.»

This example contains many of the concepts used in the literature on machine safety, in particular in the standards, which we will now present.

1.2 Machine safety conceptual framework

Over the recent years (starting in the early 1990s), standards have been developed on machine safety, especially on the aspect regarding risk analysis. Two of the most regarded such standards are CSA Z432 and ISO12100. Furthermore, in Quebec many safety guides have been developed to help industry understand and implement the underlying ideas on machine safety and risk:

Risk is viewed in this segment of the literature in a framework composed of different elements which were illustrated in the above example and which we will know introduce.

The basis of any situation involving a risk[2] is a *hazard*: a potential source of harm. In the above example, two main hazards were mentioned:

- *Engine fuel*: highly volatile, flammable, explosive, toxic, carcinogenic, damaging to the environment
- *Vehicles* with speeds of 120 mph

In machine safety, hazards are, in particular, created by the motion of machine components and parts.

[2] We will expand on the definition of risk in the following pages.

These hazards can create many *hazardous situations* which are defined as situation in which people are exposed to these hazards:

- People can inhale fuel vapours
- People can inhale nitrogen oxide produce by the burning of the fuel
- People can expose their skin by handling liquid fuel without proper clothing
- Thousands of vehicles will circulate in close vicinity to each others, creating possibilities of collisions
- Vehicles will circulate in all weather conditions

In machine safety, hazardous situations are created when operators find themselves, by necessity, in close proximity to machines, notably when they must perform common tasks such as:

- Placing tools, parts in the machine
- Installing tools, fixtures in the machine
- Removing parts from a machine after a normal production cycle
- Cleaning in or around machine
- Un-jamming a part in a machine
- Inspecting a part.

Krϋger and al. (2009) give a comprehensive survey of human-machine interaction in a complex robot-assisted assembly line.

From these hazards and situations, *hazardous events*, which are events which can lead to harm, can be produced, such as:

- Health problems
- Fires and explosions
- Collisions between vehicles

In the field of machine safety, hazardous events commonly stem from two main sources:

- Technical (machine-related) failures and
- Human failures resulting from actions taken by operators, like for instance reaching into a press while it is in its downward motion to retrieve a misplaced part.

These hazardous events can therefore produce harm or more generally *damages* to property and the health and safety of humans.

Before we continue, it is worthwhile to review the literature on the definition of «risk», a concept which turns out to be surprisingly slippery and elusive.

1.3 Definitions of risk

Indeed, as Bahr (1997) puts it, «Risk is probably one subject we all feel we understand yet admit that we know nothing about.»

Kumamoto and Henley (1996) mention in their seminal treatise on risk, that risk is defined differently by various people. «This disagreement causes serious confusion in the field of risk assessment and management.»

The Webster's Collegiate Dictionary, for instance, defines risk as the chance of loss, the amount of possible loss, the type of loss that an insurance policy covers, and so forth. Le Petit Robert gives, in French, a similar definition. Such dictionary definitions are not sufficiently precise for our purposes.

To further illustrate the complex and multifaceted nature of risk, let us mention an example given by Horlick-Jones (1998):

«In 1992, Britain's Royal Society, one of the world's most prestigious scientific institutions, published a report entitled *Risk: Analysis, Perception and Management,* In his carefully worded preface to the preface, Sir Francis Graham-Smith, Vice-President of the Society, reflected upon its lineage and composition, and went on to say that:

«*Chapters 5 and 6 differ somewhat, in style and in content, from the earlier chapters. In particular, chapter 6 sets up, as an expository device, as series of referenced points of view as opposed positions in the debate. Some of the contending positions will undoubtedly strike many practitioners as extreme…*»

What was so strange or problematic about chapters 5 or 6? They were written by social scientists and dealt with risk perception and «related matters in the social context.» A committee later formed to investigate this «crisis» concluded that the root of the problem lied in the multidisciplinary nature of risk assessment and in the gulf that exists between social and physical and engineering scientists.

And yet, that society's perception of risk is an essential component of any quantitative risk evaluation is a fundamental idea first put forth by Starr (1969) in his seminal article published in *Science*. Starr argued that engineers' traditional method of cost-benefit risk analysis – equating risk to monetary return – was not sufficient to accurately determine technological risk.

Despite the fascination that these discussions exert, it is not our purpose to dwell further into these issues. We now, rather, turn to other (engineering) researchers, for further guidance on useful definitions of risk.

Modarres et al. (1997) offer a qualitative and a quantitative definition of risk. Qualitatively, risk can be defined as the potential of loss resulting from exposure to a hazard. Quantitatively, risk can be defined as the following set of triplets:

Si = a scenario of events that lead to hazard exposure

Pi = the likelihood of scenario i, and

Ci = the consequence of scenario i, i.e. a measure of loss or damage.

It is interesting to note that the definition of scenario is not in perfect accordance with the normalized definitions given above. Indeed, it is not clear if scenario of events corresponds to hazardous events or hazardous situation.

Villemeur (1988) proposes a broad definition of risk: Risk is the measure of a danger associating a measure of the occurrence of an undesirable event and a measure of its effects or consequences.

However, most authors, among them Kumamoto & Henley (1996), Ridley & Pierce (2006), Marszal & Scharpf (2002), Guyonnet (2006) define risk as being:

The product of the probability of the undesirable event and the extent of the consequences.

In summary, risk is a likelihood times a consequence. What does differ, however, among the different sources, is to what does the probability refer to exactly. Nevertheless, this is the definition we will adhere to for our purposes.

1.4 Risk management process

The literature, including in particular the standards on machine safety, refers often to the process of risk management. In order to put our work in the context of the general field of risk and safety, the process in question shall be described.

Following the presentation of Ridley & Pearce (2006), we can describe risk management as the series of stages in the design and manufacturing of a machine which are central to achieving its ultimate safety in use.

The machine safety standard ISO 12100-1 describes four such stages in the design and manufacture of a machine to ensure safe use with minimum risk:

1. Design hazard reduction terminating with remaining hazards that cannot be designed-out (ISO 12100-1; 5.2 and 5.3)
2. Risk assessment of the remaining hazards.
3. Risk reduction of the remaining hazards through the provision of safeguards based on the findings of the risk assessment (ISO 12100-1; 5.4)
4. Preparation of operating and maintenance manuals and information for the user (ISO 12100-1; 6.5)

In this work, we will focus on the first two stages of this process. We will attempt to develop tools that help eliminate hazards at the design stage in the case of a part which must be manufactured. Another of the tools we will work on is a number of quantitative risk assessment methods.

1.5 Risk assessment methods

A vast number of risk assessment methods have been developed over the years. Gauthier (1995), for instance, lists (and discusses) no less than ninety-three such methods. It must be added though that many of these methods are only variations of one another, while others apply to very specific industrial processes.

1.5.1 Semi-quantitative methods

1.5.1.1 Description of methods

These methods are very popular among practitioners in the manufacturing industries. In Quebec, the CSST, the regulatory body in charge of enforcing occupational health and safety laws, teaches these methods to its field inspectors. The IRSST, roughly the research arm of the CSST, has made extensive studies of these methods and has developed pedagogical guides aimed at industry (Pâques et al. (2006)).

These methods are based on (or, at the least, on variations thereof) the hazards-hazardous situations - events - damages framework presented earlier. We will refer to these methods as Operating and Support Hazard Analysis (O&SHA), following the classification made by Ericson (2005).

In these methods, once these elements identified, risk is evaluated (assessed) using four factors:

- Severity of damage (injury)
- Frequency of exposure to hazard
- Probability of occurrence of hazardous event
- Possibility of avoidance of the damage

The next step is to devise a risk scoring system. In semi-quantitative methods, scales are used for each of the factors. As Main (2004) points out, these scoring schemes attract considerable attention in discussions of risk assessment processes, as they can be contentious and confusing.

IRSST has promoted the following system.
Severity is assessed on a two-level scale:

- Level 1 Slight consequences, reversible injuries, (stitches, medical attention)
- Level 2 Serious consequences, irreversible injuries (amputations, loss of vision, death)

Frequency of exposure is, as well, assessed on a two-level scale:

- Level 1 Infrequent exposure (less than daily)
- Level 2 frequent exposure (daily)

Probability of occurrence of the hazardous event is a more complex factor to rate. The method put forward by the CSST and the IRSST distinguishes between events which originate from a human action from those which basically are machine components failures. Without going into details, a three-level scale is used.

Possibility of avoidance is considered either impossible (level 2) or possible (level 1).

These ratings are combined to yield the overall risk rating according to a graph-type diagram or a matrix-type risk rating scheme.

A second type of semi-quantitative method is the Failure mode and Effects Analysis. This method aims at identifying, as the name implies, failure modes of the system under consideration. It therefore focuses less on the hazardous situation aspect of risk, the human presence. It is nevertheless used extensively in industry in particular for ensuring product safety before launch into the market. Probabilities of failures and severity are also estimated on a qualitative scale.

In the literature, both these methods have been used by Jiang and Cheng (1990) in robotics safety.

1.5.1.2 Limitations and advantages of semi-quantitative methods

Semi-quantitative methods, as we have alluded, have been heavily criticised over the years. One of the most perceptive papers evaluating these methods was published in *Prevent Focus* (Anonymous (2009)). In this reference, the most important criticism aimed at these methods is the fact that different users will obtain a different result in face of the same machine or work situation. In other words, these methods are highly subjective. The same observation is made by Pâques et al. (2006). Practice in the field also leads to the same conclusion.

One study cited by the authors dealt with trench excavation on a construction site in Belgium. The risk of a land slide was rated as negligible by the heavy-machinery operator (risk score 3), possible by the company safety advisor (risk score 38) and major by a safety coordinator, a public health doctor and a student (risk score 1500). Other risks considered saw similar fluctuations. The priorities that are drawn up as a result of these analyses vary considerably as well, which lead to confusion. Another disadvantage is that the method is ill-suited to long-term health risks such as those related to ergonomics, noise, contaminants, and the like.

Moreover, the risk scale does not give a proportionality, in the sense that a score (a risk) of 10 is not necessarily twice as big as a score (a risk) of 5.

Another disadvantage of these methods is that they only identify the immediate causes that lead to a hazardous event. The underlying causes are not investigated.

On the other hand, semi-quantitative methods have a very positive impact on all personnel involved with the work. Machine operators, for example, become familiar with concepts of severity of possible injuries, probabilities of injuries and possible accident scenarios. All in all, these methods have a pedagogical value in the workplace.

Furthermore, semi-qualitative method, retain their value, as they serve to identify the hazards which will be used in the more quantitative and in-depth methods which will next be discussed. Such an approach was promoted and applied by some authors such as Dougherty (1994), in an editorial paper in a major journal.

1.6 Quantitative risk assessment methods

As the foregoing discussion hopefully has demonstrated, there is a need for a more quantitative approach to risk. Some methods have emerged as alternatives, in particular, failure tree methods, event tree methods, Markov chains and more recently, at least in the field of machine safety, Petri nets.

Even though, particularly in the case of fault and event tree methods, these methods have been used since the sixties, their use has been largely concentrated in the more technologically complex industries such as nuclear energy, petrochemical, chemical process industries, aerospace and defence industries. As some authors such as Moriyama and Ohtani (2009) and Fera and Macchiaroli (2010) have pointed out, their use in connection with more traditional manufacturing processes such as metal machining for instance and in small and medium-sized industries has been more limited. Therefore there seems to be a need to study these methods in those contexts.

1.6.1 Fault tree analysis

Fault tree analysis is a deductive method in as much as one, starting from an undesirable hazardous event previously identified attempts to determine the chain of events or combination of events which eventually can lead to that event. This method enables one to backtrack from one contributing factor to another down to the basic events which are considered to be at the root of the hazardous event.

The following discussion is largely based on INERIS (2003).

Basic events generally correspond to:

- Elementary events which are generally sufficiently well understood such that it is not useful to investigate their underlying causes. Hence, their probability of occurrence is known.
- Events which can be further decomposed but which are not for they are not deemed of interest.
- Events whose causes are going to be developed in subsequent studies.
- Events which occur under normal operating and environmental conditions (also called primary failures in the literature)

Once the basic events identified, failure tree analysis proceeds on the following principles:

- The events are independent, mutually exclusive (in the sense understood in probability theory). So-called common-cause failures require careful attention as they can seriously degrade the reliability and safety of a system or process.
- The basic events are not decomposable in more basic entities.
- Their frequency or probability of occurrence can be evaluated.

Thus, the fault tree analysis enables one to identify the sequences and combinations of events which can lead to the undesirable hazardous event. However, as Kumamoto & Henley (1996) point out, a fault tree is a snapshot taken at a certain time t.

The links between the various basic events are implemented via logical Boolean AND and OR gates. The results of the analysis then take a tree-like structure.

With the help of mathematical and probability rules, the probability of occurrence of the final event being investigated can be evaluated (at least in theory) in terms of the probabilities of the basic events identified in the analysis.

The starting point of a fault tree analysis is, as already mentioned, the identification of the hazardous event or events. But even prior to this step, a solid knowledge of the machine, process or system must be gained.

Let us consider now an example (see figure 1) of evaluation of a fault tree, taken from Villemeur (1988). We first notice that events A, B and C appear several times in the tree: therefore it does appear to be independence of the basic events. It is necessary therefore to eliminate these redundancies before evaluating the tree.

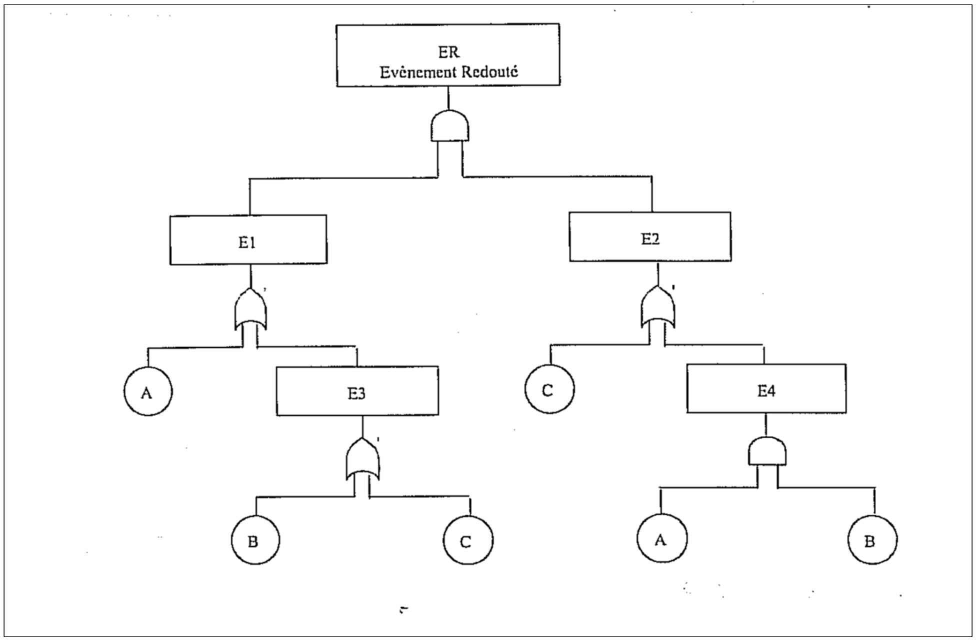

Figure 1.1 Fault tree example. (Source: Villemeur, 1988))

The elimination of these false redundancies can be done with several methods which are mostly based on the principles of minimal cut-sets and tree reduction.

A minimal cut-set is the smallest combination of events which can lead to the undesirable event. In the preceding example, events A, B and C effectively lead to the top event. However it does not constitute a minimal cut-set since the A, B combination can be at the origin of the top event.

Minimal cut-sets have to be searched using the rules of Boolean algebra.

Thus, in our example,

ER = E1*E2

But E1 = A*E3 with E3= B + C

E2 = C + E4 with E4 = A*B

So, ER = (A = B + C)* (C+A*B) = A*C + A*B + B*C + A*B + C + C*A*B
Using the Boolean absorption rule, A*C + C= C and A*B A*B*C = A*B
ER = C + A*B + B*C + A*B
By the idempotence rule, we have A*B + A*B = A*B

Thence, ER = C + A*B

Thus, event C alone or the combination of events A and B lead to the undesirable event. There are no smaller combinations leading to that event. The minimal cut-sets are thus C and A*B.

Once the fault tree reduced in this form, a quantitative estimation of the probability of occurrence of the undesirable event is possible. This is done by combining the probabilities associated with the basic events.

In practice, it is often difficult to obtain exact values for the various probabilities. In order to estimate these, it is possible to invoke:

- data bases (in particular for machine components failures)
- expert judgements
- tests when possible
- past experience on the equipment under consideration or similar ones.

Calculations then proceeds based on the following probability laws:
OR gates:
P(S) = P(E1) + P(E2) – P(E1)*P(E2) if both events can both occur
= P(E1) + P(E2) if the probabilities are small.

AND gates:
P(S) = P(E1)* P(E2)

As an example, let us apply this procedure to the above tree, supposing that the basic probabilities are:

P(A) = 10E-3

P(B) = 10E-2

P(C) = 10E-6

We then obtain:

P(ER) = P(C+A*8) = P(C) + P(A)*P(B)-P(A)*P(B)*P(C)

Hence,

P(ER) = P(C) + P(A)*P(B),

which yields a final probability of 1.1E-5

In Quebec, the IRSST has applied Fault Tree Analysis in a qualitative fashion, without probability calculations, to lift truck loading of tractor-trailers (Gauthier et al. (2004)), conveyor safety (Giraud et al., (2003)), and textile-weaving machines (Gagné et al., (2004)).

1.6.2 Event tree analysis

This method was developed in the 1970s in the nuclear industry. Its use has spread to other industries. The discussion that follows is modelled after Marszal and Scharpf (2002).

Inspired by the fault tree analysis, this method allows the estimation of probabilities of occurrences of accident sequences. It is indeed used in particular for the investigation of accidents in order to establish the chain of events that lead to the accident.

Unlike the fault tree method which being deductive in nature proceeds from the undesirable event under study to its causes, the event tree method starts from the failure of a system and attempts to determine the chain of events that results from it. A tree-like structure is thus formed again and the tree branches determine the different sequence paths to the various outcomes. A typical event tree then takes a form like the illustrated in figure 2.

Branches of event trees are usually complementary events. For instance, a branch could be the failure of a relief valve. The event set includes two complementary events, namely: (1) relief valve fails and (2) relief valve operates. Although complementary events often occur, this is not always the case. For instance, an event tree branch might be the state of a chemical that is released, with a set of three possible states: (1) gas, (2) liquid and (3) solid. In this case, the set of events does not even have to be mutually exclusive. If liquefied propane were released, the state of the release would be liquid and gas, so both branches would be true.

An interesting question which this method raises concerns the sequence of the subsequent events. Is the order in which these events cascade relevant? It appears that the answer is not necessarily in all cases. The next two methods are designed to address this problem more properly.

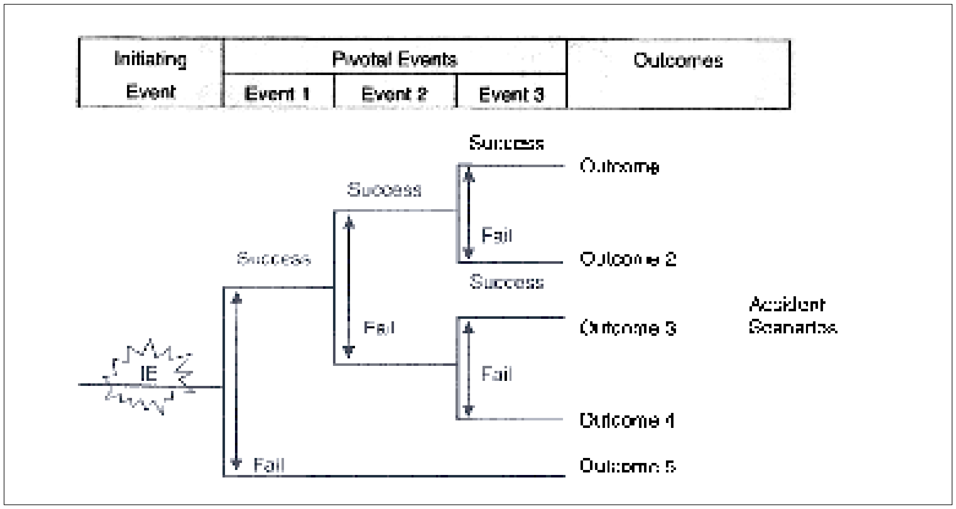

Figure 1.2 Event tree example (Source: Ericson, 2005)

The quantitative evaluation of an event tree is calculated as the logical combination of the events that fit together to cause the outcome, starting with the initiating events. These events are related through a logical AND. In this case, the probability of the combination of the events is calculated using probability multiplication.

In the literature, Khodabadehloo (1996) has applied both Fault and Event Tree analyses to a robot system. The author suggests that both methods are valuable mostly a means of developing awareness of the hazards present in a system and hence provide a basis for the selection of preventive measures. The assignment of probabilities is seen by the author as more difficult, especially in regards to human action.

1.6.3 Markov analysis

Markov analysis is a technique used for modelling system state transitions and calculating the probability of reaching various system states from the model (Ericson (2005)). Markov analysis is a tool for modelling systems (often complex) involving timing, sequencing, repair, redundancy, and fault tolerance.

Markov chains are random processes in which changes occur only at the fixed times. On the other hand, Markov processes involve changes that occur continuously over time, where the future depends only on the present state and is independent of history.

According to Ericson (2005), Markov analysis does not provide the safety analyst with as much benefit as the other techniques such as fault tree and event tree techniques. Markov analysis does not identify the hazards; its main purpose is to model state transitions for better understanding of the system as well as calculating failure state probabilities. This same author provides also examples where Markov and Fault tree analyses are used on the same systems and compared.

To illustrate Markov analysis, typical of what is found in textbooks and papers, consider the following example from Andrews and Moss (2002) for a simple single-component failure/repair process.

The component can be considered to start in the working state at time t=0. Transition from the working state1, to the failed state, 2, occurs with constant rate λ. Therefore the probability of failure at t + dt given that the component is working at t is λdt. Failure is immediately revealed and transition back to the working state, the repair process, occurs at the constant rate μ. For component in state 1, they can either move to state 2 with probability λdt or remain in the state 1 with probability 1 – λdt. The time interval dt must be small enough such that the two or more transitions cannot occur in dt.

Let x(t) be an indicator variable denoting the state of the system at time t, i.e.

x(t) = 1 failed or 0 working

The probability that component exists in the failed state after time increment dt only the state of the component at present, i.e.

P [x(t+dt) = 1] = P (the component was working at time t and undergoes failure in time dt OR the component was failed at time t and remained in the failed state during dt).
P [x(t+dt) = 1] = P [x(t) = 0] λdt + P [x(t) = 1] (1 – μdt).

This equation can be generalized to the following form :

$$P_f(t + dt) = P_w(t)\,\lambda dt + P_f(t)\,(1 - \mu dt)$$

Re-arranging

$$P_f(t + dt) - P_f(t) = P_w(t)\,\lambda - P_f(t)\,\mu$$

$$\frac{P(t + dt) - P(t)}{dt} = P(t)\lambda - P(t)\mu$$

This equation can be solved to yield

$$\mathrm{P(t)} = \frac{\mu}{\lambda + \mu} + \frac{\lambda(e - (\lambda + \mu)t)}{\lambda + \mu}$$

When considering more complex systems more than one equation arise and the mathematical description of the system dynamics takes on a matrix form.

1.6.4 Petri nets

In his introduction to Petri net analysis, Ericson (2005) describes the possible applications of this technique in much the same way as he did for Markov analysis. Petri nets are useful for identifying hazards associated with timing, state transitions, sequencing and repair. Petri net analysis consists of drawing graphical diagrams in order to locate and understand design problems. This graphical model can then be translated into a mathematical model for probability calculations. Ericson (2005) mentions that Petri nets, in the field of system safety, have been used mainly in the study of software control systems. Indeed, a search through journals such as *Reliability Engineering and Systems Safety*, confirms this observation. Furthermore, Vernez et al. (2003) state that «despite the PNs (Petri nets) intrinsic properties regarding safety, safety-oriented uses are still scarce».

Petri nets show some similarities with Markov processes in that it shows graphically the various states of a system as circles with arcs between them indicating transitions. These transitions occur at random times when certain conditions are met. States, transitions, conditions are represented graphically using certain symbols. The following figure (figure 3), taken from Murata (1989), provides an example of the symbols and the terminology used with Petri nets.

Consider the well-known chemical reaction: $2H_2 + O_2 \rightarrow 2\ H_2O$. Two *tokens* in each input place in figure show that two units of H2 and O are available, and the transition t is *enabled*.

After *firing* transition t, the *marking* will change to the one shown in the figure, where the transition t is no longer enabled.

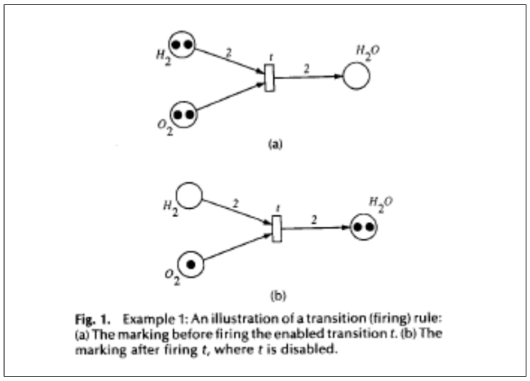

Fig. 1. Example 1: An illustration of a transition (firing) rule: (a) The marking before firing the enabled transition *t*. (b) The marking after firing *t*, where *t* is disabled.

Figure 1.3 Petri net concept (Source : Murata, 1988)

As a more general example, figure 4, from a significant paper by Adamyan and He (2002), shows a Petri net with an initial *state* indicated by the number of *tokens* (black dots) in corresponding *places*. The transitions are represented by bars. The system under study is a most interesting application of the method to a robotic cell.

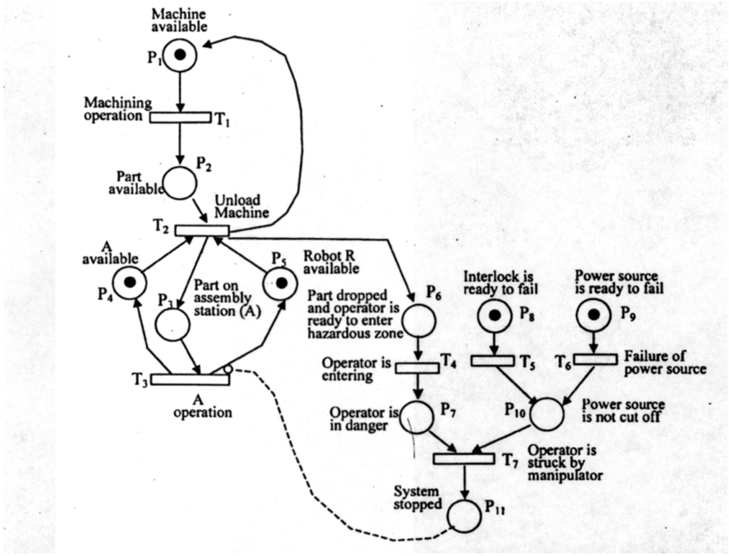

Figure 1.4 Fault Petri net example (Source: Adamyan and He, 2002)

In a Petri net, the firing of a transition obeys certain rules:

- Tokens in place with arcs towards a transition indicate that the transition is ready to fire (event to occur).
- Upon firing, transition t consumes one token along each input arc.
- Upon firing, transition t produces one token along each output arc.

Once the system under study has been represented using the Petri net graphic language, it is then possible to make probability calculations.

The steps in the analysis go as follows:

- Define the set of transitions corresponding to the events that pertain to the hazard studied along with associated firing rates λ_i analogous to failure rates in fault tree, event tree analyses.
- Define the markings denoting the states of the state as it evolves through time.
- Calculate probability distribution of the time intervals between the time at which the transition is able to fire and the time at which the firing is completed. Intuitively, these are related to the failure rates just defined and, thus, are also similar to times between failures.
- Calculate transitional probabilities based on the preceding step.
- The final probability of hazardous event occurrence which is what is being sought will then be given as the sum of the various transitional probabilities.

A significant difference between Petri net analysis and more «traditional» methods in safety such as Fault tree analysis lies in the timing of the events being considered.

Indeed, as Vernez et al. (2003) have explained,

«the FTA (fault tree analysis) process is only able to cope with trivial time logic: each event entering a logical gate (a causal event) must occur before the outgoing event (a consequence).

Time logic, especially when it concerns events duration, is not fully taken into account into fault or event-trees. Consequently, systems with dynamic constraints, such as concurrency or parallelism, cannot be depicted accurately in such ‘‘branched chain’’ structures. ».

In other words, in fault tree analysis, the sequences of the failures are assumed to be given. With Petri nets, it becomes possible to identify many possible failure sequences.

Returning to the example by Adamyan et He (2002), they considered the situation where an operator enters a robotic cell to retrieve a dropped part and is struck by the robot due to an interlock failure. The pertinent sequence for study is: interlock fails before operator enters the hazardous zone.

It must be noted, on the other hand, that Markov analysis should provide the same benefit. However, Adamyan and He (2002) claim that in Petri nets, the number of places and transitions increase only slightly with system complexity, whereas the number of states in Markov chains increases exponentially.

Kontogiannis et al. (2000) have applied, for their part, Fault tree analysis and Petri analysis to the Piper Alpha offshore oil rig explosion which occurred in 1988. The authors give a table comparing the two methods. It serves as an interesting reference for a similar exercise in the context of this thesis.

1.7 Human reliability

Implementation of the quantitative methods just described will involve taking into account failures related to human presence, in another words, human reliability.

As mentioned by numerous authors, human reliability is a difficult issue, by virtue of the subject matter itself. According to Modarres (2006), literature shows that that there is not a strong consensus on the best way to capture all human actions and quantify human error probabilities. Modarres (2006) cites three major limitations and difficulties in human reliability analysis:

- Human behaviour is complex
- Human actions cannot be considered to have binary success and failure states, as in hardware failure.
- The most difficult problem with human reliability is the lack of appropriate data on human behaviour in extreme situations.

On this theme, a fascinating aspect of the human reliability problem (which we will only mention) is the difference between the prescribed task and the real activity of machine operators; see, for example, Montmayeul et al. (1994).

Despite these limitations, various methods have been devised in human reliability:
SHARP (Systematic human action reliability procedure) attempts to identify all human actions involved in a given situation and uses fault trees and event trees. The probabilities are estimated from various sources such as accident reports, safety procedures, reliability studies, etc. Computer simulations of human performance are also used.

Expert Judgement Methods, as the name suggests, relies on a team of experts to supply the appropriate human reliability data. The method is similar to decision-making techniques such as AHP (Analytical Hierarchical Process). This approach has been criticised in the literature as reported by Bley et al. (1992). The authors state that expert opinions are often received with scepticism. The authors see the value of expert opinions as a way of analyzing the relevant evidence once a considerable effort has been made in gathering it.

THERP (Technique for human error rate prediction) is the oldest and most widely used method in this field. The method categorizes human errors as:

- Errors of omission
- Errors of commission
- Selection error

- Sequence error
- Time error
- Qualitative error (doing too little or too much)

The basic tool then used is an event tree in which task sequences are considered. If the possible human action sequences are considered and associated probabilities known, overall reliability of the task can be estimated. Holywell (1996) gives a discussion of this technique applied to an emergency cooling system in a nuclear plant. Johnson (1996) also integrates Markov chains in his human error analysis, also in the context of nuclear industry. Stanton and Baber (1996) use a states-transition method akin to Markov analysis to model electrical repair work.

Moriyama et Ohtani (2009) use these concepts and develop elaborate tables where human reliability data is gathered from various sources for a variety of tasks performed by workers on commonly used equipment in the context of small- and medium-sized industries.

On the other end of the spectrum, Raafat (1989) in his an accident analysis involving a stamping press uses a very simple model of human error probability. The action «operator places part of body between closing dies» as simply the percentage of time the operator performs this action compared to his total time spent operating the press. Finally, and interestingly, Pyy and Whalstrom (1988) review the different approaches to human reliability which have been mentioned and give a useful selection matrix according to the nature of the system being studied.

1.8 Machine reliability data

Obtaining reliability data is equally important with regards to technical failure modes. Data bases exist and manufacturers keep data on component failure rates .

In the literature, there appear to be some recent papers on reliability data. Among them, Wang et al. (1999) and Wang et al. (2001) have collected failure rates on 80 CNC lathes over a period of two years, in the Chinese industry.

CHAPTER 2

FUZZY APPROACH TO INDUSTRIAL PROCESSES [3]

Accepted for publication as a book chapter in
Advances in Fuzzy Multidimensional Approach in Social Science (Social Economics)

Abstract

Industrial processes and machines (industrial systems) pose risks in terms of equipment failure and worker accidents. Occupational laws and regulations as well as safety codes and standards call for a risk assessment process in order to effectively identify measures to prevent these risks from materializing. Risk assessment involves identifying the risk factors and estimating their importance in terms of their associated probability of occurrence and the severity of the consequences they can bring about. Probabilities are commonly expressed in terms of linguistic expressions (such as: ‘’very low, ‘’low’’, ‘’moderate’’, ‘’high’’ and many other terms). There is therefore a subjectivity and vagueness associated with these assessments. Other methods such as fault trees are also often used to identify the combinations of events which can lead to accident-causing events. If data is available such as failure and human error probabilities the probability of occurrence of accidental events could be calculated. But in real life, often, these values are not known precisely. Furthermore, these analyses often have to be performed without full knowledge of the processes being examined. There is therefore a degree of uncertainty associated with the data and the knowledge used in the analyses. In these situations, fuzzy numbers are an attractive method for dealing and taking into account this uncertainty. A

[3] Venditti, T.,Tran, N.D.P., Ngô, A.D. (2020) Advances in Fuzzy Multidimensional Approach in Social Science (Social Economics). G. Betti and A. Lemmi, editors. Routledge Publishing House. London (U.K.).

fuzzy probability assessment number or linguistic expression instead of being a single data can belong instead to several sets in various degrees of memberships. Using the rules of fuzzy logic, a fuzzy number can then be calculated as a single number encapsulating the underlying associated uncertainty. In this chapter, fuzzy concepts are explained and applied to industrial risk estimation methods and fault tree analysis.

2.1 Introduction

The operation of industrial machines, involves various risks, particularly for the operators. In most jurisdictions, employers must take the necessary measures to protect the health, safety and physical integrity of the workers .Among these measures, performing a risk assessment is paramount. The importance of risk assessment appears clearly for instance in the European Machinery Directive, which requires a risk assessment to be performed and be documented during the machine design phase, (Hietikko, M. et al. 2011).

By the same token, engineers who design machines are required by their Professional Code of Practice to know and follow recognized safety standards which are published by various institutions around the world such as CSA, ISO, ANSI and others, (Hietikko, M. et al., 2011). These standards demand risk assessment be performed. Risk assessment more specifically requires identification of the hazards as well as an estimation (qualitative, as it is often seen in practice, or quantitative) of the probability of occurrence of the events associated with these hazards and of the gravity of the consequences following the event.

2.2 Risk and Uncertainty

By definition, risk analysis deals with uncertain situations, that is, with situations in which we do not have complete and accurate knowledge about the state of the system, (Gurcali, and Mungen, 2009). It is therefore very important to be able to represent uncertainty in risk analysis as adequately as possible.

Three types of uncertainties can be distinguished:

1. completeness uncertainty,
2. modeling uncertainty,
3. parameter uncertainty.

The completeness uncertainty refers to the question whether all significant phenomena and all relationships have been considered. This uncertainty is difficult to quantify but this type is a major contributor in a qualitative hazard analysis.

Modeling uncertainty refers to inadequacies and deficiency in various models used to assess accident scenario probabilities and consequences. Availability and validity of these models may enable the assessment of different degrees of belief in each model. This is a major type of uncertainty in consequence assessment. This is a subjective type of uncertainty of knowledge elicited from experts, which is often incomplete, imprecise and fragmentary.

The imprecision and inaccuracies in the parameters which are used as an input to risk assessment models are called parameter uncertainty.

In addition, as we have seen, risk assessment is a complex subject shrouded in uncertainty and vagueness. Vague terms are unavoidable, since safety professionals often assess risks in qualitative linguistic terms.

2.3 Modelling uncertainty with fuzzy sets

Under these circumstances, conventional approaches may not be able to model safety effectively. These safety assessment approaches, such as probabilistic risk assessment, have been widely utilized; but they may be difficult to use under circumstances where there is a lack of information about past experience. For these cases, fuzzy sets are a useful tool.

A fundamental idea behind the concept of fuzzy number is that it may belong to more than one set, (Markowski et al., 2010). This multiple membership to many sets concept provides not only a useful representation of uncertainties, but also a meaningful representation of vague concepts expressed in natural language, (Markowski et al., 2009). Thus, fuzzy variables can reflect and express uncertainties in measurements, observations or knowledge. Traditional variables, which we may refer to as crisp variables, do not have this capability. Although the definition of states by crisp sets is mathematically correct, it is unrealistic in the face of unavoidable uncertainty for certain applications.

2.4 Applications of fuzzy concepts to risk and safety

Fuzzy logic has been used in various contexts related to work and safety, as can be seen by consulting the references at the end of this chapter, such as: Oil drilling risk, safety and ergonomics in oil & gas refineries, construction site safety, safety in chemical process plants and many others.

2.4.1 Chemical safety

Here is now an example of the use of fuzzy numbers in the context of chemical safety, (Kentel, et al. 2004), compared the behaviour of an interval-based safety index and the fuzzy logic approach for a simplified chemical reaction involved in the industrial production of acetic acid. The reaction takes place around the proposed pressure range (25–50 bar) and temperature range (150–300 °C). At a pressure of 24 bar and temperature of 149°C, the interval-based index indicates an inherent safety score of 27, while the fuzzy logic-based index provides a score of 9.95. When conditions change to 25 bar and temperature to 150 °C, the interval-based index yields an inherent safety score of 29, and the fuzzy logic index a score of 10.04. When the conditions are changed to the upper limits of the temperature and pressure intervals (300 °C and 50 bar), the interval-based index is not sensitive, resulting in a score of 29, while the fuzzy logic index presents 10.83. These results show that the fuzzy approach is more sensitive to changes in index due to the smooth transitions between sub-ranges provided by the overlap of the fuzzy sets, (Jamshidi et al., 2013). However, some others use fuzzy sets (distributions) that do not overlap for «ease of analysis», (Gentile, M. et al., 2003).

2.4.2 Fuzzy risk scale in occupational health and safety

Risk indices are often used to estimate the risk levels associated with various industrial work situations, (Murè and Demichela, 2009). The following example from (Gurcanli, and Mungen, 2009) illustrates the concept.

Risk can be defined conveniently as:

Risk = Probability of Occurence x Severity x Current Safety Level = AL x AS x CSL.

Each parameter can be characterized by a score between say 0 and 10 which can be represented on a fuzzy scale. As explained previously, the idea of a fuzzy number is that it can be belong to more than one set.

For instance, consider a potentially hazardous situation to which workers can be exposed. Experts have estimated that the probability of occurrence AL of an injury in such a situation as 7.69 on 10 (based on an accepted risk estimation scheme).

Fuzzy-logic based risk calculation shows that AL=7.69 belongs at a 46,2 % degree to the set ‘’Reasonably Low‘’ and at a 53,8 % degree to the fuzzy set «Average». The same procedure is applied to the 2 other parameters AS and CSL. These fuzzy values can then be ‘’aggregated‘’ so as to obtain a final value, expressed as a numerical value. Ultimately, the value of the Risk index can then be found by multiplication.

2.4.3 Risk matrices

Risk matrices are another well-known technique used in occupational health and safety used to express risk levels. The concept of a fuzzy number belonging to many sets can generate a risk matrix with more precise, nuanced risk levels, (Markowski and Mannan, 2008). An example from this same reference will illustrate the point.

Consider the following “traditional” risk matrix (Table 2.1).

Table 2.1 An example of standard risk matrix

	I	II	III	IV	V
G	TNA	TNA	NA	NA	NA
F	TA	TNA	TNA	NA	NA
E	TA	TA	TNA	TNA	NA
D	A	TA	TA	TA	TNA
C	A	A	TA	TA	TNA
B	A	A	A	A	TA
A	A	A	A	A	TA

Key: Frequency categories: A: remote, B: unlikely, C: very low, L: low, M: medium, H: high, G: very high; Severity categories: I: negligible, II: low,III: moderate, IV: high, V: catastrophic; risk categories: A: acceptable, TA: tolerable–acceptable, TNA: tolerable–unacceptable, NA: unacceptable.

Consider a particular risk for which the Risk Index is calculated to be equal to 2 corresponding to a risk level TA which is Tolerable-Acceptable. A fuzzy risk assessment, on the other hand, yields a value of 1.35 belonging to a 0.75 extent to the TA fuzzy set and to a 0.25 extent to the A fuzzy set, Acceptable. Thus, the fuzzy assessment is more nuanced.

2.4.4 Fuzzy concepts in Human Reliability Analyses

Human error is a component of all industrial machines whenever human operation and interaction is necessary. Various techniques have been developed to analyze human reliability and estimate the probability of occurrence of a human error. Two such techniques are known by the acronyms HEART and CREAM.

2.4.4.1 Fuzzy HEART

The HEART technique is based on the principle that any task performance is influenced by Error Promoting Conditions (EPCs), also called Performance Shaping Factors (PSFs), Akyuz et al., 2008). Nine generic tasks have been identified and for them, human (un)reliability values have been proposed.

The human error probability for a given task is calculated with the help of the expression:

$$P = P_0 \left\{ \prod_i [EPC_i - 1]\, A_{P_i} + 1 \right\}$$

Where the index i run through all the EPCs and P_0 is the failure probability value associated with a generic identified task taken from a list of nine tasks. The factors, A_{P_i} are assigned to each EPC_i by experts and are used to modify the influence of the EPC_i on the probability of occurrence of the actual task being considered. These factors can be expressed as fuzzy numbers reflecting the experts' opinions.

2.4.4.2 Fuzzy CREAM

The basis CREAM model assumes that the probability of human failure depends on the level of control and knowledge of the operator regarding the task which he is requested to perform,(Castiglia and Giardina, 2013).

Nine so-called Contextual Control Modes are defined which are considered to determine four types of human actions that can be followed for a given task. These are defined as "scrambled", "opportunistic", "tactical", and "strategic". For each, human error probability values are assumed according to Table 2.2.

For a given scenario in which the task is performed, the control mode is determined by nine Common Performance Conditions (CPCs) that qualify the context in terms of linguistic descriptors. For example, regarding "Adequacy of Organization" the descriptors are: "deficient", "inefficient", "efficient", and "very efficient", depending on whether the organization reduces or improves human performance levels.

To estimate the probability of human error, the procedure applies “if-then-else” fuzzy rules (fuzzy inference) following the logic of CREAM, as described above. The input parameters are the fuzzy CPCs sets and the output values are the fuzzy action failure probabilities, in accordance with Table 2. An example will make the process clearer (from the same reference).
“If the adequacy of organization (CPC number 1) is inefficient AND the working conditions (CPC number 2) are compatible AND the availability of procedures and plans (CPC number 4) is acceptable AND the adequacy of man machine interface and operational support (CPC number 3) is tolerable AND the number of simultaneous goals (CPC number 5) is more than actual capacity AND the available time (CPC number 6) is adequate AND the time of the day (CPC number 7) is day AND the adequacy of training and experience (CPC number 8) is highly accurate AND the crew collaboration quality (CPC number 9) is efficient, THEN the operator would act in a ‘’OPPORTUNISTIC way”.
This fuzzy probability output is then defuzzified by one of the methods in use in fuzzy logic such as, for instance, the centroid method, thus yielding the crisp human failure probability value for the task being analyzed. These probability intervals quite naturally lend themselves to a triangular fuzzy number representation.

Table 2.2 Human Action Failure Probability in CREAM Method

Control Mode	Action Failure Probability
Strategic	$5 \times 10^{-6} < p < 0.01$
Tactical	$0.001 < p < 0.1$
Opportunistic	$0.01 < p < 0.5$
Scrambled	$0.1 < p < 1.0$

2.5 Fuzzy numbers

In safety analyses like the ones we just surveyed, then, we often do not know the precise values of the probabilities of occurrence or of failure of the systems or of its components. So one way to deal with this problem is to consider that the variables of interest follow a normal probability distribution with a mean value and a standard deviation. However, another approach to the problem is to use fuzzy triangular number.

2.5.1 Fuzzy numbers

A fuzzy number is represented by three numbers <a_1, a_2, a_3>. This representation is interpreted as a membership function such as depicted in figure 2.1.

$$\mu_A(\mathbf{x}) = \begin{cases} \mathbf{0} & \mathbf{x} < \mathbf{a_1} \\ \dfrac{\mathbf{X} - \mathbf{a_1}}{\mathbf{a_2} - \mathbf{a_1}} & \textbf{for } \mathbf{a_1} \leq \mathbf{x} \leq \mathbf{a_2} \\ \dfrac{\mathbf{a_3} - \mathbf{X}}{\mathbf{a_3} - \mathbf{a_2}} & \textbf{for } \mathbf{a_2} \leq \mathbf{x} \leq \mathbf{a_3} \\ \mathbf{0} & \mathbf{x} > \mathbf{a_3} \end{cases}$$

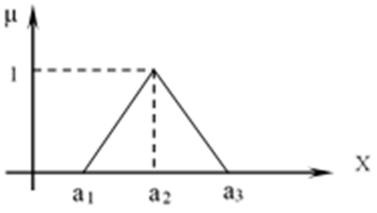

Figure 2.1 A fuzzy number

In this representation, a_2 corresponds to a membership value of 1 meaning that we think that the most probable value of the variable under consideration is a_2. So a_2 is akin to the mean value in a normal probability distribution. In this representation, we mean also that the variable under interest lies between the values a_1 and a_3, which have “membership values” of 0. In other words, a_1 and a_3 are akin to the 3σ values from the mean in a standard normal probability distribution.

2.5.2 Introduction to fuzzy operations and operators

In order to perform calculations on fuzzy fault trees, arithmetic operations on fuzzy numbers have to be introduced.

2.5.2.1 Basic Arithmetical Operations with Fuzzy Numbers for ease of Computation

The following are the four operations that can be performed on fuzzy triangular numbers, (Gani, 2012):

Let μ_A=<a_1, a_2, a_3> and μ_B = <b_1, b_2, b_3> where a_i and b_i are positive numbers, then we have:

(i) Addition: $\mu_A + \mu_B$ = <a_1+ b_1, a_2+ b_2, a_3+ b_3>

(ii) Subtraction: $\mu_A - \mu_B$ = <a_1- b_3, a_2- b_2, a_3- b_1>

(iii) Multiplication: $\mu_A \times \mu_B$ = <a_1b_1, a_2b_2,a_3b_3>

(iv) Division: μ_A / μ_B = <a_1/b_3, a_2/b_2,a_3/b_1>

A problem with triangular fuzzy numbers is that addition and subtraction as well as multiplication and division are not reciprocal operations. To overcome this difficulty, subtraction and division operations definitions have to be modified.

Thus, subtraction can be performed as <a_1-b_1, a_2-b_2, a_3-b_3> if the following condition is satisfied, (Gani, 2012):

$$DP(\mu_A) \geq DP(\mu_B) \tag{2.2a}$$

where

$$DP\ (\mu_A) = \frac{a_3 - a_1}{2} \text{ and } DP\ (\mu_B) = \frac{b_3 - b_1}{2} \tag{2.2b}$$

If this condition is not met, then the definition given above in (ii) applies.

As for division, this operation can be written as: μ_A / μ_B = < a_1/b_1, a_2/b_2, a_3/b_3> if the following condition is satisfied:

$$\frac{DP\ (\mu_A)}{MP\ (\mu_A)} \geq \frac{DP\ (\mu_B)}{MP\ (\mu_B)} \tag{2.3a}$$

where

$$MP\ (\mu_A) = \frac{a_3 + a_1}{2} \text{ and } MP\ (\mu_B) = \frac{b_3 + b_1}{2}$$

If this condition is false, then definition (iv) above applies.

2.5.2.2 Fuzzy operators

In order calculate probabilities in a fuzzy fault tree, we need the ANF, ORF and NEGF operators. In a fuzzy fault tree, the probability of occurrence μ of the top event in the ANF case is evaluated as follows:

$$\mu_{\mathrm{ANF}} = \prod \mu_{\mathrm{i}} \qquad (2.4a)$$

As for the ORF case,

$$\mu_{ORF} = 1 - \prod(1 - \mu_{\mathrm{i}}) \qquad (2.4b)$$

$$\mu_{\mathrm{NEGF}} = 1 - \mu_{\mathrm{i}} \qquad (2.5$$

2.6 Fuzzy fault tree analysis

In order to illustrate these concepts, we will consider the case of a press brake used in many parts of industry. Our goal will be to evaluate a fuzzy fault tree whose top event is an accident such as: “an operator gets his hand caught between the closing dies of the press”.

2.6.1 Fuzzy fault tree (FSFT)

As the methodology that will be followed uses a fault tree, let us review this concept. A fault tree is a logical diagram that attempts to identify the ways that the various causes can combined to lead to an accident. Once this causal chain of events is established, the probability of occurrence of the accident can be calculated, (Yiu, 2015).

The situation under consideration will be that of an operator faced with an industrial machine such as a metal bending press (also often called a brake press), see (Burlet-Vianney et al., 2010) for more details on press brake operation and safety aspects. In such machines, a crushing zone exists due to the closing of mating parts. In order to do a more quantitative analysis, the probabilities of occurrence of the contributing (bottom) events must be determined or at least estimated. A press brake is a machine commonly found in the metal manufacturing industry. It is used to bend sheet metal in different shapes. A typical press brake is illustrated here in Figure 2.2.

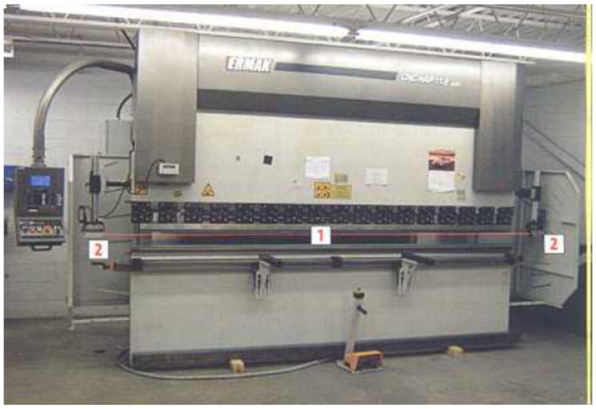

Figure 2.2 A Press brake (source: CNESST, 2008)

The machine is composed of two main structural components, a top beam mounted on a plate and a bottom table. Dies are clamped on the top and bottom parts. Either the top or the bottom half of the press then closes in (via a hydraulically-powered mechanism) on the stationary part. The operator holds the piece-part and actuates the closing motion with a foot pedal, in most applications. A hazardous situation is thus created from the proximity of the workers hands to the press closing motion. A possible undesirable event (often called a hazardous event) in such a situation is then that the worker gets his hands caught between the closing dies (the hazardous zone of the machine).

These are indicated in the fault tree shown here in Figure 2.3

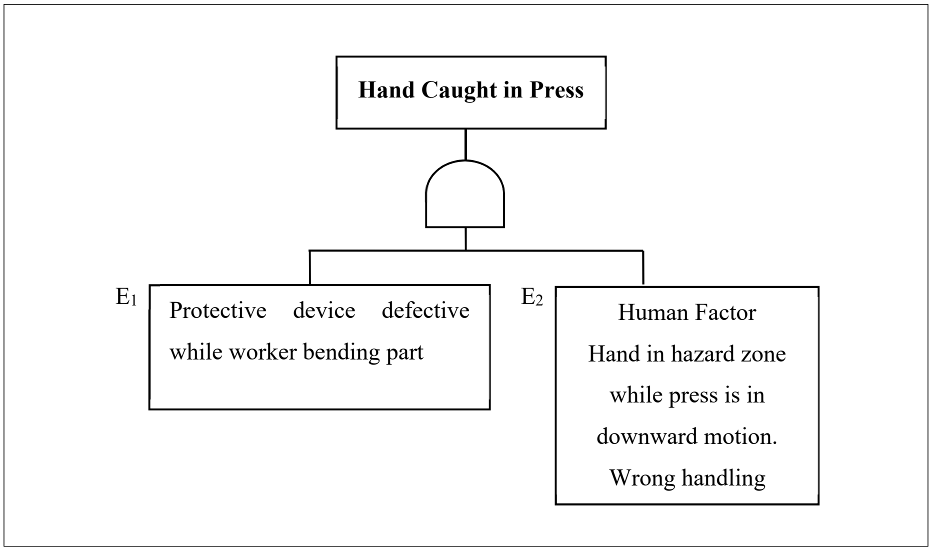
Hand Caught in Press
E1
Protective device defective while worker bending part
E2
Human Factor
Hand in hazard zone while press is in downward motion.
Wrong handling

Figure 2.3 A Fault tree

In this diagram, the boxes labelled E_1 and E_2 represent events (causes) which can contribute to the occurrence of the accident.

Safety regulations and standards require that such machines be equipped with protective devices which either prevent entry of the operator in the hazardous zone or stop the hazardous motion when parts of the workers body are in the hazardous zone. The protective device often utilized with press brake takes the form of a light (laser) sensor beam which spans the length of the press and is mounted between the two dies. Such a device is shown in the above picture of a press brake (1 is the sensor beam and 2 refers to the emitting and receiving components of the device).

An accident can occur when the operator gets his hands caught between the closing dies. The contributing events that can lead to such an accident can then be represented in a fault tree and are:

- an equipment failure event such as the protective device fails while worker is bending, E_1, and
- the human factor event, hands in danger zone due to wrong handling part, E_2.

The top event is then the result of the conjunction of events E_1 and E_2 and its probability is therefore evaluated using an AND gate.

2.6.2 Expert elicitation

The data needed for the probability calculation were obtained using a structured expert elicitation process as found in the literature, see for instance, (Knol et al., 2010). Participants were solicited for this purpose. These were eight bending press operators in a large manufacturing plant. The health and safety coordinator as well as the workers' supervisor were also solicited.

A questionnaire was handed to them which consisted of a set of brief instructions followed by three questions which were provided with multiple possible answers to chose from. The three questions posed were the following:

1 A bending sequence requires the worker to turn off a protective device in order to complete a certain bend due to the complexity of the shape. The worker must then turn the protective device back on to resume the bending sequence. What is your estimate of the probability that a worker forgets to re-activate the protective device?

2 What is your estimate of the probability that the protective device fails while the worker is bending a part?

3 What is the probability that a worker has his hands between the dies of the press while operating the machine?

The participants were given a choice of answers phrased in this manner:

(1) Very probable
(2) Probable
(3) Not too probable
(4) Improbable
(5) Very improbable

The questionnaire also contained examples corresponding to each of these probability statements to serve as comparison points.

A general introduction was given by the analyst to the participants in a group meeting on the shop floor which consisted of presentation the thesis and its purpose. The questions and the choice of answers were read to the group. The questionnaire was then handed to them. The whole process took little time to complete.

The following table shows partial results of an expert elicitation conducted by the authors at one industrial establishment:

Table 2.3 Partial results from Expert Elicitation Experiment

Participant #	Title/Function	Years of experience	Questions #		
			1 Worker forgets turn laser back on	2 Protective device defective while worker bending part	3 Hands in die while operating press
1	Brake Press Operator	23	Probable	Very improbable	Very improbable
2	Id.	30	Improbable	Very probable	Improbable
3	Id.	37	Very probable	Very improbable	Improbable
4	Id.	36	Probable	Very probable	Improbable
5	Id.	28	Probable	Probable	Improbable
6	Id.	2,5	Not too Probable	Not too Improbable	Not too Probable
7	EHS Coordinator	20	Improbable	Very improbable	Improbable
8	Supervisor	10	Probable	Probable	Not too probable

These estimates represent the experts' estimates of the probability of occurrence of the events in question, expressed in linguistic, qualitative terms. In order for us to perform the necessary calculations, we need to first transform these qualitative statements into quantitative, fuzzy numbers. Then, the fuzzy estimates must be aggregated in order to obtain one final fuzzy probability estimate.

The aggregation is then taken as a weighted average of the experts' opinions, the weighing method taking into account various factors.

Since linguistic terms are not mathematically operable, to cope with that difficulty, each linguistic term is associated with a fuzzy number, which represents the meaning of each generic verbal term.

The principle of this system is to pick a scale that matches all the linguistic terms in a row (attribute) of the decision matrix and use the fuzzy numbers on that Scale to represent the meaning of these linguistic terms.

In this work, we thus adopted a scale which combines the direct fuzzy number translation approach with a probability level from recognized safety standards such as (Dept. of Defense USA, 1993).

Table 2.4 Linguistic estimate to fuzzy number conversion

Very improbable	<0, 0.1, 0.2>x10^{-4}
Improbable	<0.2, 0.3, 0.4> x10^{-4}
Not too probable	<0.4, 0.5, 0.7> x10^{-4}
Probable	<0.7, 0.8, 0.90> x10^{-4}
Very probable	<0.90, 0.95, 1> x10^{-4}

2.6.3 Opinion Aggregation

The final aggregated fuzzy estimate of the probabilities is obtained by simply taking the average of the experts' estimates for each of the three components of the fuzzy numbers corresponding to the expert's linguistic probability estimate, as given in the scale. No weighing has been done for the following reasons. All workers have extensive experience except for one worker who had 2.5 years of experience. However, all workers get thorough technical training on all aspects of press brake operation. In addition, specific health and safety training sessions are periodically given to all workers. The company in question is a large, unionized, well-structured enterprise which performs extensive, on-going, health and safety monitoring and preventive activities.

First, the (fuzzy) probability of events E1 and E2 will be taken as being equal to:
For E1 we get $<0.4125, 0.5000, 0.6125>*10^{-6}$
For E2 we get: $<0.225, 0.325, 0.450>*10^{-6}$

We are now in a position to finally calculate the fuzzy probability associated with the top event, according to the rules explained earlier:
$<0.9281, 1.625, 2.756>*10^{-12}$

2.7 Optimization of a fault tree

The problem we wish to tackle now is the following. We want to first define a cost function which is related to the accidents that can occur on an industrial process or machine, (Avner, 2004). A legitimate objective is to minimize this cost function, given the constraints that must be faced. These constraints can be, typically, a maximum failure or accident rate imposed by safety or company or industry standards. This constraint might correspond to the probability of occurrence of the top event in a fault tree. In addition, the failure rates and occurrence probabilities must necessarily be numbers (in our case, triangular fuzzy ones) between 0 and 1.

The cost function can logically be thought to depend on the contributing (bottom) events in a fault tree. In such a fault tree, some of these factors can be taken as variables which can then be designed to achieve the required minimization. These variables can be determined, in particular, in two ways. First, we may use a FFMEA approach. In this method, the contributing events are ranked by calculating the product fuzzy risk priority number (FRPN) of the probabilities of occurrence times the severity of each event and the detection capability of the system for each failure or accident event. We can then choose as design variables the ones with the highest rankings. The second way is to choose as variables, the ones that can be controlled.

2.7.1 Nonlinear inequality constraints fuzzy optimization

2.7.1.1 The problem

The problem just stated when formulated in mathematical terms will lead to a minimization problem with linear and nonlinear inequality constraints (all in terms of fuzzy numbers) of the following general form, (Rogers et al., 2009):

$$\min \mathrm{f}(\mu_\mathrm{X}) \qquad \text{such that } \mathrm{h_i}(\mu_\mathrm{X}) \leq 0 \text{ for } = 1 \ldots \mathrm{p} \tag{2.6}$$

where f and the functions $\mathrm{h_i}$are differentiable.

2.7.1.2 Karush-Kuhn-Tucker (KKT) Conditions

The stated problem can be solved using an extension the Lagrange multipliers method.

which can be expressed as: $$\begin{cases} \nabla f(\mu_\mathrm{X}) + \sum_{i=1}^{p} \lambda_\mathrm{i} \nabla \mathrm{h_i}(\mu_\mathrm{X}) = 0 \\ \lambda_\mathrm{i} \mathrm{h_i}(\mu_\mathrm{X}) = 0 \\ \mathrm{h_i}(\mu_\mathrm{X}) \leq 0 \\ \lambda_\mathrm{i} \geq 0 \end{cases} \tag{2.7}$$

2.7.2 Method for solving fuzzy nonlinear equations

Once the satisfying conditions above have been determined, the final result will be a nonlinear equation in one of the unknown variables equal to zero. The solution could be solved by the above method involving the Lagrange multipliers. However, the solution can also be found using the fmincon Matlab function, applied to the three members of the given fuzzy numbers at hand. This is the approach that will be taken here. The design variables which will have been found can then be used to determine the minimized cost function, thus achieving our goal.

2.7.3 Example for a press brake

In order to perform the mathematical analysis, the example of the press brake presented previously will be taken.

Referring to the fault tree presented in Figure 2.1, we will choose as design variables, a human factor variable and a method-related variable which we will denote by μ_{X_1} and μ_{X_2}. These are variables which can be controlled, for instance, by training and selection of experienced personnel. For this case, the probability associated with the top event will be taken as a given constraint μ_{SF} .

The cost function is composed of two components. The first reflects the cost of achieving a given level of reliability while the second part reflects the costs of accidents or failures which can still occur. Thus the cost function is chosen to be of the following general form:

$$\mathrm{CF} = \sum(\mu_{pc_i}\,(1 - \mu_{x_i})^{kp_i} + (\mu_{fc_i}\mu_{x_i})^{kf_i}) \qquad (2.8)$$

This expression reflects the fact that higher reliability (less accident) involves higher costs, hence the factors (1-μ_{X_i}) which express reliability are used instead of just μ_{X_i} which represent failure probabilities. The coefficients μ_{pc_i} and $\mu_{fc_i}$are fuzzy numbers as well. The reason for this is that the cost of obtaining a certain component of required reliability varies with the supplier or, in the case of a human factor, it might vary with the person.

We will consider a quadratic cost function for calculation purposes.
So, our optimization model will take the following form
Minimize the Cost Function:

$$\mu_{pc_1}(1 - \mu_{x_1})^2 + \mu_{pc_2}(1 - \mu_{x_2})^2 + \mu_{fC_1}\mu_{x_1}{}^2 + \mu_{fC_2}\mu_{x_2}{}^2 \qquad (2.9)$$

subject to:

$$\begin{cases} (\mu_{SS})(\mu_{X_1})(\mu_{X_2}) \leq \mu_{SF} \\ \mu_{X_1} - 1 \leq 0 \\ \mu_{X_2} - 1 \leq 0 \\ -\mu_{X_1} \leq 0 \\ -\mu_{X_2} \leq 0 \end{cases} \qquad (2.10)$$

μ_{SS} is a variable introduced because of the ≤ sign in the first condition.
The values of the coefficients will be taken, purely for demonstration purposes, as:

μ_{pc_1} =<90, 100, 110>

μ_{pc_2} =<100, 110, 120>

μ_{fC_1} =<95, 105, 115>

μ_{fC_2} =<105, 115, 125>

μ_{SS} =<1, 1, 1>

μ_{SF} =<0.3, 0.4, 0. 5>

μ_{C_1}will be taken as <90, 100, 110> and μ_{C_2} =<100, 110, 120>
This problem was solved, with Matlab, using the fmincon function.
With this method, we obtained the following results:

μ_{x_1} = < 0.4865, 0.4878, 0.4889 >

μ_{x_2} = < 0.4878, 0.4889, 0.4898 >.

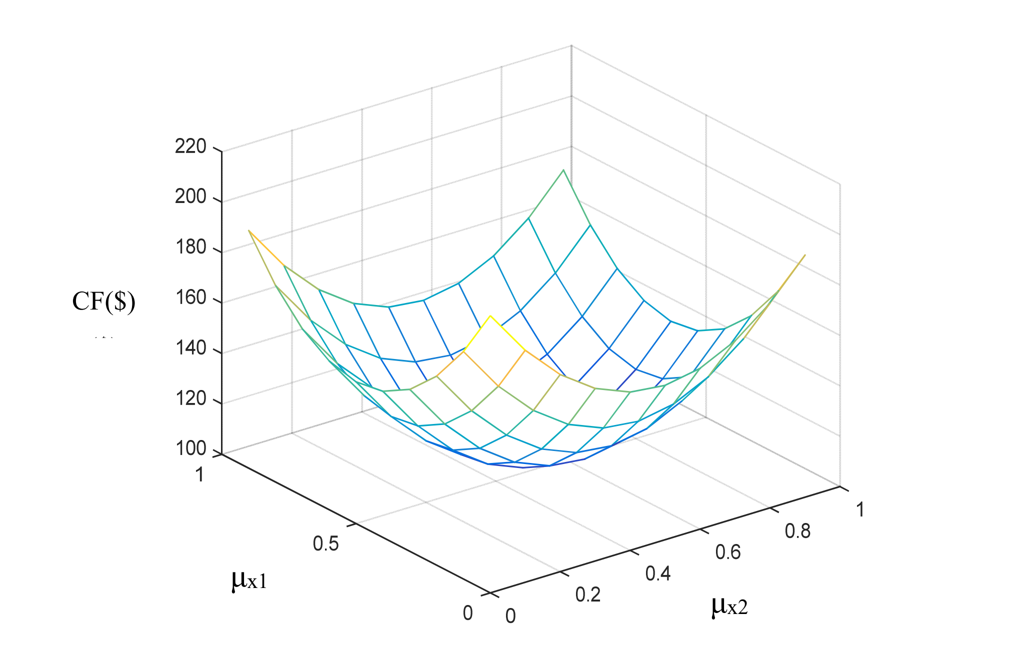

Figure 2.4 Plot of Cost Function

To test the validity of our results, we plotted the cost function (Figure 2.4) and found indeed a zero in the vicinity of 0.5. The corresponding cost function value (as defined in eq. (2.9)) was CF = < 97.022, 107.9457, 121.7209>. We may conclude from the plot of the cost function that this is a global minimum.

2.7.4 Conclusion

In this chapter we presented a survey of applications of fuzzy methodology to occupational risk analysis. A safety analysis of an industrial bending press was analyzed based on fuzzy fault tree analysis. The probabilities associated with the bottom events have been assumed in this paper. These probabilities were assumed to possess a normal probability distribution which was converted into triangular fuzzy numbers. These fuzzy numbers possess particular algebra rules which were discussed and which will be used later on in this research. The fuzzy probability of occurrence of the top event which represented a worker accident was then calculated.

We also addressed a so-called inverse problem in static fuzzy fault tree analysis in which a cost function reflecting work accidents is minimized subject to the constraint that the accident probability of occurrence is specified, by regulation or standard. The problem was expressed mathematically as an optimization problem and solved using a Matlab algorithm with fuzzy numbers as arguments. The optimized variables corresponding to the contributing events probabilities of occurrence were calculated as well as the cost. This gives the analyst target values to reach for the variables that are under his/her control

CHAPITRE 3

SYSTEM SAFETY ANALYSIS OF AN INDUSTRIAL PROCESS USING FUZZY METHODOLOGY[4]

This chapter was presented at the the 4th International Conference on
Fuzzy Systems and Data Mining (FSDM 2018)

Abstract

Industrial processes and machines pose risks in terms of equipment failure and worker accidents. In order to prevent these unwanted occurrences, the associated risks must first be analyzed. However in traditional fault tree analysis, exact data values are used. But in real life often these values are not known precisely. There is therefore a degree of uncertainty associated with the data. Fuzzy numbers, expressed in this paper as triangular fuzzy number, provide a method for dealing and taking into account this uncertainty. In this paper, fuzzy fault tree analysis is then used. An example of a metal brake press is used to demonstrate this approach. A fault tree for a particular accident scenario is built and the fuzzy probability of occurrence of the accident under consideration is evaluated. An interesting second problem consists in starting with this value and deducing from the fault tree, what values of the occurrence probabilities of the contributing events in the fault tree minimize a function expressing the cost of work accidents. This problem is expressed mathematically and solved using a Matlab-based method over fuzzy numbers. The optimized contributing event probabilities are obtained along with the optimal cost function.

[4] Venditti, T., Tran, N.D.P., Ngô, A.D. (2018) 4th International Conference on Fuzzy Systems and Data Mining (FSDM 2018) in Bangkok, Thailand, November 13th-15th 2018

3.1 Introduction

3.1.1 Machine safety context and regulations

In most jurisdictions throughout the world, such as the province of Canada, Québec, employers must take the necessary measures to protect the health, safety and physical integrity of the workers, (Government of Québec, S-2.1). Notably, employers must:
- develop methods and techniques which ensure that the work performed is safe;
- use methods and techniques which aim to identify, control and eliminate the risks which can affect the health and safety of the workers;
- provide materials (a term which is meant to encompass machines, tools, parts, etc.) which are safe and kept in good condition.

In addition to these general duty requirements, regulations spell out for employers, specific requirements regarding machine safety. The salient feature of these requirements is that hazardous zones in and around machines must be made inaccessible failing so, the machine must be equipped with at least one protective device which either prevents access to the hazardous zones or stops or interrupts all hazardous phenomena in case of access into a hazardous zone, (Government of Québec, S-2.1). Examples of these requirements in relation to presses include a safety light curtain placed at an appropriate distance, in front of the closing dies (the device stops the hazardous motion of the press when entry into the hazardous zone is attempted).

Employers must demonstrate the safe performance of these devices. Safety standards addressing the design, installation, use and care of these devices have been developed and are available.

3.1.2 The concept of risk

Risk is at the same time an intuitively obvious concept understandable to all but, at the same time, is a surprisingly subtle and difficult to pinpoint. Indeed, to illustrate vividly this point, a prominent risk researcher, (Kaplan, 1997) recalls the story that when the Society for Risk Analysis was formed, a committee was created to define the word risk. After laboring for four years, the committee gave up and decided it was better not to define risk and let every author clearly explain their own definition.

Nevertheless, a common definition, adopted by safety standards on risk assessment such as (ISO/TR 14121-2, 2012, CSA Z432, 2017, ANSI B11-TR3, 2000) defines risk as the combination of the probability of occurrence of a damage (material damage or injury) and the severity of such a damage. Yet other references, adopt a similar definition but use the probability of occurrence of the hazardous event leading to the injury instead. Either way, the probability is assessed using a qualitative scale. It is one of the aims of this paper to present a more quantitative evaluation of the probability of occurrence of the event leading to an injury.

3.1.3 Risk analysis of industrial machines. The case of presses

The operation of industrial machines, in particular presses such as metal punch presses, brake presses, compression molding presses, involves various risks, particularly for the operators.
In order to analyze these risks and better protect the operators, a methodology is needed. Many methods have been developed, among them fault tree analysis; see for a review, for example, (Flaus, 2013). Fault tree analysis attempts to identify the various events that lead to an accident. The probability of occurrence of such an accident can then also be evaluated by this method. In order to carry out such an analysis, different steps have to be followed. First, the sequence of relevant events has to be established. In order to do so, a root cause analysis can be done. This will identify the events. Then, the fault tree will show the sequence of events (often called bottom events) in their right order leading to the accident (often termed the top event).

In traditional fault tree analysis, the probabilities associated with the basic events are known precisely. However, in real life, these values are rarely known. There is always uncertainty surrounding them. It has been pointed out, in many papers (for instance in (Purba et al., 2014),, that the probabilities associated with the events making up the tree are seldom known with precision and gathering the required information has proved to be very difficult. To remedy this difficulty, fuzzy numbers can be used. The probabilities associated with the events which make up the fault tree under consideration can then be expressed as fuzzy numbers. Calculations will then be performed with fuzzy arithmetic. This process can thus be called Fuzzy Fault Tree Analysis (FFTA).

FFTA has been applied in many fields, among others:

- Fuel cells, (Whiteley et al., 2016);
- Marine cargo transportation, (Yunus et al. 2015);
- Risks in healthcare, (Komal, 2015);
- Probability of explosion of marine diesel engines, (Celik and Celik, 2013);
- Probability of oil and gas wells explosion, (Lavasini et al., 2015);
- Probability of breakdown during construction contract negotiation, (Yiu, 2015);
- Risk analysis in metro construction, (Zhang et al., 2014);
- Safety analysis of offshore oil drilling platform, (Ramzali et al., 2015);
- Probability of crude oil tanks fire and explosion , (Wang, 2013).

However there are few published fuzzy analyses of the risk involved with press operations.
In this paper, a «static» fuzzy fault tree analysis was performed on a metal brake press. For illustrative purposes, a simplified fault tree consisting of two basic events is considered. The probabilities of the contributing events were obtained from an expert elicitation process.
The term «static» refers to the fact that the sequence in which events leading to a undesirable event (an accident) happens is not taken into account.

The paper is organized as follows. The methodology used to build a fuzzy fault tree is first discussed. Fuzzy number arithmetic needed for fault tree quantitative evaluation is explained.

These concepts are then applied to the operation example of a brake press machine. In the second part of the paper, the fuzzy fault tree is optimized in terms of the cost of safety investments. The problem is posed mathematically as a cost function to be minimized with the fault tree providing as the constraints.

3.2 Fuzzy risk evaluation methodology

3.2.1 Root cause analysis (RCA)

RCA attempts to identify the factors that might cause an unwanted event (a product defect, or, more to our point, an accident at work) to occur. To carry out such an analysis, the potential causes are most often subdivided into the «3 M's», namely Man, Machine and Methods, (Sharma and Sharma, 2010). This method, while helpful in causal analysis, does not however provide quantitative estimates of risk. Furthermore it does not show how the factors combine to lead to the unwanted event.

3.2.2 Fuzzy failure mode and effects analysis (FFMEA)

Traditional failure mode and effects analysis (FMEA) is one of the first methods invented for system reliability analysis purposes. The objective of FMEA is to identify all the potential failure modes of a system's components, identify the causes of these failure modes, and assess the effects that each of these failure modes may have on the entire system.

FFMEA works on the same principle but the assessment of the effects is done in terms of fuzzy numbers as to account for the uncertainty of the available data.

3.2.3 Fuzzy static fault tree (FSFT)

Traditional fault tree analysis attempts to identify the various events that lead to an accident. The probability of occurrence of such an accident can then also be evaluated using fault tree analysis. In order then to carry out such an analysis, different steps have to be followed. First, the relevant events have to be identified. In order to do so, a root cause analysis can be carried out. This will identify the events. Then, the fault tree will show the sequence of events (often called bottom events) in their right order and combination leading to the accident (often termed the top event).

An example can best illustrate the concept of a fault tree. Consider the following figure 3.1.

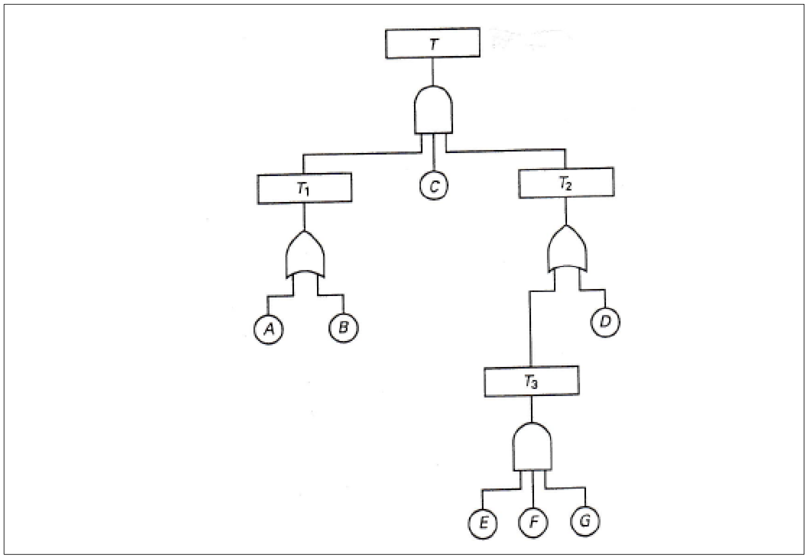

Figure 3.1 An example of a fault tree

In this example, T at the top of the tree represents the undesirable event like an accident. The boxes and circles represent underlying events which combined in the way shown in the tree lead to the event T. This particular tree shows that event T can occur if events T_1, C and T_2 occur in conjunction (as shown by the and gate symbol). The analysis has further established that event T_2 can occur if either event D or event T_3 occur. T_3 was further analyzed in terms of underlying contributing events.

Similarly to FFMEA, FSFTA works on the same principle but the assessment of the effects is done in terms of fuzzy numbers as to account for the uncertainty of the available data.

3.3 Evaluation of probability of occurrence of one possible type of accident

3.3.1 Building the fault tree of the accident under consideration

Building the fault tree can be based on a root cause analysis. The situation under consideration will be that of an operator faced with an industrial machine such as a metal punching press, a composite materials molding press or a metal brake (bending) press. In such machines, a crushing zone exists due to the closing of mating parts. In order to do a more quantitative analysis, the probabilities of occurrence of the contributing (bottom) events must be determined or at least estimated.

3.3.2 Calculation of the top event of the fault tree

3.3.2.1 Conversion between normal probability distribution and fuzzy triangular numbers

In risk analysis we often do not know the precise values of the probabilities of occurrence or of failure of the systems or of its components. So one way to deal with this problem is to consider that the variables of interest follow a normal probability distribution with a mean value and a standard deviation. However, another approach to the problem is to use fuzzy triangular number.

A fuzzy number is represented by three numbers <a_1, a_2, a_3>. This representation is interpreted as a membership function such as shown in the following Figure 3.2, which was presented previously in chapter 2.

$$\mu_A(x) = \begin{cases} 0 & x < a_1 \\ \frac{X-a_1}{a_2-a_1} & \text{for } a_1 \leq x \leq a_2 \\ \frac{a_3-X}{a_3-a_2} & \text{for } a_2 \leq x \leq a_3 \\ 0 & x > a_3 \end{cases}$$

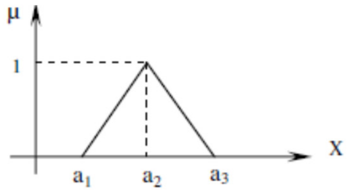

Figure 3.2 A triangular fuzzy number

In this representation, a2 corresponds to a membership value of 1 meaning that we think that the most probable value of the variable under consideration is a2. So a2 corresponds to the mean value in a normal probability distribution. In this representation, we mean also that the variable under interest lies between the values a1 and a3, which have "membership values" of 0. In other words, a1 and a3 correspond to the 3σ values from the mean in a standard normal probability distribution. This is the basic definition of a fuzzy number (triangular or of a different distribution shape). The meaning of fuzzy numbers and concepts can be further developed and understood as the following discussion shows.

(Dadone, 2001) offers the following example. Consider the question of deciding whether a person is tall or not. The property "tall" is inherently fuzzy. Indeed, reasoning according to strict logic, we would like to define a height threshold that divides tall people from non-tall ones. If someone is taller than the threshold (even by 1/10 of an inch) than he or she is tall, otherwise, not tall. This is obviously far from the way we decide whether someone is tall or not. Our perception of the person is better described as a sort of soft switching rather than a threshold mechanism. This is also why we often add a modifier to the word "tall" (i.e., not, not very, somewhat, very, etc.) in order to express "degrees of tall" rather than absolute true or false answers. In defining in a strict way, the set of "tall persons" we could fix a threshold somewhere between 5'5" and 6', say 5'10". Therefore, someone who is 5'9" would not be tall, while someone who is 5'11" would. Conversely, in the fuzzy set "tall person" a degree of tall is defined, thus providing a *continuum* rather than an abrupt transition from true to false.

Another question that comes up often in discussions of this topic concerns the relationship of fuzziness to probability. Are fuzzy sets and fuzzy numbers just a clever disguise for statistical models? The answer is in fact no**.** An editorial article by (Bezdek, 1993) which introduced the inaugural issue of the IEEE Transactions on Fuzzy Systems offers an explanation with an example.

First, define the set of all liquids be the universe of objects, and let fuzzy subset *L* = {all potable (i.e., "suitable for drinking") liquids}. Consider now the following example. Suppose you had been in the desert for a week without drink and you came up on two bottles, *A* and *B*. You are told that the (fuzzy) membership of the liquid in *A* to *L* is 0.9 and also that the probability that the liquid in *B* belongs to *L* is 0.9. In other words, *A* contains a liquid that is potable with degree of membership 0.9, while *B* contains a liquid that is potable with probability 0.9. The question now is, Confronted with this pair of bottles and given that you must drink from the one that you choose, which would you choose to drink from first?

The bottle you should drink from is *A*, because this 0.9 value means that the liquid contained in *A* is fairly close to being a potable liquid, thus it is very likely to not be harmful. On the other hand, *B* will contain a liquid that is very probably potable. So by choosing it, we would run the risk, 1 out of 10 times on average, of drinking a harmful liquid such as, say, sulfuric acid from *B*! Moreover, after an observation is made and the content of the bottles is revealed, the membership for *A* stays the same while the probability for *B* changes and becomes either 0 or 1 depending on the fact that the liquid inside is potable or not.

As his work rests on the use of fuzzy numbers, their arithmetic is of great importance. For convenience, the previous expositions are repeated here for convenience.

3.3.2.2 Fuzzy operations and operators

In order to perform calculations on fuzzy fault trees, arithmetic operations on fuzzy numbers have to be introduced. The following are the four operations that can be performed on fuzzy triangular numbers, (Rogers et al., 2009) :

Let μ_A=<a_1, a_2, a_3> and μ_B = <b_1, b_2, b_3> where a_i and b_i are positive numbers, then we have:

(i) Addition: $\mu_{A\,+}\,\mu_B$ = <a_1+ b_1, a_2+ b_2, a_3+ b_3>

(ii) Subtraction: $\mu_{A\,-}\,\mu_B$ = <a_1- b_3, a_2- b_2, a_3- b_1>

(iii) Multiplication: $\mu_A \times \mu_B$ = <a_1 b_1, a_2 b_2,a_3 b_3>

(iv) Division: μ_A / μ_B = <a_1/b_3, a_2/b_2,a_3/b_1>

Intuitively, these definitions can be understood by viewing fuzzy numbers as numbers on an interval. The idea is that the given operation must correctly yield the boundaries of the interval of the resulting fuzzy number. For instance, in the case of the subtraction operation, the left boundary has to be the result of subtracting the most distant boundaries of the two fuzzy numbers being considered; the same reasoning applies to the right boundary.

It will be noticed that subtraction and division are not defined in a "natural way", that is in the order of the fuzzy numbers components. Stated differently, with the definitions given as above, addition and subtraction as well as multiplication and division are not reciprocal operations. To overcome this difficulty, subtraction and division operations definitions have to be modified.

(Gani and Assarudeen, 2012) have shown that subtraction can be performed as <a_1-b_1, a_2-b_2, a3-b_3> if the following condition is satisfied :

$$DP(\mu_A) \geq DP(\mu_B), \qquad (3.1)$$

where

$\mathrm{DP}\ (\mu_A) = \frac{a_{3-a_1}}{2}$ and $\mathrm{DP}(\mu_B) = \frac{b_{3-b_1}}{2}$

If this condition is not met, then the definition given above in (ii) applies.

As for division, this operation can be written as: $\mu_A / \mu_B = < a_1/b_1, a_2/b_2, a_3/b_3>$ if the following condition is satisfied:

$$\frac{\mathrm{DP}(\mu_A)}{\mathrm{MP}(\mu_A)} \geq \frac{\mathrm{DP}(\mu_B)}{\mathrm{MP}(\mu_B)} \tag{3.2}$$

where

$$\mathrm{MP}(\mu_A) = \frac{a_3 - a_1}{2} \text{ and } \mathrm{MP}(\mu_B) = \frac{b_3 - b_1}{2}$$

If this condition is false, then definition (iv) above applies.

In order calculate probabilities in a fuzzy fault tree, we need the ANF, ORF and NEGF operators. In a fuzzy fault tree, the probability of occurrence μ of the top event in the ANF case is evaluated as follows:

$$\mu_{\mathrm{ANF}} = \prod \mu_i \tag{3.3}$$

As for the ORF case,

$$\mu_{\mathrm{ORF}} = 1 - \prod (1 - \mu_i) \tag{3.4}$$

As for the negation operator, NEGF, it is simply

$$\mu_{\mathrm{NEGF}} = 1 - \mu_i \tag{3.5}$$

3.3.2.3 Example for a press brake

As a way of illustrating the theory, brake press operation will be consider. Before delving into calculations, a brief overview of the process involved will be given. A press brake is a machine commonly found in the metal manufacturing industry. It is used to bend sheet metal in different shapes. A typical press brake is illustrated in Figure 3.3.

The machine is composed of two main structural components, a top beam mounted on a plate and a bottom table. These two parts are usually connected by two C-frames on each side of the machine. Dies are clamped on the top and bottom parts. Either the top or the bottom half of the press then closes in (via an hydraulically-powered mechanism) on the stationary part. The operator holds the piece-part and actuates the closing motion with a foot pedal, in most applications. An hazardous situation is thus created from the proximity of the workers hands to the press closing motion. A possible undesirable event (often called a hazardous event) in such a situation is then that the worker gets his hands caught between the closing dies (the hazardous zone of the machine).

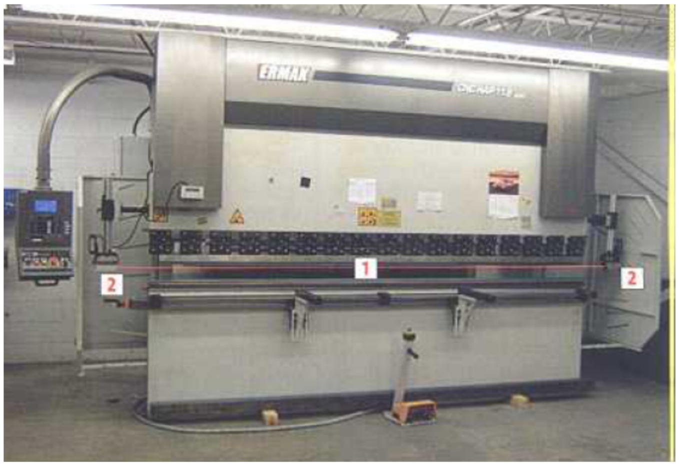

Figure 3.3 A Press brake (Source: CNESST, 2008)

The machine is composed of two main structural components, a top beam mounted on a plate and a bottom table. These two parts are usually connected by two C-frames on each side of the machine. Dies are clamped on the top and bottom parts. Either the top or the bottom half of the press then closes in (via an hydraulically-powered mechanism) on the stationary part. The operator holds the piece-part and actuates the closing motion with a foot pedal, in most applications. An hazardous situation is thus created from the proximity of the workers hands to the press closing motion. A possible undesirable event (often called a hazardous event) in such a situation is then that the worker gets his hands caught between the closing dies (the hazardous zone of the machine). Safety regulations and standards require that such machines be equipped with protective devices which either prevent entry of the operator in the hazardous zone or stop the hazardous motion when parts of the workers body are in the hazardous zone. The protective device often utilized with press brake takes the form of a light (laser) sensor beam which spans the length of the press and is mounted between the two dies. Such a device is shown in the above picture of a press brake (1 is the sensor beam and 2 refers to the emitting and receiving components of the device).

Now we must build the fault tree for this event. A preliminary step, as explained above, consists in identifying the contributing events which can lead to the accident under consideration. This can be accomplished by means of a Root cause analysis which takes the form of a fishbone diagram whose structure consists of the 3M's discussed previously. Figure 3.4 shows a root cause diagram for an accident occurring on a brake press.

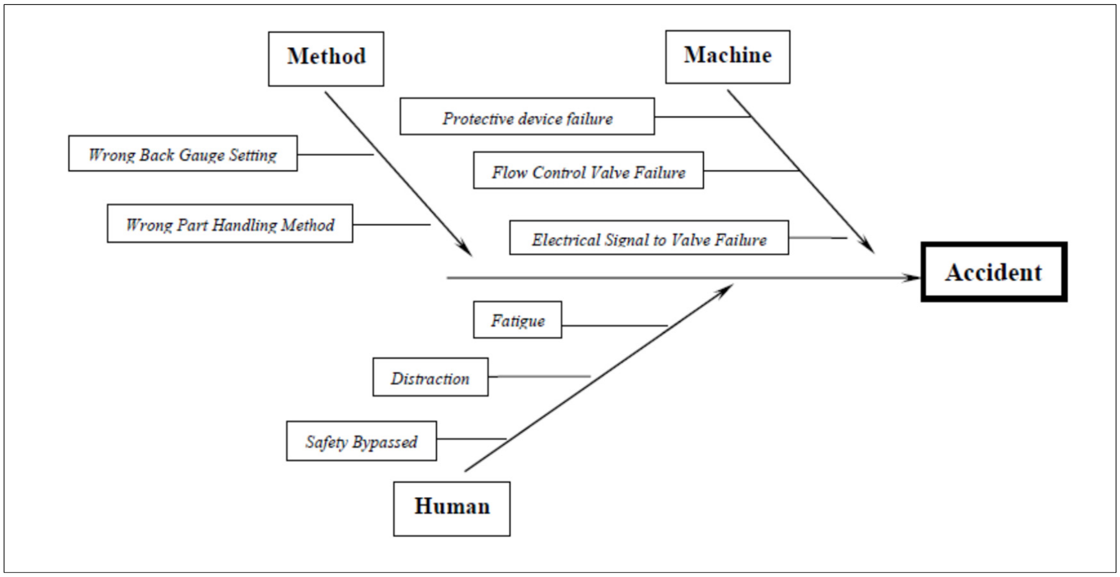
Method
Machine
Protective device failure
Wrong Back Gauge Setting
Flow Control Valve Failure
Wrong Part Handling Method
Electrical Signal to Valve Failure
Accident
Fatigue
Distraction
Safety Bypassed
Human

Figure 3.4 Root Cause Diagram for the Brake Press

From this root cause analysis, a fault tree containing the factors identified therein can be constructed, see Figure 3.5. The contributing elements which are the skeleton of the fishbone structure become the branches representing the bottom events in the fault tree. For evaluation purposes, we assume that only two events have a significant probability of occurring. The simplified fault tree is shown in Figure 3.6. The context of occurrence of this situation in the case of a press brake is the following. In press brake work, some parts can be very complex and the protective device can impede the making of certain bends. In this case, the protective device must then be turned off for those bends. The subsequent bends in a particular bending sequence can be made with the proper protective device back in place. But it can happen that the operator forgets to turn the protective device back on. The risks of an injury are then obviously increased. This represents one the events in the fault tree considered here. The second event is that of the hands in the operator between the dies due to a wrong handling method.

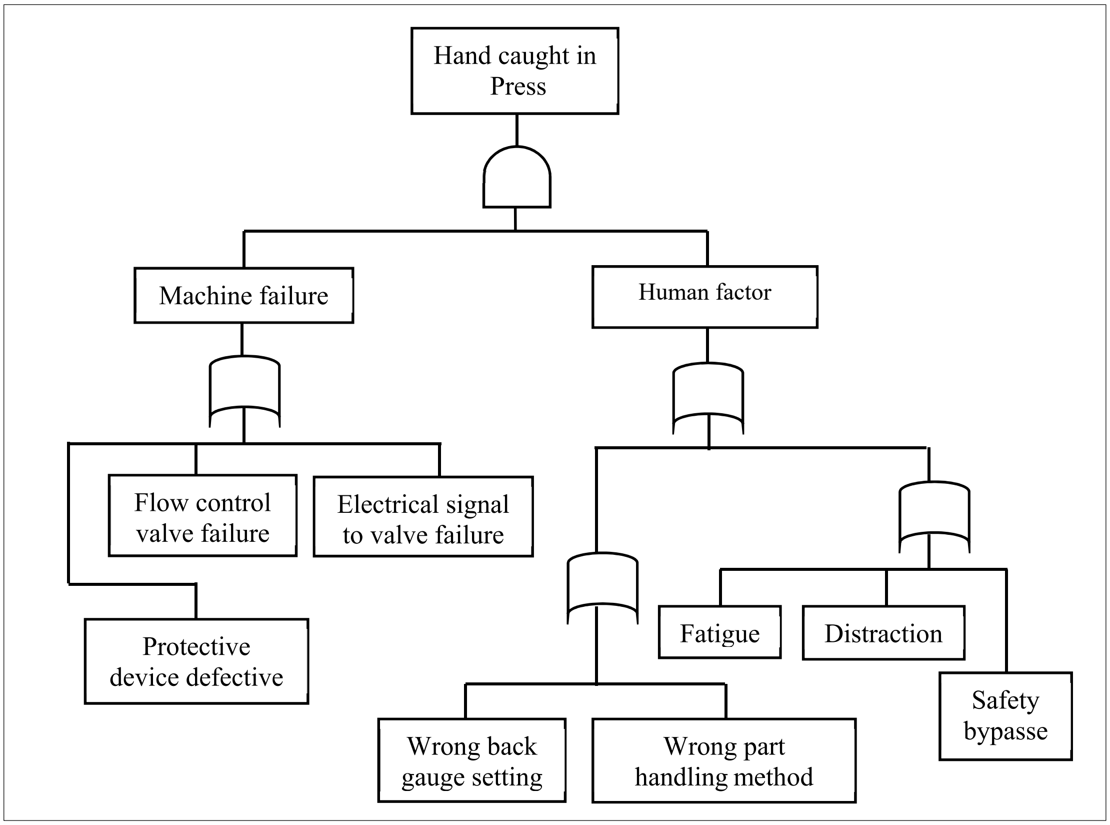
Hand caught in Press
Machine failure
Human factor
Flow control valve failure
Electrical signal to valve failure
Protective device defective
Fatigue
Distraction
Safety bypasse
Wrong back gauge setting
Wrong part handling method

Figure 3.5 Tree Diagram for the Brake Press

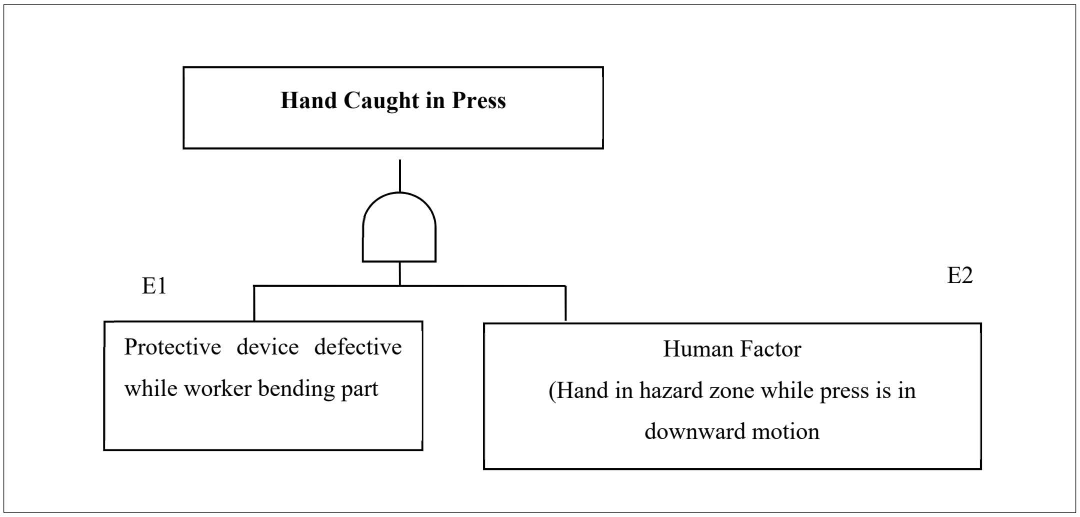
Hand Caught in Press
E1
E2
Protective device defective while worker bending part
Human Factor
(Hand in hazard zone while press is in downward motion

Figure 3.6 Simplified Fault Tree

The contributing bottom events in the fault tree are: the technical factor event, protective device fails while worker is bending, E1, and the human factor event, hands in danger zone due to wrong handling part, E2. The top event is then the result of the conjunction of events E1 and E2 and its probability is therefore evaluated using an ANF gate. The probability of occurrence of the top event is thus evaluated as follows:

First, the (fuzzy) probability of events E1 and E2 are obtained using an expert solicitation method which will be described in detail in a later paper. Briefly, the method consists of conducting structured interviews with individuals knowledgeable with the machine and process under study. Instructions and training on the concepts of risk and probability in the contex of occupational health and safety are given. Specifically worded questions asking for qualitative, linguistic assessment of probabilities of the events under study are then addressed to the participants. A method involving fuzzy numbers is then used to combine the answers. Using this method , for E1 the probability of occurrence was given by $<0.4125, 0.5000, 0.6125>*10^{-6}$ whereas for E2 the result was: $<0.225, 0.325, 0.450>*10^{-6}$.

The fuzzy probability associated with the top event can now be calculated, according to the rules explained earlier:

$<0.9281, 1.625, 2.756>*10^{-12}$

In other works such as the study made by Ramzani et al. ([15]), fuzzy numbers are used in fault tree or event tree to demonstrate the capacity of the method presented to produce an estimate of the probability of occurrence, as was done here. In these types of study, the results depend on the estimates of the probabilities of the underlying basic events. Comparisons with other published results are therefore difficult or even plainly not possible. The objective is rather to demonstrate that more quantitative assessment of risks can be obtained.

3.4 Inverse problem: Optimization of a fault tree

The problem we wish to tackle is the following. We want to first define a cost function which is related to the accidents that can occur on an industrial process or machine. A legitimate objective is to minimize this cost function, given the constraints that must be faced. These constraints can be, typically, a maximum failure or accident rate imposed by safety or company or industry standards. This constraint might correspond to the probability of occurrence of the top event in a fault tree. In addition, the failure rates and occurrence probabilities must necessarily be numbers (in our case, triangular fuzzy ones) between 0 and 1.

The cost function can logically be thought to depend on the contributing (bottom) events in a fault tree. In such a fault tree, some of these factors can be taken as variables which can then be designed to achieve the required minimization. These variables can be determined, in particular, in two ways. First, we may use a FFMEA approach. In this method, the contributing events are ranked by calculating the product fuzzy risk priority number (FRPN) of the probabilities of occurrence times the severity of each event and the detection capability of the system for each failure or accident event. We can then choose as design variables the ones with the highest rankings. The second way is to choose as variables, the ones that can be controlled.

3.5 Nonlinear inequality constraints fuzzy optimization

This paper presents here the same discussion of the fuzzy optimization problem as presented in Chapter 2 as this is fundamental to the method utilized in what follows. The theory of optimization is described in its general form with nonlinear constraints. The method of Lagrange multipliers is described briefly even though the problem will be solved using existing Matlab functions.

3.5.1 The problem

The problem just stated when formulated in mathematical terms will lead to a minimization problem with many nonlinear inequality constraints (all in terms of fuzzy numbers) of the following general form:

$\min f(\mu_X)$ such that $h_i(\mu_X) \leq 0$ for $= 1 \ldots p$ (2.7)

where f and the functions $h_i$are differentiable

3.5.2 Karush-Kuhn-Tucker (KKT) Conditions

The stated problem can be solved using an extension the Lagrange multipliers method which can be expressed as:

$$\begin{cases} \nabla f(\mu_X) + \sum_{i=1}^{p} \lambda_i \nabla h_i(\mu_X) = 0 \\ \lambda_i h_i(\mu_X) = 0 \\ h_i(\mu_X) \leq 0 \\ \lambda_i \geq 0 \end{cases} \quad (2.8)$$

3.5.3 Method for solving fuzzy nonlinear equations

Once the satisfying conditions above have been determined, the final result will be a nonlinear equation in one of the unknown variables equal to zero.

The solution could be solved by the above method involving the Lagrange multipliers. However, the solution can also be found using the fmincon Matlab function, applied to the three members of the given fuzzy numbers at hand. This is the approach that will be taken here.

The design variables which will have been found can then be used to determine the minimized cost function, thus achieving our goal.

3.6 Example for a press brake

In order to perform the mathematical analysis, the example of a press brake introduced in the first paper will be used. This problem statement will then lend itself to a mathematical representation as follows.

Referring to the fault tree presented in Section 3, we will choose as design variables, a human factor variable and a method-related variable which we will denote by μ_{X_1} and μ_{X_2}. These are variables which can be controlled, for instance, by training and selection of experienced personnel. For this case, the probability associated with the top event will be taken as a given constraint μ_{SF} .

The cost function is composed of two components. The first reflects the cost of achieving a given level of reliability while the second part reflects the costs of accidents or failures which can still occur. Thus the cost function is chosen to be of the following general form:

$$\mathrm{CF} = \sum(\mu_{pc_i}\,(1 - \mu_{x_i})^{kp_i} + (\mu_{fc_i}\mu_{x_i})^{kf_i}) \tag{2.9}$$

In which the range of the index i covers all the basic events in the problem at hand. This expression reflects the fact that higher reliability (less accident) involves higher costs, hence the factors (1-μ_{x_i}) which express reliability are used instead of just μ_{X_i} which represent failure probabilities .

The coefficients μ_{C_i} are fuzzy numbers as well. The reason for this is that the cost of obtaining a certain component of required reliability varies with the supplier or, in the case of a human factor, it might vary with the person. We will consider a quadratic cost function for calculation purposes. We will first draw the fault tree for our problem , similar to figure 3.6 but with fuzzy numbers values and symbols associated with the events making up the tree. See Figure 3.7.

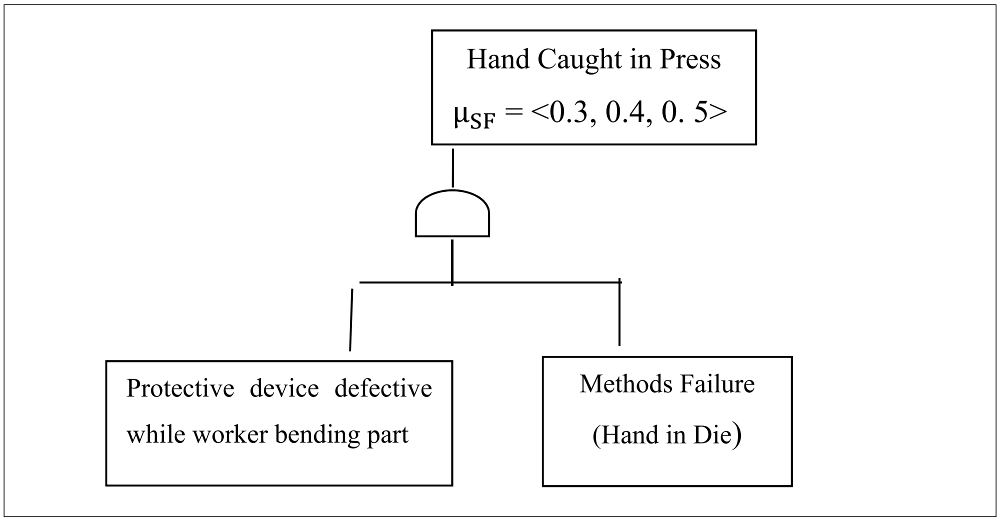
Hand Caught in Press
μ_{SF} = <0.3, 0.4, 0. 5>
Protective device defective while worker bending part
Methods Failure (Hand in Die)

Figure 3.7 Example Fault Tree

So, our optimization model will take the following form

Minimize the Cost Function:

$$\mu_{pc_1}(1 - \mu_{x_1})^2 + \mu_{pc_2}(1 - \mu_{x_2})^2 + \mu_{fC_1}\mu_{x_1}{}^2 + \mu_{fC_2}\mu_{x_2}{}^2 \qquad (2.10)$$

subject to:

$$\begin{cases} (\mu_{SS})(\mu_{X_1})(\mu_{X_2}) \leq \mu_{SF} \\ \mu_{x_1} - 1 \leq 0 \\ \mu_{x_2} - 1 \leq 0 \\ -\mu_{x_1} \leq 0 \\ -\mu_{x_2} \leq 0 \end{cases} \qquad (2.11)$$

μ_{SS} is a variable introduced because of the < sign in the first condition.

The values of the coefficients will be taken, purely for demonstration purposes, as:

μ_{pc_1} = <90, 100, 110>

μ_{pc_2} = <100, 110, 120>

μ_{fC_1} = <95, 105, 115>

μ_{fC_2} = <105, 115, 125>

μ_{SS} = <1, 1, 1>

μ_{SF} = <0.3, 0.4, 0. 5>

μ_{C_1} will be taken as <90, 100, 110> and μ_{C_2} = <100, 110, 120>

This problem was solved, with Matlab, using Lagrange multipliers and Newton's root solving method. The algorithm checked the conditions on the fuzzy numbers stated in section 3.2.2.1 and used the appropriate arithmetic operations.

With this method, we obtained the following results:

μ_{x_1} = < 0.4865, 0.4878, 0.4889 >

μ_{x_2} = < 0.4878, 0.4889, 0.4898 >.

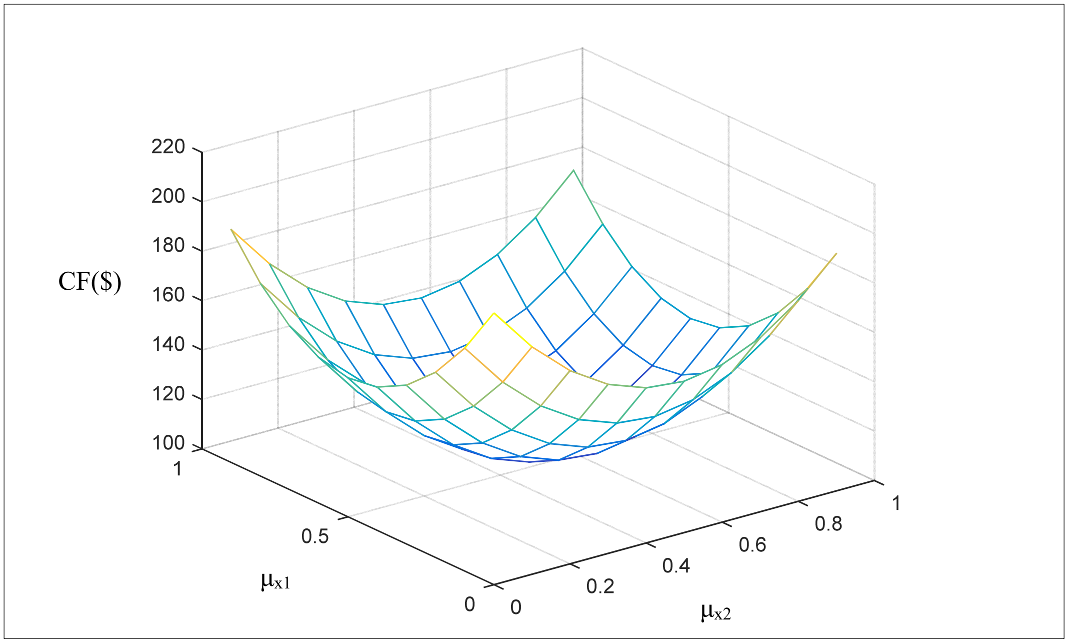

Figure 3.8 Plot of Cost Function

To test the validity of our results, we plotted the cost function (see Figure 3.8) and found indeed a zero in the vicinity of 0.5. The corresponding cost function value (as defined in eq. (1)) was CF = < 9.7022, 17.9457, 41.7209>.

We may conclude that this is a global minimum because λ_1 is calculated from equation (a), inserting the found values of μ_{x1} and of μ_{x2} , is found to be positive, as necessary from the Kuhn-Tucker conditions. To the knowledge of the authors, similar results have not been previously published.

3.7 Conclusion

In this paper we presented a methodology for risk analysis of an industrial machine based on fuzzy fault tree analysis. The fault tree for the system under consideration was built, based on a root cause analysis. The probabilities associated with the bottom events can be obtained using FMEA methods, but have been assumed in this paper. These probabilities were assumed to possess a normal probability distribution which was converted into triangular fuzzy numbers. These fuzzy numbers possess particular algebra rules which were discussed and which will be used later on in this research. The fuzzy probability of occurrence of the top event which represented a worker accident was then calculated.

In the second part of this paper we addressed a so-called inverse problem in static fuzzy fault tree analysis in which a cost function reflecting work accidents is minimized subject to the constraint that the accident probability of occurrence is specified, by regulation or standard. The problem was expressed mathematically as an optimization problem and solved using a Matlab algorithm with fuzzy numbers as arguments. The optimized variables corresponding to the contributing events probabilities of occurrence were calculated as well as the cost. This gives the analyst target values to reach for the variables that are under his/her control.

CHAPITRE 4

DYNAMIC FUZZY SAFETY ANALYSIS OF AN INDUSTRIAL SYSTEM[5]

This chapter has been presented at the 8th International Conference on Applied Human Factors and Ergonomics held in Los Angeles, California, USA, July 17th to 21st 2017

Abstract

In many industrial systems, equipment failures and worker accidents result from contributing events which occur in a certain sequence in time. These events must be analyzed, assessed and prioritized. This endeavour can be hindered by the fact that, in real life, often, the data associated with these events are not known precisely. Fuzzy numbers, provide a method for taking into account the uncertainty problem. Dynamic fault trees and Markov analyses, on the other hand, provide a means of handling the sequential character of events which can lead to work accidents. Thus, in this paper, a system safety analysis is performed using fuzzy dynamic fault tree method and Markov analysis.   A simple example is used to demonstrate this approach. In the first part of this paper, the relevant dynamic fault tree and Markov diagram are drawn and the fuzzy probability of occurrence of the accident under consideration is evaluated. The probability is calculated, not on the basis of theoretical values but, rather, on qualitative evaluation given by press brake operators in the field.

Keywords: fuzzy Markov chain, dynamic fault tree.

[5] Venditti, T., Tran, N.D.P., Ngô, A.D. 8th International Conference on Applied Human Factors and Ergonomics. Los Angeles, California, USA. July 17th to 21st 2017

4.1 Introduction

Traditional fault tree analysis takes a static view of the system; that is, the sequence in which the events leading to the undesirable event happens is not taken into account. Sometimes the sequence is important in determining the outcome. For example, consider the operation of a power press. If the protective device fails before the operator reaches into the hazardous zone of the machine, the operator may not be aware of it and the machine may not be set-up to stop in case of such a failure. In that case, the motion of the press may not be stopped and the operator's arms and hands may be caught in the closing dies of the press. If, on the other hand, the failure of the device occurs after the operator reached in the press, the hazardous motion may have stopped and the failure will not have initiated any further motion. Thus, no accident occurs. A traditional fault tree analysis would not have differentiated these two sequences. To remedy this deficiency, several approaches have been proposed. (Dugan et al., 1990), have used an approach by which sub-trees are identified with dynamic gates. (Amari et al., 2003) proposed a method where the dynamic fault tree is solved without converting it to a Markov model. (Bobbio et al., 2001) have used a Bayesian network-based approach to solve the problem.

All these approaches are capable of evaluating the dynamic fault tree under consideration but they assume that failure data or states of the systems are known and can be expressed with exact values. But in reality, uncertainties and difficulties in obtaining data are a common difficulty.

Fuzzy set theory first proposed by (Zadeh, 1965) has proven to be a useful methodology to cope with these cases where uncertainty and scarcity of data are important features.

(Li et al., 2012), have solved a dynamic fault tree problem by solving the associated Markov state equations, with fuzzy numbers in the context of the reliability analysis of the hydraulic system of a CNC machining center. However, the origin of the fuzzy data used in the paper is not explained. (Mechri et al., 2011) have used fuzzy Markov chains to analyze the reliability of Safety Instrumentation Systems. The data they used were provided by one expert. However, the process by which the expert's opinion was solicited is not explained. In this paper, a dynamic fault tree and its associated fuzzy Markov chain is solved in the case of a different type of industrial system, a brake press operation, using data collected from experts. Furthermore, in these works, the human element in the operation of these equipments and systems is not considered. In this paper, on the other hand, we solve a fuzzy Markov diagram model which represents the safety of a brake press operation. Besides the machine failure, a human factor failure is also considered.

4.2 Forward problem

The term «forward» refers to the process of evaluating the top event of a fault tree starting from the bottom events, with everything being done in terms of fuzzy numbers.

4.2.1 Fuzzy dynamic fault tree (FDFT)

A dynamic fault tree is one which contains takes into account the sequential nature of events which are related to the system under consideration. Referring to Figure 4.1 showing a general situation involving just two components, instead of using static AND gates as in a traditional static fault tree, a dynamic fault tree uses a PAND gate whose output changes to a failure state only if all of its inputs have failed in a predetermined order. Thus, in the example shown in the figure, failure 1 occurs before event 2. When these two events occur in that sequence, the top event of the fault tree, «System fails», occurs. The opposite sequence, failure of component 2, X_2, arising before failure of component 1, X_1, does not lead to the top event. One of the uses of fault trees is to calculate probabilities of occurrences of the failures or events represented in the fault tree in question. A fuzzy dynamic fault trees involves probabilities expressed as fuzzy numbers.

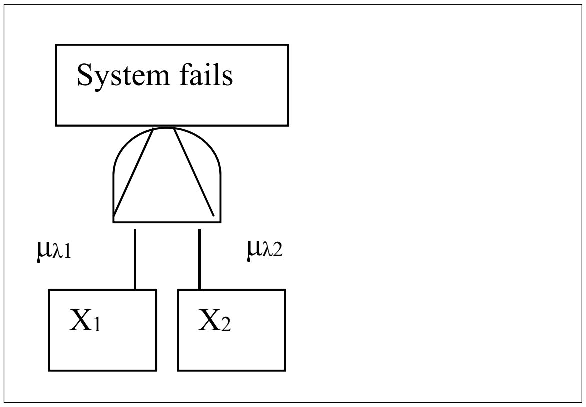

Figure 4.1 Dynamic Fault Tree

4.2.2 Fuzzy Markov Chain (FMC)

From a dynamic fault tree, a so-called Markov diagram can be drawn. This enables one to write a first-order differential state equation which can then be solved.

Markov analysis is a technique used for modeling system state transitions and calculating the probability of reaching various system states from the model, (Buckley and Eslami, 2008).

In a Markov model, a system is supposed to possess a given number of states, each defined by a set of variables. The transitions from one discrete state i to state j are considered to occur at transition rates λij. In a fuzzy Markov model, these transition rates are expressed as fuzzy numbers. Fuzzy numbers are introduced to reflect the fact that the possibility of a transition from one state of a system to another state is uncertain. Markov Chains are used mainly in reliability studies involving failures of components but can also be used in relation to human interactions with engineered systems.

4.2.3 Calculation of the top event of the dynamic fault tree using the fuzzy Markov model

In risk analysis we often do not know the precise values of the probabilities of occurrence or of failure of the systems or of its components. One way to deal with this problem is to consider that the variables of interest follow a normal probability distribution with a mean value and a standard deviation. However, another approach to the problem is to use fuzzy triangular numbers.

A fuzzy number is represented by three numbers <a_1, a_2, a_3>. Its mathematical form and graphical shape can be given as shown in Figure 4.2.

$$\mu_A(x) = \begin{cases} 0 & x < a_1 \\ \frac{X-a_1}{a_2-a_1} & \text{for } a_1 \leq x \leq a_2 \\ \frac{a_3-X}{a_3-a_2} & \text{for } a_2 \leq x \leq a_3 \\ 0 & x > a_3 \end{cases}$$

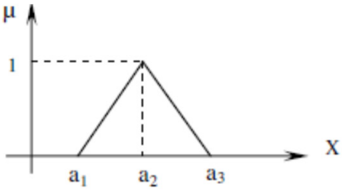

Figure 4.2 Triangular fuzzy number

In this representation, a_2 corresponds to a membership value of 1 meaning that we think that the most probable value of the variable under consideration is a_2. So a_2 corresponds to the mean value in a normal probability distribution. In this representation, we mean also that the variable under interest lies between the values a_1 and a_3, which have "membership values" of 0. In other words, a_1 and a_3 resemble the 3σ values from the mean in a standard normal probability distribution. For example, it might be ascertained that the probability of failure of a given component is «around 0.0007». This information could be expressed as a fuzzy number such as <0.00065, 0.00070, 0.00075>. What this means is that we believe that the actual probability in question is most likely equal to 0.00070 but we do not believe that it could equal a value as low as 0.00065 or a value as high as 0.00075.

In the FDFT method adopted in this work, the fuzzy probabilities associated with the basic events forming the fault tree under study are needed for the calculation of the top event probability. These probabilities are often expressed in terms of qualitative linguistic statements such as «the probability of this occurrence is thought to be low, or high, or somewhat low, etc.». For calculation purposes, these statements must be translated into fuzzy numbers (triangular in this study). This process is generally called fuzzification in the literature.

4.3 Example

As a way of illustrating the theory, brake press operation will be consider. Before delving into calculations, a brief overview of the process involved will be given. A press brake is a machine commonly found in the metal manufacturing industry. It is used to bend sheet metal in different shapes. A typical press brake is illustrated here in Figure 4.3.

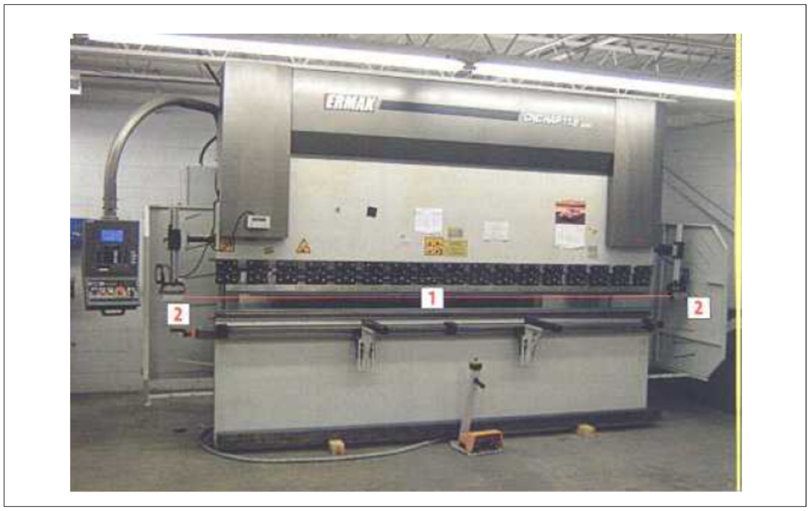

Figure 4.3 A Press brake (Source: CNESST, 2008)

The machine is composed of two main structural components, a top beam mounted on a plate and a bottom table. These two parts are usually connected by two C-frames on each side of the machine. Dies are clamped on the top and bottom parts. Either the top or the bottom half of the press then closes in (via an hydraulically-powered mechanism) on the stationary part. The operator holds the piece-part and actuates the closing motion with a foot pedal, in most applications. An hazardous situation is thus created from the proximity of the workers hands to the press closing motion. A possible undesirable event (often called a hazardous event) in such a situation is then that the worker gets his hands caught between the closing dies (the hazardous zone of the machine).

Safety regulations and standards require that such machines be equipped with protective devices which either prevent entry of the operator in the hazardous zone or stop the hazardous motion when parts of the workers body are in the hazardous zone. The protective device often utilized with press brake takes the form of a light (laser) sensor beam which spans the length of the press and is mounted between the two dies. Such a device is shown in the above picture of a press brake (1 is the sensor beam and 2 refers to the emitting and receiving components of the device).

From this general description, a simple fault tree can be drawn.

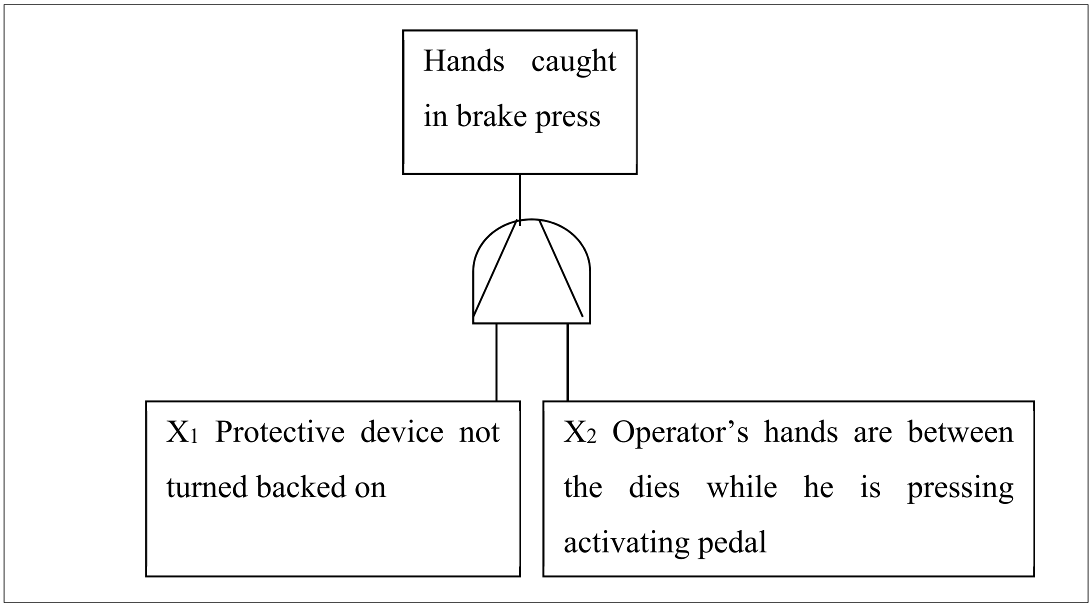
Hands caught in brake press
X1 Protective device not turned backed on
X2 Operator's hands are between the dies while he is pressing activating pedal

Figure 4.4 Fault tree

In this example, the top event occurs if two events arise. One of these consists of the worker not withdrawing his hands from between the dies. In practice, such accidents have occurred due to contributing factors such as, for example, worker fatigue due to high job repetition leading to loss of concentration, stressful work situations, very noisy or hot and humid work environment. These factors would appear in the fault tree below event X_2.

The fault tree is indeed dynamic in nature as per our definition because event X₁, protective device failure, must occur before the bending action by the worker; otherwise a properly functioning device would stop (safely) the press and no accident then occurs.

The equivalent associated Markov diagram is then as shown in Figure 4.5.

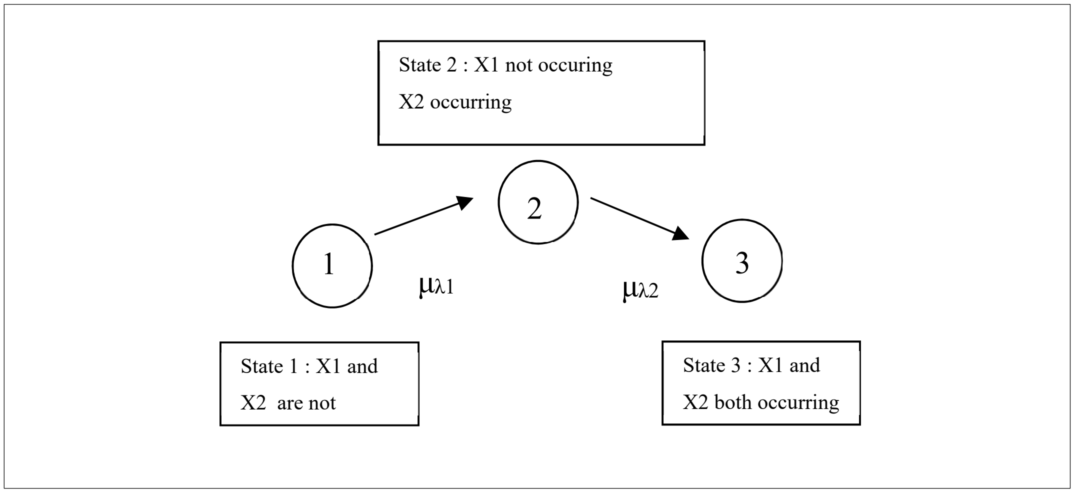

Figure 4.5 Markov Diagram

The equations of state are then:

$$\frac{dP}{dt} = \begin{bmatrix} \mu_{\lambda 1} & 0 & 0 \\ \mu_{\lambda 1} & \mu_{\lambda 2} & 0 \\ 0 & \mu_{\lambda 2} & 0 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \tag{4.1}$$

or

$$\frac{d}{dt}P = Q^T P \tag{4.2}$$

Solving with Symbolic Matlab, we obtain the expression for the probability:

$$P = 1 - \left[(1 - \frac{\mu_{\lambda 1}}{\mu_{\lambda 1} - \mu_{\lambda 2}})e^{-\mu_{\lambda 1}t} + \frac{\mu_{\lambda 1}}{\mu_{\lambda 1} - \mu_{\lambda 2}} e^{-\mu_{\lambda 2}t} \right] \quad , \tag{4.3}$$

where:

P = Probability of failure expressed as a fuzzy term;

$\mu_{\lambda 1}$, $\mu_{\lambda 2}$ = fuzzy failure rates of events X_1 and X_2

t = time which must be set , i.e we consider the state of the system after t hours.

We calculated P with the following data:

We shall take t = 50000 hours.

Calculation of the probability of occurrence P of the accident requires knowledge of the failure rates (expressed as fuzzy numbers). Specifically what is needed are: the failure rate of the protective device and, the failure rate associated with the human action consisting in having one's hands between the press dies while the operator is bending a part. The first data could, in principle be obtained from the manufacturer of the device. However, in practice, this data may not necessarily exist. In the same manner, the number of times a press brake operator places his hands between the dies of a press is not a statistic that is collected by workplaces. So, a another way to obtain the data is through expert elicitation, that is consulting people knowledgeable with the problem at hand and asking them to estimate, based on their judgement, the probabilities or failure rates that are sought.

Participants were thus solicited for this purpose. These were eight bending press operators in a large manufacturing plant. The health and safety coordinator as well as the workers' supervisor were also solicited.

The final aggregated fuzzy estimate of the probabilities is obtained by simply taking the average of the experts' estimates for each of the three components of the fuzzy numbers corresponding to the expert's linguistic probability estimate, as given in the scale.

With the final fuzzy probability estimates then on hand, the top event in the relevant fault tree is calculated. The fuzzy failure rates are calculated as $\mu_1 = <2.1203, 2.7100, 2.7871> x10^{-5}$ and $\mu_2 =<0.53434, 1.0306, 1.2963> x\ 10^{-5}$. Inserting those values into equation (4.3), we obtained P= $<0.0932, 0.1944, 0.2380> x10^{-5}$.

4.4 Conclusion

In this paper we presented a method for calculating the top event probability of occurrence of a dynamic fuzzy fault tree, a process which can be referred to as a forward problem. The fault tree models the dynamic aspect of the problem at hand, namely that the top undesirable event occurs depends on the time sequence in which the initiating events occur. A Markov diagram was derived which allows the appropriate equations of state to be written. Solving them then yielded the desired probability.

Acknowledgment: The authors acknowledge financial support from ÉREST

CHAPITRE 5

EXPERT ELICITATION METHODOLOGY IN THE RISK ANALYSIS OF AN INDUSTRIAL MACHINE[6]

This chapter was presented at The 9th International Conference on Applied Human Factors and Ergonomics held in Orlando, Florida, USA, July 21th to 25st 2017

Abstract

Calculation of the probability of occurrence of an accident involving an industrial machine such as a metal bending press requires knowledge of the failure rates. Specifically what is needed are the failure rate of the protective device and, the failure rate associated with the human action consisting in having one's hands between the press dies while the operator is bending a part. The first data could, in principle be obtained from the manufacturer of the device. However, in reality, this data involves knowledge of the reliability of not only the protective device but also of the associated command circuitry. In reality, such data may be difficult to obtain. Also, many important statistics relating to human performance are not collected by workplaces. So, another way to obtain the data is through expert elicitation, that is consulting people knowledgeable with the problem at hand and asking them to estimate, based on their judgement, the probabilities or failure rates that are sought. This process is often used in the literature but is seldom described in detail. In this paper, expert elicitation is used and described in order to gather relevant data for the purpose of probability estimation. Thus,

[6] Venditti T, Tran, N.P.D, Ngô, A.D., 2018 Expert elicitation methodology in the risk analysis of an industrial machine 9th International Conference on Applied Human Factors and Ergonomics (AHFE) Orlando, Florida, USA July 21st to 25th 2018.

eight bending press operators in a large manufacturing plant, the health and safety coordinator as well as the workers' supervisor were solicited.

A questionnaire was handed to them consisting of a set of brief instructions followed by three questions which were provided with multiple possible qualitative probability estimates to choose from. In order to improve the quality of the probability estimates, the suggested probabilities were associated with typical accidental events which serve as a comparison basis for the participants. A general introduction was given by the author to the participants in a group meeting on the shop floor which consisted of presentation the research project, its purpose. The questions and the choice of answers were read and explained to the group. The questionnaire was then handed to them. The whole process took little time to complete. These estimates represent the experts' estimates of the probability of occurrence of the events in question, expressed in linguistic, qualitative terms. These estimates were translated in quantitative terms through fuzzy logic technique. More specifically, a scale composed of qualitative statements and their corresponding triangular fuzzy number was established with two main simple guiding principles in mind. Firstly, the scale should reflect the probability scales found in often-used safety standards. Secondly, the fuzzy triangular numbers should not overlap so that there is no need to invert any of their components as required by the rules of fuzzy number arithmetic.

Keywords: expert elicitation, industrial machines, brake press safety

5.1 Introduction

Calculation of the probability of occurrence of an accident involving an industrial machine such as a metal bending press requires knowledge of the failure rates. The probability of occurrence P of the accident requires knowledge of the failure rates (expressed as fuzzy numbers). Specifically what is needed are: the failure rate of the protective device and, the failure rate associated with the human action consisting in having one's hands between the press dies while the operator is bending a part. The first data could, in principle be obtained from the manufacturer of the device. However, in practice, this data may not necessarily exist.

In the same manner, the number of times a press brake operator places his hands between the dies of a press is not a statistic that is collected by workplaces. So, an alternative to having the necessary data is to revert to expert elicitation, that is conduct a process by which people knowledgeable with the problem at hand are asked to estimate, based on their judgement, the probabilities or failure rates that are sought.

5.2 Expert Elicitation

Expert elicitation can be defined as a structured process by which experts are consulted on a subject where there is insufficient knowledge or data, (Knol et al., 2010). It is widely used in fields such as public health, (Knol et al., 2009); environmental health, (Acosta et al., 2010), in particular. Published risk assessments studies of industrial equipment and processes such as oil and gas pipeline operation, (Yuhua and Datao, 2005); chemical plants, (Renjith et al., 2010); and nuclear engineering systems, (Purba et al., 2014), on the other hand, revert to experts judgements for data gathering but this process is only scantily described.

In this study, an effort is being made to apply expert elicitation in a structured manner. The quality of the knowledge derived from experts depends on a number of factors ((Knol et al., 2010), Acosta et al., 2010); Apeland et al., 2002).

Choice of experts. What constitutes an expert is not a clearly defined notion in the literature, (Kruger et al., 2012). Should one consider scientists, professionals, managers, or field people? To answer these types of questions, the literature often adopts a broad definition of experts based on the experience, training and knowledge of the individuals, (Acosta et al., 2010).

Number of experts. The literature offers no specific advice on this issue. The number chosen seems to be dictated mostly by time/cost and availability constraints, (Acosta et al., 2010). However according to a panel of expert elicitation practitioners, as reported in (Knol et al., 2010), at least six experts should be included; otherwise the robustness of the results might be doubted. The feeling of the practitioners was that beyond 12 experts (in one elicitation session), the benefit of including additional experts seem to diminish.

Elicitation process format. An elicitation session can be conducted individually in face-to-face interviews with a prepared questionnaire or in a group meeting. Surveys or questionnaires can be mailed to participants as well. Mailed-in surveys usually have low response rates, (Ferraro, 2009). Face-to-face interview is preferred as it allows for explanations (Knol et al., 2010) and for easier engagement on the part of the participants. On the other hand, the interviewer must be careful not to influence the participants.

Experts' biases. Research (Knol et al., 2010) has shown that people use various heuristics (learned rules or hard-coded by evolution) when judging uncertain information. Some of these (Knol et al., 2010) may introduce bias in the judging process that may affect the outcome. It has also been shown that individuals consistently overestimate the likelihood of events similar to those they have recently experienced (or read about), and underestimate the probabilities of less familiar events.

(Acosta et al., 2010) suggests five specific elements designed to address these issues and improve the accuracy of the elicitation process. First, the questionnaire used in the individual interview should include an introduction which explains the aim of the exercise and the methodology that will be followed. Second, specific baseline information should be included at the beginning of the process so all the experts have a common knowledge of the issues considered. Third, technical terms and words with unclear or potentially confusing meanings must be avoided. Similarly, a plausible and specific scenario should always be given when experts have to estimate probabilities. Fourth, after giving an initial estimate, experts were required to think about one reason that could "make it wrong" (i.e., disconfirming information) and decide whether this would lead them to change their answer. Finally, and most importantly according to the authors, experts had to express their assessments of probability through simple and commonly used words (e.g., likely, high).

Once the experts' judgements gathered, they should be aggregated according to well-defined scheme. In risk assessment studies, such as the ones cited above on industrial systems, fuzzy numbers are often recommended for this purpose.

5.3 Case study

Before presenting the expert elicitation process that was followed in this study, brake press operation will be consider. A press brake is a machine commonly found in the metal manufacturing industry. It is used to bend sheet metal in different shapes. A typical press brake is illustrated here (refer to Figures 3.3 and 4.3 in previous chapters of this thesis).

The machine is composed of two main structural components, a top beam mounted on a plate and a bottom table. These two parts are usually connected by two C-frames on each side of the machine. Dies are clamped on the top and bottom parts. Either the top or the bottom half of the press then closes in (via an hydraulically-powered mechanism) on the stationary part. The operator holds the piece-part and actuates the closing motion with a foot pedal, in most applications. An hazardous situation is thus created from the proximity of the workers hands to the press closing motion. A possible undesirable event (often called a hazardous event) in such a situation is then that the worker gets his hands caught between the closing dies (the hazardous zone of the machine).

Safety regulations and standards require that such machines be equipped with protective devices which either prevent entry of the operator in the hazardous zone or stop the hazardous motion when parts of the workers body are in the hazardous zone. The protective device often utilized with press brake takes the form of a light (laser) sensor beam which spans the length of the press and is mounted between the two dies. Such a device is shown in the above referred picture of a press brake (1 is the sensor beam and 2 refers to the emitting and receiving components of the device).

From this general description, a simple fault tree can be drawn (refer to Figure 4.4 in this thesis). In this example, the top event occurs if two events arise. One of these consists of the worker not withdrawing his hands from between the dies. In practice, such accidents have occurred due to contributing factors such as, for example, worker fatigue due to high job repetition leading to loss of concentration, stressful work situations, very noisy or hot and humid work environment. These factors would appear in the fault tree below event X_2.

The data needed for the probability calculation were obtained from participants who were solicited for this purpose. These were eight bending press operators in a large manufacturing plant. The health and safety coordinator as well as the workers' supervisor were also solicited.

A questionnaire was handed to them which consisted of a set of brief instructions followed by three questions which were provided with multiple possible answers to chose from. The three questions posed were the following:

1 A bending sequence requires the worker to turn off a protective device in order to complete a certain bend due to the complexity of the shape. The worker must then turn the protective device back on to resume the bending sequence. What is your estimate of the probability that a worker forgets turn the protective device back on ?

2 What is your estimate of the probability that the protective device fails while the worker is bending a part?

3 What is the probability that a worker has his hands between the dies of the press while operating the machine?

The participants were given a choice of answers phrased in this manner:

(1) Very probable

(2) Probable

(3) Not too probable

(4) Improbable

(5) Very improbable

The questionnaire also contained examples corresponding to each of these probability statements to serve as comparison points.

A general introduction was given by the author to the participants in a group meeting on the shop floor which consisted of presentation the thesis and its purpose. The questions and the choice of answers were read to the group. The questionnaire was then handed to them. The whole process took little time to complete.

The following table summarizes the results:

Table 5.1 Results from Expert Elicitation Exercice in one Company

Participant #	Title/Function	Years of experience	Questions #		
			1	2	3
1	Brake Press Operator	23	Probable	Very improbable	Very improbable
2	Id.	30	Improbable	Very probable	Improbable
3	Id.	37	Very probable	Very improbable	Improbable
4	Id.	36	Probable	Very probable	Improbable
5	Id.	28	Probable	Probable	Improbable
6	Id.	2,5	Not to probable	Not too Improbable	Not too Probable
7	EHS Coordinator	20	Improbable	Very improbable	Improbable
8	Supervisor	10	Probable	Probable	Not too probable

These data represent the experts' estimates of the probability of occurrence of the events in question, expressed in linguistic, qualitative terms. In order for us to calculate a probability, we need to first transform these qualitative statements into quantitative, fuzzy numbers. Then, these probabilities of failure can be used to obtain failure rates. Then, the fuzzy estimates must be aggregated in order to obtain one final fuzzy estimate. In the literature, various methods are used to accomplish this process. In (Ferraro, 2009), the linguistic estimates are related to fuzzy numbers expressed mathematically in the form of an equation representing a triangular fuzzy number. The final aggregated estimate is then a weighted average of these fuzzy numbers. In (Page, 2012), (LAvasini et al., 2015), Gierczak, 2014), Je farina and Rezvani, 2012) translate the linguistic estimates of the experts into fuzzy numbers expressed as a triplet of numbers. The aggregation is then taken as a weighted average of the experts' opinions, the weighing method taking into account various factors.

In this work, we adopted a scale which combines the direct fuzzy number translation approach with a probability level from recognized safety standards such as (Departement of Defense, USA).

We translate the linguistic statements into fuzzy numbers by establishing a fuzzy scale which consists in associating a fuzzy number with each qualitative statement:

Table 5.2 Linguistic terms and fuzzy numbers

Very improbable	<0, 1, 10>x10^{-6}
Improbable	<1, 5, 10> x10^{-4}
Not too probable	<1, 5, 10> x10^{-3}
Probable	<1, 5, 10> x10^{-2}
Very probable	<1, 5, 10> x10^{-1}

The final aggregated fuzzy estimate of the probabilities is obtained by simply taking the average of the experts' estimates for each of the three components of the fuzzy numbers corresponding to the expert's linguistic probability estimate, as given in the scale. No weighing has been done for the following reasons. All workers have extensive experience except for one worker who had 2.5 years of experience. However, all workers get thorough technical training on all aspects of press brake operation. In addition, specific health and safety training sessions are periodically given to all workers. The company in question is a large, unionized, well-structured enterprise which performs extensive, on-going, health and safety monitoring and preventive activities.

Probability of occurrence can be related to failure rates using reliability theory and assuming that the failure rates are constant, the probability of occurrence of the accidental event considered in the constructed fault tree can then be calculated.

5.4 Conclusion

In this paper we presented an expert elicitation method for extracting the required daa needed for probability calculations related to an accidental event in an industrial machine such as a metal brake press. An expert elicitation exercice was conducted in a large manufacturing plant. Linguistic judgement of probabilities were obtained. The data was quantified and aggregated so that the final probability of occurence of an accidental event could be estimated.

CHAPTER 6

ANALYSIS OF AN INDUSTRIAL SYSTEM USING MARKOV RELIABILITY DIAGRAM WITH REPAIR[7]

This Chapter was presented at The 12th International Virtual Conference on Applied Human Factors and Ergonomics held in San Diego, California, USA, July 15th to 17st 2020

Abstact

In many industrial systems, accidents result from equipment failures and human errors. The latter can thus be viewed as a form of system failure which must be identified and analyzed. In this paper, an industrial system made up of a brake press operated by a single operator is analyzed. a reliability Markov diagram including repair states is drawn to model the system. The probability of a work accident (failed state of the system) is calculated using fuzzy numbers. An innovative aspect of this study is that repair states for human failures are also defined and their repair rates are estimated. The equations of state of the system are then derived and solved. Thus, the probability of the system being in a failed state is calculated.

Keywords: Fuzzy Methods · Markov Diagram · Human Error · Repair Rate

[7] Venditti, T., Tran, N.D.P., Ngô, A.D. (2020) 12th International Virtual Conference on Applied Human Factors and Ergonomics held in San Diego, California, USA, July 15th to 17st 2020

6.1 Introduction

Industrial machine constitute systems composed of different components such as, in particular the machine itself, the operator, the work-piece, and the command interface and circuit. As a way of illustrating the theory, brake press operation will be consider. A press brake is a machine commonly found in the metal manufacturing industry. It is used to bend sheet metal in different shapes. A typical press brake is illustrated here (refer to previous figures in this thesis such as Figure 5.1).

The machine has been described in some detail a previous paper, (Venditti et al., 2017). But briefly, in the operation of the press, the operator holds the piece-part and actuates the closing motion of the press with a foot pedal, in most applications. A hazardous situation is created from the proximity of the workers hands to the press closing motion. A possible undesirable event (often called a hazardous event) in such a situation is then that the worker gets his hands caught between the closing dies (the hazardous zone of the machine). Safety regulations and standards require brake presses to be equipped with safeguarding protective devices such as light curtains of laser beam sensors.

A dynamic fault tree related to this situation, see (Venditti et al., 2018), for more details, appears like so:

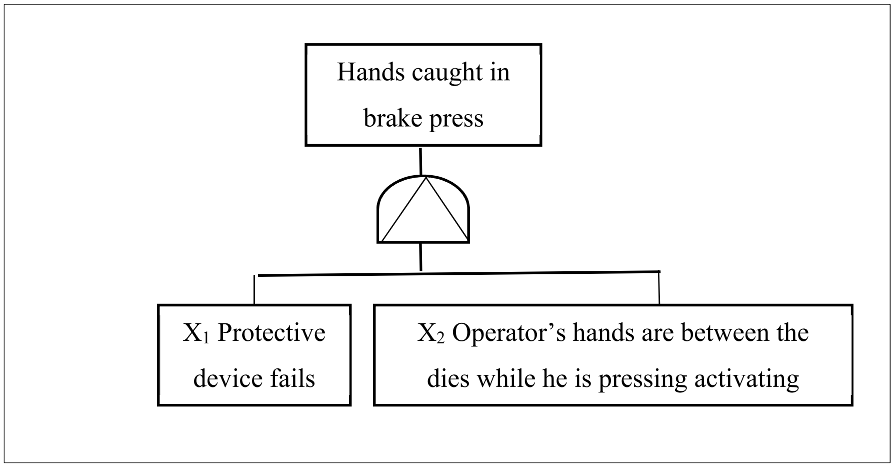
Hands caught in brake press
X_1 Protective device fails
X_2 Operator's hands are between the dies while he is pressing activating

Figure 6.1 Dynamic Fault Tree

The fault tree is dynamic in nature because event X_1, protective device failure, must occur before the bending action by the worker; otherwise a properly functioning device would stop (safely) the press and no accident then occurs.

6.2 Markov Analysis

The equivalent associated Markov diagram is then:

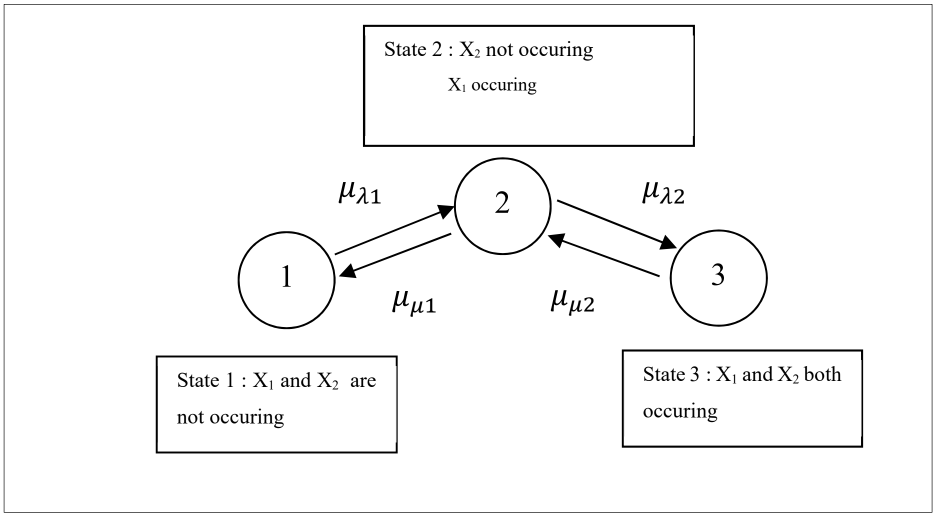
State 2 : X2 not occuring
X1 occuring
$\mu_{\lambda 1}$
$\mu_{\lambda 2}$
2
1
3
$\mu_{\mu 1}$
$\mu_{\mu 2}$
State 1 : X1 and X2 are not occuring
State 3 : X1 and X2 both occuring

Figure 6.2 Markov Diagram with Repair

In this diagram, State 1 represents the condition where the protective device functions properly and the operator keeps his hands out of the hazardous zone. State 2 describes the situation where the protective device fails to detect the hands of the worker and fails to stop the closing motion. In State 3, the worker commits a human error by putting his hands in the hazardous zone due to various contributing factors such as fatigue, repetitive task, distraction, etc.

The equations of state are then

$$\frac{d}{dt}P = \begin{bmatrix} -\mu_{\lambda 1} & \mu_{\mu 1} & 0 \\ \mu_{\lambda 1} & -\mu_{\lambda 2}-\mu_{\mu 1} & \mu_{\mu 2} \\ 0 & \mu_{\lambda 2} & -\mu_{\mu 2} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \tag{6.1}$$

or $$\frac{d}{dt}P = Q^T P \tag{6.2}$$

The initial conditions for the problem are: $P_1 = 1$ because state 1 represents the system in working conditions and no failures are occurring.

The basic assumptions used in the model are as follows:
- component failures and repair rates are statistically independent, constant, very small and obey exponential distribution function
- the product of the failure rate and repair time is small (less than 0.1);
- there are no simultaneous failures among the subsystems;
- separate maintenance facility is available for each component;
the repair process begins soon after a unit fails;
- after repairs, the repaired component is considered as good as new;
- system structure is precisely known.

In this equation, in the right hand side, the matrix Q contains terms having units hr^{-1}. Therefore, on the right hand side , the units should also be hr^{-1}. Hence, P has no units and therefore represents a probability, not a rate.

The meaning of the terms are:
$\mu_{\lambda 1}$ = the failure rate of the protective device in units of h^{-1} (a fuzzy number)
$\mu_{\lambda 2}$= the human failure rate in units of h^{-1} (a fuzzy number)
These data come from an expert elicitation exercise performed by the authors, details provided in (Venditti, 2018b).
$\mu_{\mu 1}$ = the repair rate of the protective device
$\mu_{\mu 2}$= the repair rate following a human failure
The repair rates merit further explanations. The repair rate is defined as

$$\frac{1}{MTTR\ (Mean\ Time\ to\ Repair)}$$

in units of h^{-1} as it should.

This definition is well suited for technical repairs a in the model. A brief search on internet led to a value of 2.5 hours average repair time for a safety light curtain as given by various brake press service suppliers.

However, what about when referring to human error? In this case, the ''repair'' refers to re-training the worker following the event ''Putting his hands between dies''. The value chosen is based on actual practical experience. It is common practice after incidents to give initially trained workers a re-training session focusing on the factors that affected the event. A typical length for this kind of re-training (a ''refresher session'') is 2 hours. Hence 0.5 h^{-1} was the adopted value.

6.3 Results

The results are then, with the following data:

$\mu_{\lambda 1}$ = <2.85, 3 ,3.15>x10^{-5}; $\mu_{\lambda 2}$ = <0.95, 1 ,1.05>x10^{-5}; $\mu_{\mu 1}$ = <0.119, 0.125 ,0.131> ;
$\mu_{\mu 2}$ = <0.475, 0.5 ,0.525> :
P_3 = <4.7878, 4.7979, 4.8070> x10-^{9}

6.4 Conclusion

In this paper we presented a method for calculating the top event probability of occurrence of a fuzzy dynamic fault tree and its associated Markov diagram which represented the operation of a brake press. The model included not only failure rates but repair rates as well. A novel feature of the model was the inclusion of a human-related repair rate. The Markov diagram was solved and the desired probability was calculated.

Acknowledgments. The authors acknowledge financial support from ÉREST.

CHAPTER 7

BRAKE PRESS SYSTEM WITH DEVICE AND HUMAN FAILURE MODES, REPAIR RATES AND REDUNDANCY

To be published

Abstract

Brake presses are machines widely used in the manufacturing industry to bend metal sheets. They pose risks in terms of equipment failure and worker accidents. In order to prevent these unwanted occurrences, the associated risks must first be analyzed. In this paper, such an analysis is conducted for a brake press system incorporating redundancies such as two operators and two point-of-operation safety devices. The probability of the system being in a failed state where an operator suffers an injury is estimated with the help of a Markov diagram which includes failure and repair rates not only for the devices but also in terms of operators' failures (errors).

7.1 Introduction

This chapter presents the case of a brake press operated by the two operators. This situation arises in actual work settings when large sheets of metal are being bent in a brake press. In that case, the second operator is necessary to hold the work-piece properly where proper work-holding tables and fixtures are not present. However in this study, the work station setup will in fact be different. The second operator will assume the role of an assistant who is there to make sure that the work proceeds correctly and safely. For instance, if the notices the first operator making an error he will be in a position to intervene and stop the machine. This set-up becomes a system which will be modelled mathematically and solved for safety-related variables of interest.

In the previous conference papers, the dynamic fault tree corresponding to two models of a brake press system were presented and solved. One model involved the case where failure events both technical and human-related occurred. The second one modelled in mathematical terms a notion of repair. In Chapters 3 and 4, the cost function concept was introduced in the case where only failures were considered but not the repairs. In this paper, following the presentation of the forward problem, the cost function concept is expanded further by including the repair costs involved.

7.2 Literature review

7.2.1 Redundancy and device failure

Redundancy can be defined as ''the existence, in an entity, of more than one means for performing a required function'' (IEC 60050-191). In the context of machine safety, the function that needs to be performed can be:

- stopping the hazardous motion
- assuring the safe position of a component of a machine. For instance, maintaining the upper die in an hydraulic brake press in an elevated position, supported by the hydraulic pressure in a cylinder.

On an industrial machine, redundancy can be achieved commonly in two important ways.

- Two safeguarding can be installed to prevent entry into the hazardous zone or contact with the hazardous zone of a machine. An example of redundant safeguarding is shown in the figure where a safety light curtain is used in conjunction with a two-hand control on a mechanical punching press to prevent entry into the hazardous zone (the dies, only partially visible on the photograph) of the press.

- Industrial machines' control systems are another area where redundancy is put in place. For instance, two electrical contactors can be placed in series with the motor of a machine. This way, if following a stop command, the contacts in one of the contactors fails by staying closed because of a malfunction, redundancy assures de-energizing of the motor provided the second contactor functions correctly.

7.2.2 Human Error and Redundancy in machine safety

7.2.2.1 Human error

The evaluation of reliability and safety of industrial systems such as industrial machines is considered important due to factors such as complexity, cost, design requirement and so on. Accidents may occur due to human errors caused by omissions or commissions of incorrect actions due to a number of reasons such as lack of training on specific equipment, systems and operating procedures, lack of existing operating procedures, incorrect operating procedures, poorly designed work stations, lack of a thorough risk identification analysis and among others. Many studies, (Dhillon, 1986), (Robinson et al., 1970) have highlighted the fact that failure of repairable systems can occur not only due to hardware failure (deficiencies in design weakness of material, manufacturing imperfections and normal wear and tear) but also due to operating human error or maintenance human error. Human interact with engineering systems in many ways. It is a well-known fact that a significant proportion of total human errors occur during the maintenance phase, (Chinniah Y. and Poisson P, 2015). For example, according to these authors, about 25 per cent of the maintenance events described in 213 problem reports from the field were due to human errors. Factors such as temperature, dust, fatigue, incomplete or inappropriate maintenance tools, incorrect operating procedures and personal problems may be the causes for human errors in both maintenance and operation phases. Redundancy is often used to increase the reliability of a system without any change in the reliability of the individual units that form the system. Standby configuration is one form of redundancy. In this case, one or more units operate and the remaining redundant units are kept in their standby mode. Each of the active units may experience a failure due to normal malfunction, common-cause failure or human error. Generally, reliability models assume that the system failure probabilities and repair times are exponentially distributed. This model thus assumes that failure rate and repair rate are constant.

Human factor contributes significantly in accident dynamics and also in severity of consequences. Human intervention is not insignificant in system failures (Kirwan, 1994). Estimates show that 60% of the accidents are caused due to errors committed by man and the technical deficiencies contribute the rest. Over 90% of nuclear industry accidents (Reason, 1990), over 80% in petrochemical and chemical industries accidents (Kariuki and Lowe, 2007), over 75% of casualties in marine sector (Ren et al., 2008), and over 70% of accidents in aeronautical sector (Hollnagel, 1998) have been reported with human faults as the prime cause. Overall on a world scale, severe accidents are believed to be caused by human error in 40% to 50% of the cases (Nascimento and de Mesquita, 2012). Thus in accident dynamics, human role should be considered in order to guarantee the effective prevention of hazardous events, during risk analysis (Ruckart and Burgess, 2007). In practice, human error proves to be a significant cause which leads to accidents in many industrial environments.

Human error can be defined as a divergence between the actual action accomplished and the action that should have been taken, (Dhillon, 2009). (Dhillon et al., 1995) cites that according to various studies the human error rate is not actually constant. In fact, it increases during period of fatigue and under stress. However, in this study, the human error rate will nevertheless be taken as constant.

Human error rate has often been considered to be constant in human-machine system analysis. But according to various studies, as cited by (Dhillon et al., 1995), it is not always the case. In fact, it increases during the fatigue period or under stress. This work presents a mathematical model to perform a reliability and safety analyses of a general industrial system with constant human error rates and failed system repair rates. However, systems can also fail due to other types of events, in particular so-called common-cause failures. In this failure mode, redundant, parallel components can both fail if they are affected and attacked by a common cause. In the model developed here, it will be assumed that the context in which the machine under consideration will not be affected or if affected the probability of such an occurrence will be well below that of the failures being analyzed.

7.2.2.2 Human redundancy

According to (Clarke, 2005), human redundancy can be defined, in a manner similar to technical redundancy, as a situation in a technical system in which ‘’two or more operators are concerned with the fulfilment of a required function and have access to information relevant to that function’’.

Through partial analogy with redundancy in hardware systems, active and standby forms of human redundancy can be identified. Active human redundancy requires that the individual fulfilling a redundant function is involved in the task at hand. Practically this can be implemented, for example, with a second worker or a supervisor checking the work of the operator. The redundant individual will often be located in the operator’s immediate work environment, but can also be engaged in a task remotely. Commonly, an operator fulfills a function while another monitors the performance of that operator with respect to the required function. Less frequently, two operators carry out identical tasks to achieve the same function. The efficacy of human redundancy in an industrial system depends on human performance. Human behavior in the context of work has been classified into skill-, rule- and knowledge-based modes (Rasmussen, 1983; Reason, 1990).

The skill-based mode refers to the smooth execution of highly practiced, largely physical actions in which there is virtually no conscious monitoring. Skill based responses are generally initiated by some specific event, e.g. the requirement to operate a valve, which may arise from an alarm, a procedure, or another individual. The highly practiced operation of opening the valve will then be executed largely without conscious thought.

In the rule-based mode, actions are accomplished to an explicit rule or procedure. This behavior is typically followed by a less experienced operator. The operator may forget parts of the procedure, not follow the procedure correctly such as in the incorrect sequence or make mistakes at some steps along the procedure.

In the knowledge-based mode, the human carries out a task in an almost completely conscious manner. This would occur in a situation where a beginner was performing the task (e.g. a trainee process worker) or where an experienced individual was faced with a completely novel situation. This requires of the operator to analyze a situation, interpret the information or make a difficult decision.

7.2.3 Cost Function involving Repair

In order to establish a cost function involving repairs on the system, it is then wise to review literature related to reliability and repair theory and to maintenance engineering.

The following presentation is based on standard texts such as the one by Lewis, (1994).

Reliability, R(t), is defined as the probability that a system/component/part operates without failure for a length of time t.

Unreliability, F(t), can then be defined as the failure probability of a system/component/part in the time interval from zero to t.

Failure rate can be defined in its simplest form as the number of failures of a system/component/part that has occurred in a given period of time t. Failure rate can also be defined as the probability of failure per unit time, Dunbar (1984).

MTTF is the Mean Time to Failure is the mean time that a system/component/part will operate before experiencing a failure.

MTBR is the Mean Time between Repair is in fact similar to the MTTF if, when a system fails it is assumed to be repaired immediately to an as-good-as-new condition.

MTTR is the Mean Time to Repair which is the expected value of the repair time or in other words the mean time that a repair will take.

Repair rate, μ, when it can be considered as constant, is calculated as:

μ (t) = Repair rate = 1/MTTR.

Similarly, the failure rate, when taken as a constant value, can be calculated as the inverse of the MTTF. Repair rate, as mentioned by Dunbar (1984), can also be defined as the probability of repair per unit time.

Maintainability is the probability that a failed system/component/part of equipment/item is restored to its satisfactory operating state within a time t by applying maintenance. Mathematically, it is expressed as:

Maintainability is the probability that a failed system/component/part of equipment/item is restored to its satisfactory operating state within a time t by applying maintenance. Mathematically, it is expressed as:

$$M(t) = 1 - e^{\int_0^t \mu(t')dt'}$$

In many analyses, it will have to be replaced. Theory shows that the probability of repair can be related to the probability that a failure may be repaired and the system fully restored to working order. To illustrate, consider a device which fails, the repair term in a Markov transition diagram relates to probability that the failed device might be repaired. Otherwise ear function of the time to repair and thus to the MTTR and thus to the repair rate. On a portion of the function curve, the relation can be linear. This can be taken as a valid approximation.

Availability of a machine, for a given period, is defined as the percentage of time during which the machine is producing its designed output adequately. Availability can be viewed as the most important measure of the effectiveness of a machine, assuming that all systems being considered are repairable.

Availability, mathematically, is given by *A* = Total uptime / (Total uptime + Total downtime)

Also, *A* = MTBF / (MTBF + MTTR)

7.2.4 Types of maintenance

Various types of maintenance and maintenance strategies exist. The following review is based on (Pérès & Noyes, 2003), in which further references can be found.

The strategies of maintenance are as diverse and varied as are the systems of production to which they are applied. But beyond their differences, the objective of each of these strategies is to maintain the system of production in a working condition as long as possible or to restore it as quickly as possible in the case of failure.

To begin with, a distinction is to be made between the works which treat the interventions of perfect maintenance (making the system as good as new) and imperfect maintenance (repairing the system to a less deteriorated state, but without completely eliminating the damage). Certain authors imagine the two scenarios with the maintenance being sometimes perfect with the probability of p, sometimes imperfect with the probability of $1 - p$. Other authors speak of minimal maintenance to describe an intervention which brings the system into a less deteriorated state, but without specifying the level of residual deterioration. The term corrective maintenance is applied to the maintenance strategy which restores the system to a pre-failure state. The term 'systematic preventive maintenance' is employed to describe preventive interventions implemented on fixed dates and with constant intervals. Conditional preventive maintenance is characterized by maintenance interventions carried out after the detection of signals emitted by the system revealing present or imminent dysfunction.

Preventive maintenance is only of interest to the extent in which it can be applied to a system which has a failure rate that is not constant. However, as mentioned, this ''Poissonian'' hypothesis, because of the simplicity of its utilization, is widely used for the modelling of the failure process. However, it must be mentioned that numerous works use other more realistic laws representing different failure rates. For example, an increasing rate may be considered. Weibull's law, reputed for accurately interpreting the failure rate increasing period but which is difficult to manipulate, is only used in certain works. The Erlang law also appears. Lastly, certain works consider non-homogenous Poisson laws, log-normal distributions, the law of extreme values or arbitrary rates to characterize the phenomenon of failure.

7.2.5 Costs in machine life cycle

Over the life cycle of a machine various costs are incurred such as installation, maintenance, operation, material, electricity, etc,, According to (Murty and Naikan, 1993) the following factors are important:

Fixed cost. Includes capital investment for machinery, structural requirements, instruments and other accessories. Fixed cost remains constant with changes in availability.

Cost of material, electricity, packing, marketing, etc. Since the rate of production is proportional to availability, this cost varies linearly with variations in plant/machinery availability.

Cost of maintenance for achieving higher availability. This includes cost of spare parts, lubricants, maintenance equipment, training of engineers and workers, application of computer for maintenance, software packages and on-line monitoring, etc. This has a non-linear variation (generally exponential: prohibitively higher expenses at higher availability) with availability.

Wages and salaries. This remains almost constant with availability.

Total cost. This is the sum of the above costs.

Total income or returns. Since rate of production is proportional to availability, total income or returns is also proportional to availability.

Net profit. This is the net benefit of running a plant:

Net profit = Total income – Total cost (expenditure).

The literature on costs contains mostly papers which deal with two general categories of problems: costs of repairs and maintenance and costs of accidents. Thus, many papers endeavor to compute the costs which work accidents and machine breakdowns entail. For example, Examples of the first category of paper include for example, Dolas et al. (2014) who considered different regression models for determining repair and maintenance costs functions of farm tractors as a function of hours of operation. Their study concluded that suggested that power (terms raised to a power) and polynomial models give better cost prediction with higher confidence and less variation than that of exponential and logarithmic models.

It seems, on the other hand, that few papers have been published that attempt to relate costs to probabilities of accidents or to failures, that is to say, to reliability. (Murty & Naikan, 1993) developed a function which relate the costs in terms of given levels of availability. Their model is a power function. The shape of the function is determined from a curve fitting with historical data. (Guikema & Paté-Cornell, 2002) tackle the problem of minimizing the probability of system failure p (Fm $|$Im) conditional on the level of investment for m=1…N components. The authors refer to the expression for p (Fm $|$Im) as the risk/cost function. (Aven, 2003) presents a model which relates the level of investment to the probability of accidents. It uses linear equation relating probability of accident and investment in safety and prevention. (Aven, 2011), in a subsequent paper, suggests a method whereby coefficients can be determined which goes as follow. Suppose a risk assessment has been perform on a given situation and has produced some values of probabilities. Quoting from his paper: ''For example, for a gas leakage of a specific size, a probability p(0) = 4×10–^{4} is assigned; the risk assessment has also produced an assignment p(10) = 2×10–^{4} corresponding to the implementation of a risk-reducing measure that costs 10. The expert group then considers several other investment levels and uses the risk assessment to produce corresponding probabilities. A smooth curve is then fitted to the assigned points. This curve represents judgments made by the expert group based on the risk assessment being conducted for the installation.'' (Feng, 2015), in a similar fashion, established an equation relating the level of safety investment necessary for a given accident rate. His shape is a negative exponential which corresponds to the terms related to the costs of failure in the present model. (Aggarwal, 1993) in his textbook presents six models of curves relating costs to levels of reliability. The shape of the functions proposed are also obtained using curve fitting and historical data. (Aubert & Bernard, 2004), (Rhee & Ishii, 2003), (Sentuge et al., 2015) and others define a Cost of Risk function in terms of the probability of undesirable events multiplied by the estimated cost associated with each event.

It can be seen from this review that the basic cost function model generally adopted is one which multiplies a probability with a cost term. The degree of the function is best determined from a curve fitting procedure. Expert judgement and/or historical data can be used.

7.3 Forward problem

The brake press described and analyzed in the previous chapter will now be considered to incorporate elements of redundancy both at the hardware level and at the human level. Hardware redundancy will take the form of two safety devices between the machine and the operator. For example, these could be as shown on Figure 7.1, a two-hand device and a safety light curtain. It is assumed that the workstation has been designed so that adequate support devices have been provided on the brake press so that the operator does not need to hold the work-piece at any time during the bending process. He only needs to handle manually the work-piece when repositioning is necessary for the subsequent bend.

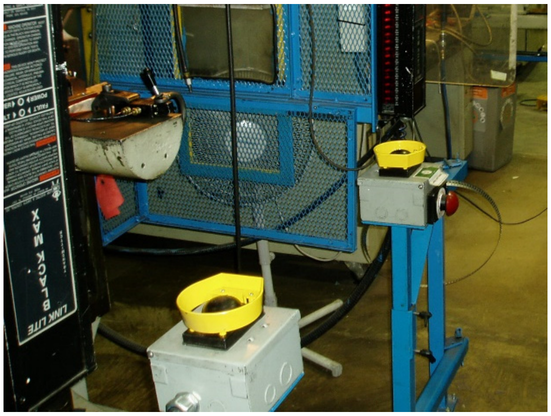

Figure 7.1 Mechanical punch press with redundant protective devices

Human redundancy will consist of two workers at the workstation. At any instant of time during production, one worker will act as the actual operator. The second worker will assume the role of a checker. This will set-up a humanly-redundant work situation in conformity with the definitions seen in the literature. Both workers will be assumed to possess similar levels of training and experience.

Two human modes of failures are assumed to be necessary for accident generation. These failures result in the worker not withdrawing his hands from between the dies. In practice, such accidents have occurred due to contributing factors (modes of failures) such as, for example, worker fatigue due to high job repetition leading to loss of concentration, stressful work situations, very noisy or hot and humid work environment. These factors would appear in the fault tree below event X_1.

In conclusion, in the industrial system studied in this work, redundancy exists at the technical level in the form of two safeguarding devices. But there is no human redundancy as understood and defined in the literature. Rather, at the human level, the system being considered here is subject to two modes of human failures.

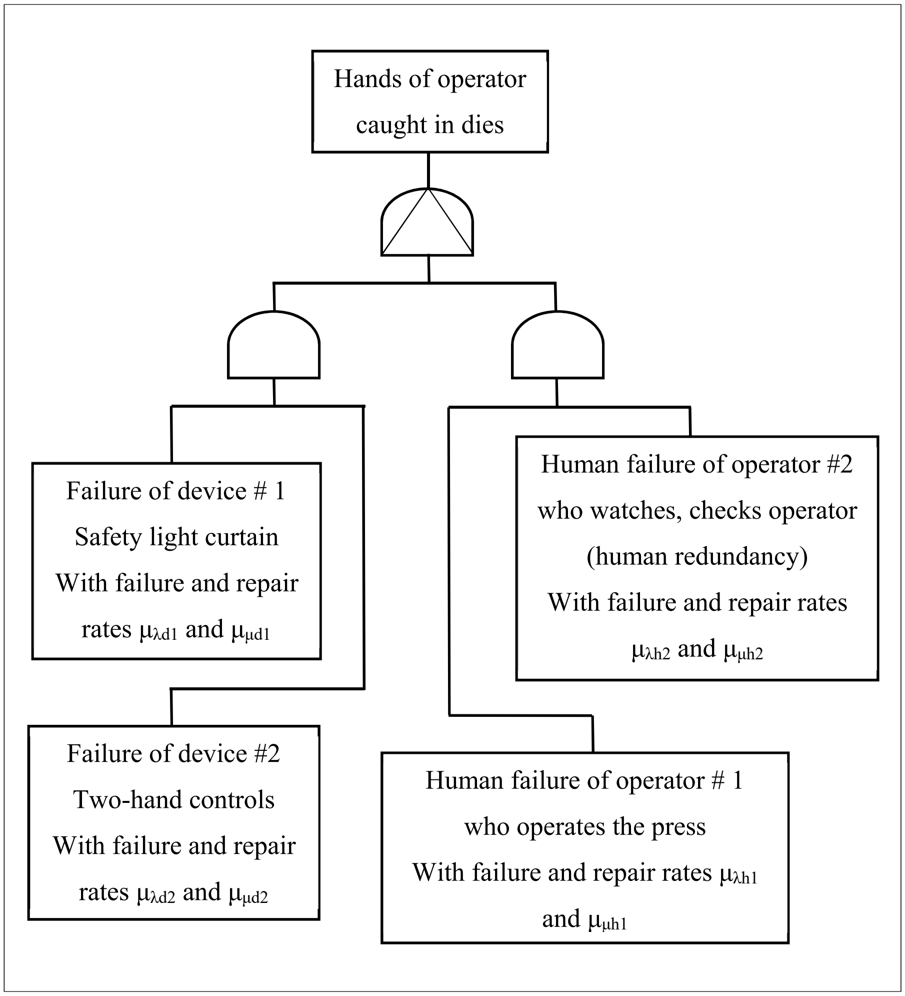
Hands of operator caught in dies
Failure of device # 1 Safety light curtain With failure and repair rates $\mu_{\lambda d1}$ and $\mu_{\mu d1}$
Human failure of operator #2 who watches, checks operator (human redundancy) With failure and repair rates $\mu_{\lambda h2}$ and $\mu_{\mu h2}$
Failure of device #2 Two-hand controls With failure and repair rates $\mu_{\lambda d2}$ and $\mu_{\mu d2}$
Human failure of operator # 1 who operates the press With failure and repair rates $\mu_{\lambda h1}$ and $\mu_{\mu h1}$

Figure 7.2 Fault Tree with Repair, Redundancy and Human Error

The fault tree is indeed dynamic in nature as per our definition because event X1, protective device failure, must occur before the bending action by the worker; otherwise a properly functioning device would stop (safely) the press and no accident then occurs.

The equivalent associated Markov diagram is then:

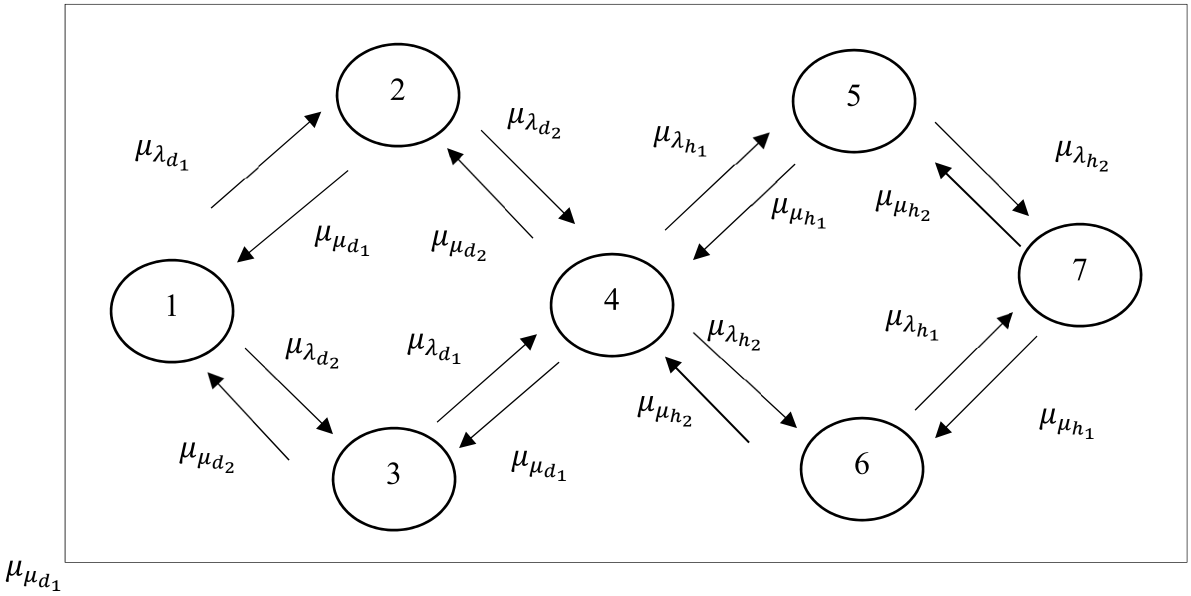

Figure 7.3 Markov Diagram with Repair, Redundancy and Human Error

The calculation presented here can be used to show that systems with redundant failure modes and redundant protective devices can result in probabilities of occurrence of accidents which are very low.

$$\frac{d}{dt}\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \end{bmatrix} = \begin{bmatrix} Q_{11} & Q_{12} & Q_{13} & 0 & 0 & 0 & 0 \\ Q_{21} & Q_{22} & 0 & Q_{24} & 0 & 0 & 0 \\ Q_{31} & 0 & Q_{33} & Q_{34} & 0 & 0 & 0 \\ 0 & Q_{42} & Q_{43} & Q_{44} & 0 & 0 & 0 \\ 0 & 0 & 0 & Q_{54} & Q_{55} & 0 & Q_{57} \\ 0 & 0 & 0 & Q_{64} & 0 & Q_{66} & Q_{67} \\ 0 & 0 & 0 & 0 & Q_{75} & Q_{76} & Q_{77} \end{bmatrix}\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \end{bmatrix} \tag{7.1}$$

or

$$\frac{d}{dt}P = Q^T P \tag{7.2}$$

where

Q_{11} = -$\mu_{\lambda_{d_1}} - \mu_{\lambda_{d_2}}$; Q_{12} = $\mu_{\mu_{d_1}}$; Q_{13} = $\mu_{\mu_{d_2}}$

Q_{21} =$\mu_{\lambda_{d_1}}$; Q_{22} = $-\mu_{\lambda_{d_2}} - \mu_{\mu_{d_1}}$; Q_{24} = $\mu_{\mu_{d_2}}$

Q_{31} =$\mu_{\lambda_{d_2}}$; Q_{33} = $-\mu_{\lambda_{d_1}} - \mu_{\mu_{d_2}}$; Q_{34} = $\mu_{\mu_{d_1}}$

Q_{42} =$\mu_{\lambda_{d_2}}$; Q_{43} =$\mu_{\mu_{d_1}}$; Q_{44} = $-\mu_{\lambda_{h_1}} - \mu_{\mu_{d_2}} - \mu_{\lambda_{h_2}} - \mu_{\mu_{d_1}}$

Q_{54} =$\mu_{\lambda_{h_1}}$; Q_{55} = $-\mu_{\lambda_{h_2}} - \mu_{\mu_{h_1}}$; Q_{57} =$\mu_{\mu_{h_2}}$

Q_{64} =$\mu_{\lambda_{h_2}}$; Q_{66} = $-\mu_{\mu_{h_2}} - \mu_{\lambda_{h_1}}$; Q_{67} = $\mu_{\mu_{h_1}}$

Q_{75} =$\mu_{\lambda_{h_2}}$; Q_{76} = $\mu_{\lambda_{h_1}}$

Q_{77} = $\mu_{\mu_{h_2}} - \mu_{\mu_{h_1}}$

$\mu_{\lambda_{d_i}}$refers to failure rates of the protective devices

$\mu_{\lambda_{h_i}}$refers to human failure rates

$\mu_{\mu_{d_i}}$refers to repair rates of the protective devices

$\mu_{\mu_{h_i}}$refers to human repair rates

The initial conditions for the problem are: P_1 =1 because state 1 represents the system in working conditions and no failures are occurring.

In this equation, in the right hand side, the matrix Q contains terms having units hr^{-1}. There fore, on the right hand side , the units should also be hr$^{-1.}$ Hence, P has no units and therefore represents a probability, not a rate.

Equation (7.2) will be solved using Euler's forward-in-time algorithm for initial-value problems whose general vector form is :

$$\mathbf{y}_{k+1\cong[\mathbf{I}+\Delta t_k\mathbf{A}_k]}\mathbf{y}_k + \Delta t_k\mathbf{g}_k \tag{7.3}$$

where bold symbols refer to column vectors.

Applying it to the present case yields

$$\mathrm{P}_{\mathrm{t}+1} = (\mathrm{I} + \Delta\mathrm{t} * \mathrm{Q}^{\mathrm{T}})\mathrm{P}_{\mathrm{t}} \tag{7.4}$$

where P has been previously defined as the vector containing the probabilities of each of the 7 states of the system. Q is the transition matrix also defined previously. The interval in time is taken as 1 hour. The initial state of the system is $\mathrm{P} = [1,0,0,0,0,0,0]'$ i.e. P is a column vector.

The algorithm was run on Matlab using the data from previous paper where values for λ_{d1} the mode of failure associated with the safety light curtain and λ_{h1} the human mode of failure ‘’Hands in dies’’ were obtained from an expert elicitation exercice. The other data are assumed and result from an elementary internet search.

For a time t = 50 000 hours, the complete set of input data is collected here:

Table 7.1 Input data set Case Study including Repair and Redundancy

Data	Lower values of TFN (h^{-1})	Middle values of TFN (h^{-1})	Upper values of TFN (h^{-1})
$\mu_{\lambda_{d_1}}$	$2.71*10^{-5}$	$2.71*10^{-5}$	$2.84*10^{-5}$
$\mu_{\mu_{d_2}}$	$2.71*10^{-5}$	$2.71*10^{-5}$	$2.84*10^{-5}$
$\mu_{\lambda_{h_1}}$	$1.03*10^{-5}$	$1.03*10^{-5}$	$1.08*10^{-5}$
$\mu_{\lambda_{h_2}}$	$1.03*10^{-5}$	$1.03*10^{-5}$	$1.08*10^{-5}$
$\mu_{\mu_{d_1}}$	0.119	0.125	0.131
$\mu_{\mu_{d_2}}$	0.119	0.125	0.131
$\mu_{\mu_{h_1}}$	0.47	0.50	0.52
$\mu_{\mu_{h_2}}$	0.47	0.50	0.52

The complete results for the vector P are then:

Table 7.2 Complete Results for Vector P Case Study including Repair and Redundancy

P	Lower values of TFN	Middle values of TFN	Upper values of TFN
P_1	0.999568161467824	0.999566492623574	0.999566502486222
P_2	0.000215873120110	0.000216706011731	0.000216699909645
P_3	0.000215873120110	0.000216706011731	0.000216699909645
P_4	0.000000046617499	0.000000046977992	0.000000046975344
P_5	0.000000038771234	0.000000042278284	0.000000045647180
P_6	0.000000085386789	0.000000089254340	0.000000092620573
P_7	0.000000038773659	0.000000042280896	0.000000045650024

We see that the algorithm produces consistent TFNs, an indication of a valid numerical procedure.

7.4 Inverse problem.

In order to perform the mathematical analysis, the example of a press brake introduced previously will be used. This problem statement will then lend itself to a mathematical representation as follows.

The cost function is composed of three components.

- the first reflects the cost of achieving a given level of reliability;
- the second part reflects the costs of accidents or failures which can still occur;
- The third part reflects the cost of repair.

Thus the cost function is chosen to be of the following general form:

$$\mathrm{CF} = \sum_1^n (\mathrm{c}_{\mathrm{pc_i}}(1 - \mu_{\mathrm{p}_{\lambda_{\mathrm{x_i}}}})^{\mathrm{kp_i}} + \mathrm{c}_{\mathrm{fc_i}}(\mu_{\mathrm{p}_{\lambda_{\mathrm{x_i}}}})^{\mathrm{kf_i}} + \mathrm{c}_{\mathrm{rc_i}}(1 - \mu_{\mathrm{p}_{\mu_{\mathrm{x_i}}}})^{\mathrm{km_i}}) \tag{7.5}$$

This expression reflects the fact that higher reliability (less accident) involves higher costs, hence the use of the factors (1-$\mu_{\mathrm{X_i}}$) which express reliability instead of just $\mu_{\mathrm{X_i}}$ which represent failure probabilities. The cost also increases with the probability of failures, accidents and repairs.

The coefficients μ_{C_i} depend on many factors such as:

- the cost of obtaining a certain component of required reliability varies with the supplier
- or, in the case of a human factor, it might vary with the person.
- and possibility of repair depends on the type of failure, whether it is repairable or not.

We will consider a quadratic cost function for calculation purposes.

7.4.1 Inverse optimization problem including device and human error and repair

The optimization problem for a system with device and human failures as well as repair (both device and human) will now be discussed. In this case, the optimization model v will take the following form:

Minimize the Cost Function:

$$c_1\mu_{\mathrm{p}_{\lambda_\mathrm{d}}}{}^2 + c_2\mu_{\mathrm{p}_{\lambda_\mathrm{h}}}{}^2 + c_3(1 - \mu_{\mathrm{p}_{\lambda_\mathrm{d}}})^2 + c_4(1 - \mu_{\mathrm{p}_{\lambda_\mathrm{h}}})^2 + c_5(\mu_{\mathrm{p}_{\mu_\mathrm{d}}})^2 + c_6(\mu_{\mathrm{p}_{\mu_\mathrm{h}}})^2 \tag{7.6}$$

where each μ_p term in the cost function represents a probability

$$\mu_{\mathrm{p}_{\lambda_\mathrm{d}}} = 1 - \mathrm{e}^{-\mu_{\lambda_d}\mathrm{t}}$$

$$\mu_{\mathrm{p}_{\lambda_\mathrm{h}}} = 1 - \mathrm{e}^{-\mu_{\lambda_\mathrm{h}}\mathrm{t}}$$

$$\mu_{\mathrm{p}_{\mu_\mathrm{d}}} = 1 - \mathrm{e}^{-\mu_{\mu_\mathrm{d}}\mathrm{t}}$$

$\mu_{p_{\mu_h}} = 1 - e^{-\mu_{\mu_h} t}$

t = 5000 h = the total time considered during operation of the press

The constraints are:

$$-\mu_{p_{\lambda_d}} \leq 0$$

$$-\mu_{p_{\lambda_h}} \leq 0$$

$$-\mu_{p_{\mu_d}} \leq 0$$

$$-\mu_{p_{\mu_h}} \leq 0$$

$$\mu_{p_{\lambda_d}} \leq 1$$

$$\mu_{p_{\lambda_h}} \leq 1$$

$$\mu_{p_{\mu_d}} \leq 1$$

$$\mu_{p_{\mu_h}} \leq 1$$

$$c \leq \mu_{SS}$$

The first four constraints reflect the fact the variables in question are probabilities, hence must have values between 0 and 1.

μ_{SS} represents a safety standard expressing a maximum tolerable probability of occurrence such as 1*10e-6.

c, on the other hand, is in fact not a variable, but actually a function which is the solution to the transition equation stemming from the Markov diagram representing the system. c was determined by solving the Markov equation as described above using the Symbolic function in Matlab. It takes an involved form which can be found in the Appendix.

7.4.1.1 Problem solution

The values of the coefficients[8] will be taken, purely for demonstration purposes as:

c_1=5000;

c_2=110;

c_3=6000;

c_4=200;

c_5=250;

c_6=50.

With time being t = 5000 h in the constraint, the failure rates (middle value of triangular fuzzy number representation) which minimize the cost are:

$\mu_{\lambda_d} = 0.000012115502753$

$\mu_{\lambda_h} = 0.000008762062477$

$\mu_{\mu_d} = 0.529628662131702$

$\mu_{\mu_h} = 0.202979628784727$

Cost function value = C.F. = $ 3098.24.

7.4.1.2 Discussion

The analysis shows that the optimal values to be reached for the failure rates are below the ones calculated from the Markov equations, which is reasonable. For instance, the middle value of the triangular fuzzy device failure rate was $3x10^{-5}$/h compared to the 1,2 $x10^{-5}$/h

[8] Shown without the units since their physical meaning is neither obvious or illuminating.

obtained through the optimization procedure. As for the human error rate, the Markov analysis yielded a rate of 1x10^{-5}/h as compared to 8,7x10^{-6} /h from the optimization calculations. Furthermore, the optimal value for the cost function implies that the human error rate should be reduced to a greater extent than the technical failure rate. The target value for human error rate determined by the analysis is substantially lower with respect to expert elicitation estimates and to values for human error found in the literature, such as, for example, in Smith (2005) who cites a general human failure rate for a plant of 20x10^{-6}/h . As for the device failure rate, according to one safety light curtain manufacturer (Rockwell automation), the dangerous failure rate or such devices range from 10^{-4} for low risk applications to 10^{-8} for higher risk applications. So, the value obtained here is within this range and thus seems reasonable.

Of course, the results depend strongly on the coefficients of the Cost Function which were chosen purely to illustrate the calculation method.

7.4.2 Inverse optimization problem including Human Failure and Repair and Redundancy

From the fault tree for the problem, the optimization model will take the following form Minimize the Cost Function:

$$\mathrm{C.F.} = \sum\nolimits_{i=1}^{12} \mathrm{CF_i}$$

$$= c_1(\mu_{p_{\lambda_{d_1}}})^2 + c_2(\mu_{p_{\lambda_{h_1}}})^2 + c_3\left(1 - \mu_{p_{\lambda_{d_1}}}\right)^2 + c_4\left(1 - \mu_{p_{\lambda_{h_1}}}\right)^2 + c_5(\mu_{p_{\mu_{d_1}}})^2 +$$
$$c_6(\mu_{p_{\mu_{h_1}}})^2 + c_7\,(\mu_{p_{\lambda_{d_2}}})^2 + c_8\,(\mu_{p_{\lambda_{h_2}}})^2 + +c_9\left(1 - \mu_{p_{\lambda_{d_2}}}\right)^2 + c_{10}(1 - \mu_{p_{\lambda_{h_2}}})^2 +$$
$$+c_{11}\,(\mu_{p_{\mu_{d_2}}})^2 + c_{12}\,(\mu_{p_{\mu_{h_2}}})^2$$

(7.7)

where each term containing the variable μ_p in the cost function represents a probability. The definition and meaning of these terms can be explained by taking a specific examples:

In a term such as $\mu_{p_{\lambda_{d_j}}}$, μ_p refers to the fact that this is a probability and it is a fuzzy number. λ shows that it refers to a failure rate. D refers to a device-related failure. j= 1, 2 corresponding to which of the two devices or operators is being considered. On the other hand, a term such as $\mu_{p_{\mu_{h_2}}}$ refers to the fuzzy repair rate of the human operator no. 2.

$$\mu_{p_{\lambda_{d_{1,2}}}} = 1 - e^{-\mu_{\lambda_{d_{1,2}}} t}$$

$$\mu_{p_{\lambda_{h_{1,2}}}} = 1 - e^{-\mu_{\lambda_{h_{1,2}}} t}$$

$$\mu_{p_{\mu_{d_{1,2}}}} = 1 - e^{-\mu_{\mu_{d_{1,2}}} t}$$

$$\mu_{p_{\mu_{h_{1,2}}}} = 1 - e^{-\mu_{\mu_{h_{1,2}}} t}$$

subject to the following constraints:

$$-\mu_{p_{\lambda_{d_{1,2}}}} \leq 0$$

$$-\mu_{p_{\lambda_{h_{1,2}}}} \leq 0$$

$$-\mu_{p_{\mu_{d_{1,2}}}} \leq 0$$

$$-\mu_{p_{\mu_{h_{1,2}}}} \leq 0$$

$$\mu_{p_{\lambda_{d_{1,2}}}} \leq 1$$

$$\mu_{p_{\lambda_{h_{1,2}}}} \leq 1$$

$$\mu_{p_{\mu_{d_{1,2}}}} \leq 1$$

$$\mu_{p_{\mu_{h_{1,2}}}} \leq 1$$

$$c \leq \mu_{SS}$$

Thus, the problem consists of 8 variables. It must be carefully noted however that the solution to the problem will yield the 8 failure rates associated with the problem, not the probabilities that are contained in the Cost Function definition.

The first eight constraints reflect the fact the variables in question are probabilities, hence must have values between 0 and 1. The last constraint μ_{SS} represents a safety standard expressing a maximum tolerable probability of occurrence such as 10^{-6}.

This constraint comes from the failed state of the Markov diagram associated with the system being analyzed. c is thus the function representing the probability of occurrence of the failed state of the system. This function is provided by the solution to the Markov matrix of the system for the final state. What needs to be provided in the fmincon routine is the function c in symbolic form. The Markov solution previously obtained yields numerical results. In order to obtain the form of the function, the Markov equation will be solved using the method of Lindhe et al. (2012).

The method consists of representing the original Markov diagram in the form previously solved having 3 states as shown in Figure 7.3 to the form appearing in the following Figure 7.4.

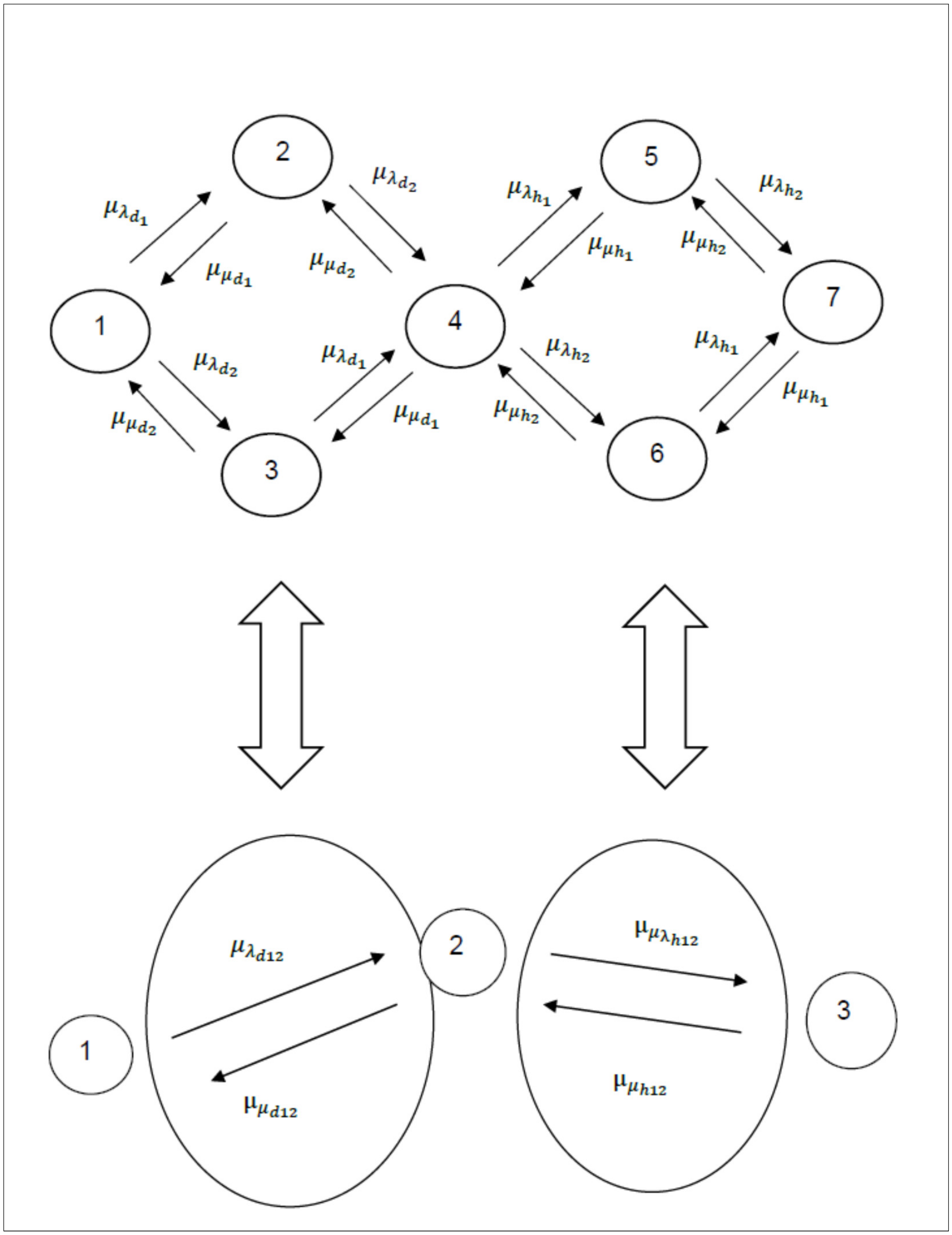

Figure 7.4 Diagram illustrating solution to redundancy, repair and human error problem

Lindhe et al. (2012) worked out the solutions:

$$\mu_{\lambda_{d_{12}}} = \left(\mu_{\mu_{d_1}} + \mu_{\mu_{d_2}}\right) * \frac{\mu_{\lambda_{d_1}} + \mu_{\lambda_{d_2}}}{\left(\mu_{\lambda_{d_1}} + \mu_{\mu_{d_1}}\right) * \left(\mu_{\lambda_{d_2}} + \mu_{\mu_{d_2}}\right) - \left(\mu_{\mu_{d_1}} * \mu_{\mu_{d_2}}\right)}$$

$$\mu_{\lambda_{d_{12}}} = \left(\mu_{\mu_{d_1}} + \mu_{\mu_{d_2}}\right) * \frac{\mu_{\lambda_{d_1}} + \mu_{\lambda_{d_2}}}{\left(\mu_{\lambda_{d_1}} + \mu_{\mu_{d_1}}\right) * \left(\mu_{\lambda_{d_2}} + \mu_{\mu_{d_2}}\right) - \left(\mu_{\mu_{d_1}} * \mu_{\mu_{d_2}}\right)}$$

$$\mu_{\mu_{d_{12}}} = \left(\mu_{\mu_{d_1}} + \mu_{\mu_{d_2}}\right)$$

$$\mu_{\mu_{h_{12}}} = \left(\mu_{\mu_{h_1}} + \mu_{\mu_{h_2}}\right)$$

The Markov matrix equation was solved using the dsolve function in Matlab in symbolic form. This output represents the Constraint Condition $c \leq 1*10^{-6}$ in the Matlab program which solves the Optimization problem which can be found in the Appendix.

The results provided by the program are the following (x(i) is the output variable from the Matlab program corresponding to the failure rate)

Table 7.3 Results for Case Study including Redundancy

x(i)	Failure rates (middle value of triangular fuzzy number)	Result (in units of /h)
x(1)	$\mu_{\lambda_{d_1}}$	0.000000698034807
x(2)	$\mu_{\lambda_{h_1}}$	0.302039049346000
x(3)	$\mu_{\mu_{d_1}}$	0.000000013928250
x(4)	$\mu_{\mu_{h_1}}$	0.807872718014522
x(5)	$\mu_{\lambda_{d_2}}$	0.944565180565187
x(6)	$\mu_{\lambda_{h_2}}$	0.000018904977641
x(7)	$\mu_{\mu_{d_2}}$	0.935254855012468
x(8)	$\mu_{\mu_{d_2}}$	0.732430521281764

The Cost Function value is calculated as \$ 999.18.

It can be seen that that the optimum solution is achieved by specifying a relatively low device failure rate (for both devices). The optimum human failure rate is higher than generally quoted values found in the literature. This constitutes a reasonably reachable goal in practice since requiring very low human error rate would mean finding very attentive, skilled and well-trained workers. Methods of achieving high human reliability are not well-researched and established. Thus the goal of finding an optimum safe work situation is easier to reach with high reliability technical components. This result is logical, since safety is assured by protective devices in the event of human failures, the very reason for protective devices in the first place.

The effect of the coefficient on the result can be seen by attempting to change, for example, the c_{10} coefficient (related to the human reliability of the operator) is changed from 500 to 200 (in units of \$). The results then become:

Table 7.4 Results when a coefficient is varied in the Cost Function

x(i)	Failure rates (middle value of triangular fuzzy number)	Result (in units of /h)
x(1)	$\mu_{\lambda_{d_1}}$	0.000000001899515
x(2)	$\mu_{\lambda_{h_1}}$	0.481771426912515
x(3)	$\mu_{\mu_{d_1}}$	0.480795627722111
x(4)	$\mu_{\mu_{h_1}}$	0.475341212218522
x(5)	$\mu_{\lambda_{d_2}}$	0.000000001831020
x(6)	$\mu_{\lambda_{h_2}}$	0.485393002122600
x(7)	$\mu_{\mu_{d_2}}$	0.548382508795762
x(8)	$\mu_{\mu_{d_2}}$	0.474693577395059

It is seen that the optimum solution now involves even lower device failure rates since lowering c_{10} means investing less in human reliability. Protective devices must then be highly reliable. The cost function value is, \$ 860.00, a value lower than in the previous instance. So, even though higher device reliability is demanded in the optimum situation, the increased level of safety achieved implies less costs related to accident and injury occurrences.

7.5 Conclusion

The safety of an industrial system consisting of a brake press operated by an operator was analysed using a Markov state diagram. The system featured redundancy not only in the form of two safety protective devices but also a form of human redundancy consisting of a second worker at the work station whose function was to watch and assist the operator in order to prevent human failures (errors). Repair was also considered in the analysis of the system. A repair rate concept for the human element was introduced. A mathematical model describing the system was developed and solved. Fuzzy values obtained from an expert elicitation process, as well as estimated crisp, non-fuzzy values were used to represent the variables involved.

Results show that the probability of reaching a failed system state where all redundant, technical and human, features fail is in the order of 10-8, below commonly accepted safety standards. The model contains however assumed values for many of the failure and repair rates. In the analysis of an actual system, the needed data can prove difficult to obtain and a well-structured elicitation process could be of great use.

Furthermore, in the second part of the analysis, a cost function describing the monetary costs of achieving a defined safety level was defined. An optimization model aiming at minimizing this cost subject to the constraints of the problem was set up and solved. The results show that the optimal solution lies with protective devices having very low failure rates. The required human failure rates were within accepted values commonly quoted in the literature.

CONCLUSION

In this thesis, the safety of industrial brake presses was studied. These machines are widely used in the manufacturing sector, in particular in small and medium sized establishments. They are often stand-alone type machine in the sense that they are not physically connected to other machines, operated by one operator, sometimes two. The person-machine interface is often an actuating foot pedal Most importantly, from the standpoint of this thesis, they present a pinch point hazard which can cause serious injury.

In relation to this problem, this thesis pursued two objectives:

1. Estimate the probability of occurrence of a given identified accident on an industrial brake press with the use of the following three concepts and techniques:
    a. Fault tree analysis
    b. Fuzzy numbers and logic
    c. Expert Elicitation
2. Optimize a monetary Cost Function based on the probabilities of the contributing events leading to the accident being considered under the constraint of meeting recognized acceptable probability of accidents.

Work accidents are the result of contributing factors which sequentially and/or concurrently occur. A methodology must be followed to allow a correct analysis. In this thesis, fault tree analysis was utilized to this end. Two types of fault trees were used. The first one was described as a static fault tree in the sense that the order in which contributing events add up to produce the accidental event does not vary with time. In other words, the time-sequence of event is immaterial. The second type of fault tree presented in this thesis is the so-called dynamic fault tree where the order in which contributing events occur does matter. Following the development of a dynamic fault tree, a Markov chain diagram was drawn up. This technique enables the representation of brake press operation as a system which transitions from one state to the other according to failure and repair rates. A matrix probability equation can be written and solved for the probability of occurrence of the states of the system including the final failed system state in which the work accident occurs.

The estimation of work accident probability can often be problematic in practice. This largely due to the fact that more quantitative estimates necessitate historical data that are not available or if so, not easily obtainable. As a consequence, estimates tend to be qualitative and subjective. A way to alleviate these difficulties is to resort to expert elicitation. This technique seeks to obtain subjective estimates of probabilities of events identified as being important factors in the generation of undesirable, adverse, accidental events. In this thesis, an expert elicitation method was followed and implemented in three companies where brake presses were being used. One company was a large (> 500 floor workers) manufacturing facility in the aeronautical industry, the second one a medium-sized (with around 200 floor employees) establishment where brake presses were used in the fabrication of metal cabinets which were components of the final product. The third was a small (with less than 50 employees in total) company where brake press was only occasional. Experts were selected in terms of brake press experience, level of education and training and actual job description. A questionnaire with brief but specific instructions and questions were handed to each participant. A verbal description of the probability of occurence of specifically described events was sought. The problem of the subjectivity of the answers was addressed by expressing the linguistic probability estimates obtained as triangular fuzzy numbers. These are triplets formed of real numbers, each of which is associated with a degree of membership to a set composed of the verbal assessments. The rules of fuzzy arithmetic were followed and the probability estimates were computed and expressed as a fuzzy number. Both static and dynamic cases were covered and fuzzy probability estimates computed for each.

These analyses were called forward problems referring to the fact that one starts with the basic contributing events in a fault tree (both static and dynamic) and proceeds towards the top event of the fault tree, i.e. the accident. In this thesis, a second problem, the inverse problem, was tackled. This consists in starting with the top event and imposing a condition on its occurrence probability. A monetary cost function related to the cost 1) of achieving a safe and reliable brake press operation; 2) of failures both human and equipment-related; and 3) of maintainability both human and equipment-related is defined. The optimization problem defined and solved in the thesis then is to calculated the failure probabilities of the related fault tree in order to minimize the cost function under the constraint that the top event must not exceed a given allowable probability of occurrence of accidents set by regulations or safety standards.

The objectives and methodology thus described were detailed in this thesis and the calculations performed accordingly Results were produced to illustrate the various methods. The question of the validity of the results were discussed in the thesis but remain a challenge. The difficulty resides in the nature of the subject itself. The calculations cannot easily be compared with an experiment where an accident is provoked. However, the methodology developed is in agreement with current research papers on the subject. The thesis has presented original contributions to knowledge in particular in regards to the subject studied, brake press safety, to the details provided in the expert elicitation process, the type of cost function developed and the optimization problem presented herein.

Contributions to knowledge

It is claimed that this thesis makes four main contributions to the literature:

1. Fuzzy static and dynamic Fault Tree Analysis is applied to evaluate the risk on safety aspects of an industrial machine of the brake press type, which is seldom treated in the literature. Fuzzy Markov diagram technique is applied in the dynamic problem which is also seldom done for these types of industrial machines.

2. The expert elicitation process used in this thesis is presented in detail and comes from actual field experience.

3. The inverse problem which presents a method of optimizing prevention costs based on a fault tree method described in this thesis is, to our knowledge, new to the literature.

4. Markov analysis is done on industrial systems which include human redundancy. The concept of human repair rate is a novel contribution to the literature in our opinion.

RECOMMANDATIONS

It is believed that this thesis can lead to valuable further research works such as the following:

1. Seek ways to validate the probability estimates presented in this work by comparing different methods among themselves.
2. Use IF-THEN fuzzy inference rules to estimate the fuzzy probability estimates. Compare with the results in this work.
3. Refine the expert elicitation process. Make a comparison between different elicitation approaches. Give participants more extensive training and background knowledge of the problem.
4. Seek and compile relevant historical failure data, both human and equipment-related.
5. Perform human reliability studies of brake press operation in conjunction with fuzzy methods.
6. Develop a cost function based on a combination of historical data and expert elicitation process with fuzzy methodology.
7. Perform a Markov analysis assuming a time-variable failure rate.

APPENDIX I

MATLAB PROGRAMS

STATIC CASE STUDY

PROGRAM fminconNoRepairPaper17032020

```
clc
clear all
A=[1 0 ;0 1 ;-1 0 ;0 -1]
b= [1;1;0;0]
x0=[.5*10^-6;.5*10^-6];
[x,fval]                                                                         =
fmincon(@CFNoRepairPaper17032020,x0,A,b,[],[],[],[],'simple_constraint_17032020')
digits(12)
 vpa(fval)
```

PROGRAM CFNoRepairPaper17032020

```
function f = CFNoRepairPaper(x)
c1=100;
c2=110;
c3=105;
c4=115;
f = c1*(1-x(1))^2+c2*(1-x(2))^2+c3*x(1)^2+c4*x(2)^2;
```

PROGRAM simple_constraint_17032020

```
function [c, ceq] = ConstraintStatic(x)
   c = [x(1)*x(2)-1*10^-6];
   ceq = [];
```

APPENDIX II

MATLAB PROGRAMS

DYNAMIC PROBLEM WITH REPAIR AND REDUNDANCY CASE STUDY

Inverse Problem

Case : Repair with redundancy

```
c=(lambda1*lambda2*exp(25000*(lambda1^2 - 2*lambda1*lambda2 + 2*lambda1*mu1 +
lambda2^2 + 2*lambda2*mu1 + mu1^2)^(1/2) - 25000*lambda2 - 25000*mu1 -
25000*lambda1)*(lambda1 + lambda2 + mu1 - 2*mu2 + (lambda1^2 - 2*lambda1*lambda2
+ 2*lambda1*mu1 + lambda2^2 + 2*lambda2*mu1 + mu1^2)^(1/2)))/((2*lambda1*mu2 -
2*lambda1*lambda2 + 2*lambda2*mu2 + 2*mu1*mu2 - 2*mu2^2)*(lambda1^2 -
2*lambda1*lambda2 + 2*lambda1*mu1 + lambda2^2 + 2*lambda2*mu1 + mu1^2)^(1/2)) -
(lambda1*lambda2*exp(-50000*mu2))/(lambda1*mu2 - lambda1*lambda2 + lambda2*mu2
+ mu1*mu2 - mu2^2) - (lambda1*lambda2*exp(- 25000*lambda1 - 25000*lambda2 -
25000*mu1 - 25000*(lambda1^2 - 2*lambda1*lambda2 + 2*lambda1*mu1 + lambda2^2 +
2*lambda2*mu1 + mu1^2)^(1/2))*(lambda1 + lambda2 + mu1 - 2*mu2 - (lambda1^2 -
2*lambda1*lambda2 + 2*lambda1*mu1 + lambda2^2 + 2*lambda2*mu1 +
mu1^2)^(1/2)))/((2*lambda1*mu2 - 2*lambda1*lambda2 + 2*lambda2*mu2 + 2*mu1*mu2 -
2*mu2^2)*(lambda1^2 - 2*lambda1*lambda2 + 2*lambda1*mu1 + lambda2^2 +
2*lambda2*mu1 + mu1^2)^(1/2))
```

where

lambda1 = μ_{λ_d}

lambda2 = μ_{λ_h}

mu1 = μ_{μ_d}

mu2 = μ_{μ_h}

MATLAB PROGRAMS

Repair19022020

```
clc
clear all
syms lambda1
syms lambda2
syms mu1
syms mu2
syms P1(t)
syms P2(t)
syms P3(t)
%syms t

P=[P1;P2;P3]
Q=[-lambda1,mu1,0;lambda1,-lambda2-mu1,mu2;0,lambda2,-mu2]
S = dsolve(diff(P) == Q*P,P(0)==[1;0;0])
```

Optimize_19022020

```
clc
clear all
format long
A=[-1 0 0 0;0 -1 0 0;0 0 -1 0;0 0 0 -1];
b= [0;0;0;0];

x0=[0.5*10^-5;0.5*10^-5;0.5;0.5];
[x,fval] = fmincon(@CF3_19022020,x0,A,b,[],[],[],[1 1 1 1],'CFIneq2')
 digits(12)
 vpa(fval)
```

```
function [c, ceq] = CFIneq2(x)
 lambda1=x(1);
 lambda2=x(2);
 mu1=x(3);
 mu2=x(4);
 t=50000
c=(lambda1*lambda2)/(lambda1*lambda2 + lambda1*mu2 + mu1*mu2) +
(lambda1*lambda2*exp(-(t*(lambda1 + lambda2 + mu1 + mu2 + (lambda1^2 -
2*lambda1*lambda2 + 2*lambda1*mu1 - 2*lambda1*mu2 + lambda2^2 + 2*lambda2*mu1
+ 2*lambda2*mu2 + mu1^2 - 2*mu1*mu2 + mu2^2)^(1/2)))/2)*(lambda1 + lambda2 + mu1
+ mu2 - (lambda1^2 - 2*lambda1*lambda2 + 2*lambda1*mu1 - 2*lambda1*mu2 +
lambda2^2 + 2*lambda2*mu1 + 2*lambda2*mu2 + mu1^2 - 2*mu1*mu2 +
mu2^2)^(1/2)))/(2*(lambda1*lambda2 + lambda1*mu2 + mu1*mu2)*(lambda1^2 -
2*lambda1*lambda2 + 2*lambda1*mu1 - 2*lambda1*mu2 + lambda2^2 + 2*lambda2*mu1
+ 2*lambda2*mu2 + mu1^2 - 2*mu1*mu2 + mu2^2)^(1/2)) - (lambda1*lambda2*exp(-
(t*(lambda1 + lambda2 + mu1 + mu2 - (lambda1^2 - 2*lambda1*lambda2 + 2*lambda1*mu1
- 2*lambda1*mu2 + lambda2^2 + 2*lambda2*mu1 + 2*lambda2*mu2 + mu1^2 - 2*mu1*mu2
+ mu2^2)^(1/2)))/2)*(lambda1 + lambda2 + mu1 + mu2 + (lambda1^2 - 2*lambda1*lambda2
+ 2*lambda1*mu1 - 2*lambda1*mu2 + lambda2^2 + 2*lambda2*mu1 + 2*lambda2*mu2 +
mu1^2 - 2*mu1*mu2 + mu2^2)^(1/2)))/(2*(lambda1*lambda2 + lambda1*mu2 +
mu1*mu2)*(lambda1^2 - 2*lambda1*lambda2 + 2*lambda1*mu1 - 2*lambda1*mu2 +
lambda2^2 + 2*lambda2*mu1 + 2*lambda2*mu2 + mu1^2 - 2*mu1*mu2 + mu2^2)^(1/2))-
1*10^-6;

ceq=[];

end


function f = CF3_19022020(x)
%x(i) are failure or repair rates

c1=5000;
c2=110;
c3=6000;
c4=200;
%c5=250000;
%c6=50;
c5=250;
```

```
c6=50;
k=1;

f = c1*(exp(-x(1)*50000))^2+c2*(exp(-x(2)*50000))^2+c3*(1-exp(-x(1)*50000))^2+c4*(1-exp(-x(2)*50000))^2+c5*(1-exp(-x(3)*50000))^2+c6*(1-exp(-x(4)*50000))^2;
```

MATLAB PROGRAM
INVERSE PROBLEM
REPAIR WITH REDUNDANCY
(Ref. Chapter 7)

A simple Matlab program implements this method:

```
%Program Markov24022020.m solves Markov diagram with Repair and Redundancy
%using Lindhe's method
clc
clear all
%syms lambdad1
%syms lambdad2
%syms lambdah1
%syms lambdah2
%syms mud1
%syms mud2
%syms muh1
%syms muh2
syms lambdad12
syms lambdah12
syms mud12
syms muh12
```

```
%lambdad12=(mud1+mud2)*(lambdad1*lambdad2)/((lambdad1+mud1)*(lambdad2+mud2)
-mud1*mud2);
%lambdah12=(muh1+muh2)*(lambdad1*lambdah2)/((lambdah1+muh1)*(lambdah2+muh2)
-mud1*mud2);
%mud12=mud1+mud2;
%muh12=muh1+muh2;
syms P1(t)
syms P2(t)
syms P3(t)
%syms t
P=[P1;P2;P3]
Q=[-lambdad12,mud12,0;lambdad12,-lambdah12-mud12,muh12;0,lambdah12,-muh12]
S = dsolve(diff(P) == Q*P,P(0)==[1;0;0])


c= (lambdad12*lambdah12)/(lambdad12*lambdah12 + lambdad12*muh12 + mud12*muh12)
+ (lambdad12*lambdah12*exp(-(t*(lambdad12 + lambdah12 + mud12 + muh12 +
(lambdad12^2 - 2*lambdad12*lambdah12 + 2*lambdad12*mud12 - 2*lambdad12*muh12 +
lambdah12^2 + 2*lambdah12*mud12 + 2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12
+ muh12^2)^(1/2)))/2)*(lambdad12 + lambdah12 + mud12 + muh12 - (lambdad12^2 -
2*lambdad12*lambdah12 + 2*lambdad12*mud12 - 2*lambdad12*muh12 + lambdah12^2 +
2*lambdah12*mud12 + 2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12 +
muh12^2)^(1/2)))/(2*(lambdad12*lambdah12 + lambdad12*muh12 +
mud12*muh12)*(lambdad12^2 - 2*lambdad12*lambdah12 + 2*lambdad12*mud12 -
2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 + 2*lambdah12*muh12 +
mud12^2 - 2*mud12*muh12 + muh12^2)^(1/2)) - (lambdad12*lambdah12*exp(-
(t*(lambdad12 + lambdah12 + mud12 + muh12 - (lambdad12^2 - 2*lambdad12*lambdah12 +
2*lambdad12*mud12 - 2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 +
2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12 + muh12^2)^(1/2)))/2)*(lambdad12 +
lambdah12 + mud12 + muh12 + (lambdad12^2 - 2*lambdad12*lambdah12 +
2*lambdad12*mud12 - 2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 +
2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12 +
muh12^2)^(1/2)))/(2*(lambdad12*lambdah12 + lambdad12*muh12 +
mud12*muh12)*(lambdad12^2 - 2*lambdad12*lambdah12 + 2*lambdad12*mud12 -
2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 + 2*lambdah12*muh12 +
mud12^2 - 2*mud12*muh12 + muh12^2)^(1/2))-1*10^-6
```

```
%Program Optimize_19022020
    %uses fmincon Matlab function to solve Problem with Redundancy
and Repair
clc
clear all
format long
A=[-1 0 0 0 0 0 0 0;0 -1 0 0 0 0 0 0;0 0 -1 0 0 0 0 0;0 0 0 -1 0 0 0 0;0 0 0 0 -1 0 0 0;0 0 0 0 0 -
1 0 0;0 0 0 0 0 0 -1 0;0 0 0 0 0 0 0 -1];
b= [0;0;0;0;0;0;0;0];
x0=[0.5*10^-5;0.5*10^-5;0.125;0.5;0.5*10^-5;0.5*10^-5;0.125;0.5];
[x,fval] = fmincon(@CF3_22022020,x0,A,b,[],[],[],[1 1 1 1 1 1 1 1],'CFIneq2_21022020')
digits(12)
vpa(fval)
```

The variables of the problem in Matlab notation are x(1) ,…, x(8)

The boundary conditions are contained in the matrix A and vector b.

x0 is the vector containing the initial values. These values were chosen to be close to the failure rates values estimated from the expert elicitation process and to the assumed repair rates assumed previously in the study.

This program calls two simple programs. The first one calculates the Cost Function:

```
function f = CF3_22022020(x)
%This is Cost Function for 7-state Markov equation
%Case with Redundancy (device and human)and Repair (device and human)
%x(i) are failure or repair rates
```

```
%x(1)=lamdad1;x(2)=lambdah1;x(3)=mud1;x(4)=muh1;x(5)=lambdad2;x(6)=lambdah2
%x(7)=mud2;x(8)=muh2
c1=5000;
c2=110;
c3=6000;
c4=200;
%c5=250000;
%c6=50;
c5=250;
c6=50;
c7=5500;
c8=150;
c9=6000;
c10=200;
c11=250;
c12=50;
f = c1*(1-exp(-x(1)*50000))^2+c2*(1-exp(-x(2)*50000))^2+c3*(1-exp(-
x(1)*50000))^2+c4*(exp(-x(2)*50000))^2+c5*(1-exp(-x(3)*50000))^2+c6*(1-exp(-
x(4)*50000))^2+c7*(1-exp(-x(5)*50000))^2+c8*(1-exp(-x(6)*50000))^2+c9*(1-exp(-
x(5)*50000))^2+c10*(exp(-x(6)*50000))^2+c11*(1-exp(-x(7)*50000))^2+c12*(1-exp(-
x(8)*50000))^2;
```

It can be seen that the chosen values (solely for the purpose of illustrating the proposed method) of the coefficients in the cost function program are the following:

```
c1=5000;
c2=110;
c3=6000;
c4=200;
c5=250;
c6=50;
```

```
c7=5500;
c8=150;
c9=6000;
c10=500;
c11=250;
c12=50
```

The second routine defines the constraint condition $c \leq 1*10^{-6}$. It takes the symbolic form of the constraint which serves as input to the fmincon function.

```
%This program defines the constraint condition from the Redundancy and Repair case.
%c is the symbolic equation which is output P3 in the program Markov24022020.m

function [c, ceq] = CFIneq2_21022020(x)
 lambdad1=x(1);
 lambdah1=x(2);
 mud1=x(3);
 muh1=x(4);
 lambdad2=x(5);
 lambdah2=x(6);
 mud2=x(7);
 muh2=x(8);
 lambdad12=(mud1+mud2)*(lambdad1*lambdad2)/((lambdad1+mud1)*(lambdad2+mud2)-
mud1*mud2);
 lambdah12=(muh1+muh2)*(lambdah1*lambdah2)/((lambdah1+muh1)*(lambdah2+muh2)-
muh1*muh2);
 mud12=mud1+mud2;
 muh12=muh1+muh2;
 t=50000
 %From program Markov24022020.m, variable P3
```

```
c= (lambdad12*lambdah12)/(lambdad12*lambdah12 + lambdad12*muh12 + mud12*muh12)
+ (lambdad12*lambdah12*exp(-(t*(lambdad12 + lambdah12 + mud12 + muh12 +
(lambdad12^2 - 2*lambdad12*lambdah12 + 2*lambdad12*mud12 - 2*lambdad12*muh12 +
lambdah12^2 + 2*lambdah12*mud12 + 2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12
+ muh12^2)^(1/2)))/2)*(lambdad12 + lambdah12 + mud12 + muh12 - (lambdad12^2 -
2*lambdad12*lambdah12 + 2*lambdad12*mud12 - 2*lambdad12*muh12 + lambdah12^2 +
2*lambdah12*mud12 + 2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12 +
muh12^2)^(1/2)))/(2*(lambdad12*lambdah12 + lambdad12*muh12 +
mud12*muh12)*(lambdad12^2 - 2*lambdad12*lambdah12 + 2*lambdad12*mud12 -
2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 + 2*lambdah12*muh12 +
mud12^2 - 2*mud12*muh12 + muh12^2)^(1/2)) - (lambdad12*lambdah12*exp(-
(t*(lambdad12 + lambdah12 + mud12 + muh12 - (lambdad12^2 - 2*lambdad12*lambdah12 +
2*lambdad12*mud12 - 2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 +
2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12 + muh12^2)^(1/2)))/2)*(lambdad12 +
lambdah12 + mud12 + muh12 + (lambdad12^2 - 2*lambdad12*lambdah12 +
2*lambdad12*mud12 - 2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 +
2*lambdah12*muh12 + mud12^2 - 2*mud12*muh12 +
muh12^2)^(1/2)))/(2*(lambdad12*lambdah12 + lambdad12*muh12 +
mud12*muh12)*(lambdad12^2 - 2*lambdad12*lambdah12 + 2*lambdad12*mud12 -
2*lambdad12*muh12 + lambdah12^2 + 2*lambdah12*mud12 + 2*lambdah12*muh12 +
mud12^2 - 2*mud12*muh12 + muh12^2)^(1/2))-1*10^-6

ceq=[];
```

BIBLIOGRAPHY

Acosta & al. (2010) Fuzzy experts on recreational vessels, a risk modelling approach for marine invasions. Ecological Modelling 221 (5) : 850-86

Adamyan, A. , He, D. (2002) *Analysis of sequential failures for assessment of reliability and safety of manufacturing systems*. Reliability Engineering and System Safety, Vol. 76() : 227-236.

Aggarwal, K.K. (1993) Reliability Engineering. Springer-Science+Business Media, B.V.

Agarwal, P. and H.S. Nayal (2015) Possibility Theory versus Probability Theory in Fuzzy Measure Theory. Int. Journal of Engineering Research and Applications, Vol. 5, Issue 5, (Part -2), pp.37-43

Ale, B., D.N.D. Hartford, D. Slater (2015) "ALARP and CBA all in the same game." Safety Science 76: 90–100

Amari S., Dill G., Howard E., 2003 A new approach to solve dynamic fault trees. In: *Annual IEEE reliability and maintainability symposium*,. p. 374–9

Andrews, J.D., Moss, T.R. (2002) Reliability and risk assessment New York: ASME Press.

Anonymous (2009) "Méthode Kinney, déjà dépassée?" Prevent Focus, No.1, p. 4-7.

ANSI B11-TR3, (2000) *Risk* Assessment and Risk Reduction – A Guide to Estimate, Evaluate and Reduce Risk Associated with Machine Tools. American National Standards Institute.

Apeland S., Aven, T ; Nilsen, T (2002) "Quantifying uncertainty under a predictive, epistemic approach to risk analysis." Reliability Engineering and System Safety, Vol.75(1), :93-102

Aubert, B. A. & Bernard, J. G. (2004) Mesure intégrée du risque dans les organisations. Montréal, Les Presses de l'Université de Montréal.

Aven T., Y. Hiriart, (2013) Robust optimization in relation to a basic safety investment model with imprecise probabilities. Safety Science 55() :188–194

Aven, T. (2011) Interpretations of alternative uncertainty representations in a reliability and risk analysis context. Reliability Engineering and System Safety 96 353–360

Bahr, N. (1997) *System safety engineering and risk assessment: a practical approach*. Washington, DC : Taylor & Francis.

Bezdek, J.C. (1993) Fuzzy models-What are they, and why? [Editorial]. IEEE Transactions on Fuzzy Systems, Vol.1(1) :1-6.

Bley, D. et al. (1992) *The strengths and limitations of PSA: where we stand*. Reliability Engineering and System Safety, Vol. 38(1) : 3-26.

Boothroyd, G. et al. (2002) Product Design for Manufacture and Assembly. New York: Marcel Dekker.

Bralla, J. (1996) *Design for excellence*. New York: McGraw-Hill.

Bobbio L., Portinale M., Minicchino E., Ciancanerla D. (2001) Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety 71 :249–260

Buckley J.J., Eslami E 2008 Fuzzy Markov Chains: Uncertain Probabilities. Mathware & Soft Computing, 9(1).

Chen, Z.,Wu,X., Qin, J. (2014) Risk assessment of an oxygen-enhanced combustor using a structural model based on the FMEA and fuzzy fault tree. Journal of Loss Prevention in the Process Industries 32 :349-357

Chinniah, Y. (2015) Analysis and prevention of serious and fatal accidents related to moving parts of machinery. Safety Science 75 :163–173

Chinniah, Y. & Poisson, P. (2015) Observation and analysis of 57 lockout procedures applied to machinery in 8 sawmills. Safety Science 72() :160–171

Cicek K, Cicek M. (2013) Application of failure modes and effects analysis to main engine crankcase explosion failure on-board ship, Safety Science 51 : 6-10.

Clarke, D.M. (2005) Human redundancy in complex, hazardous systems: A theoretical framework. Safety Science 43(9) : 655-677

CNESST (2008) *Dix machines dangereuses.* Prévention au travail. Numéro Automne. pp. 33-37.

CSA Z432 (2016) Safeguarding of machinery Canadian Standards Association (CSA).

CSA Z1002 (2012) Occupational health and safety : hazard identification and elimination and risk assessement and control. Canadian Standards Association (CSA).

Dadone, P. (2001) “Design Optimization of Fuzzy Logic Systems.” PhD thesis. Virginia Polytechnic Institute and State University. USA.

Dhillon, B.S. (1986) Mechanical reliability : theory, models, and applications Washington, D.C. : American Institute of Aeronautics and Astronautics.

Dhillon, B.S. and N. Yang (1995) Probabilistic analysis of a maintainable system with human error. Journal of Quality in Maintenance Engineering, 1(2) :50-59.

Dolas, D.R., M.D. Jaybhaye., S.D.Deshmukh, (2014) Prediction of Repair & Maintenance Costs of Diesel Engine. International Journal of Recent advances in Mechanical Engineering (IJMECH) 3(1).

Dougherty, E. (1994) *On merging system safety and quantitative risk assessment*. Reliability Engineering and System Safety76(): 227-236.

Dugan J.B., Bavuso M., Boyd M., (1990) Fault Trees and Sequence Dependencies. Proc. Ann. Reliability & Maintainability Symp., Jan: 286-293.

Dunbar, L.C. (1984) A mathematical expression describing the failure probability of a system of redundant components with finite maximum repair time. Reliability Engineering, 1984, Vol.7(3):169-179

Ericson, C.A. (2005) Hazard Analysis Techniques for System Safety. New-York: Wiley

Feng, Y. (2015) Mathematical Models for Determining the Minimum Level of Voluntary Safety Investments for Building Projects. J. Constr. Eng. Manage., 141(7) : 04015015

Fera, M., R. Macchiaroli (2010) Appraisal of a new risk assessment model for SME. Safety Science 8(10):1361-1368.

Ferraro, D.O. (2009) Fuzzy knowledge-based model for soil condition assessment in Argentinean cropping systems. Environmental Modelling & Software 24 :359–370

Flaus, J.-M (2013) Risk Analysis Socio-technical and Industrial Systems. Hoboken NJ Wiley

Gagné, N. (2004) La sécurité des cardes : identification des risques et exploration des possibilités d'amélioration. IRSST.

Gani A.D., (2012) A new operation on triangular fuzzy numbers for solving fuzzy linear programming problems, Applied Mathematical Sciences 6 (11): 525-532

Gauthier, F. (1997) Développement d'une approche méthodologique permettant l'intégration systématique des aspects de la santé et de la sécurité du travail dans le processus de conception d'outils, de machines et de procédés industriels. Thèse de doctorat. Université de Sherbrooke.

Gauthier, F. (2004) Développement d'un outil d'évaluation des mesures de retenue des camions aux quais de transbordement. IRSST

Gierczak,M. (2014) The qualitative risk assessment of MINI, MIDI and MAXI horizontal directional drilling projects. Tunnelling and Underground Space Technology incorporating Trenchless Technology Research, 44:148-156.

Giraud, L. et al. (2003) Sécurité des convoyeurs à courroie : généralités, protection contre les phénomènes dangereux : guide de l'utilisateur. CSST.

Giraud, L. (2004) Belt conveyor safety: understanding the hazards. Professional Safety, 49, (11): 20-26.

Government of Québec *An act respecting occupational health and safety* Chapter S-2.1

Guikema,S. D. & M.E. Paté-Cornell (2002) Component choice for managing risk in engineered systems with generalized risk/cost functions. Reliability Engineering and System Safety 78(3):227-238.

Gurcanli, G.E. and U. Mungen, (2009) An occupational safety risk analysis method at construction sites using fuzzy sets International Journal of Industrial Ergonomics 39(2):371-387.

Haffner, S. (2002) Cost Modeling and Design for Manufacturing Guidelines for Advanced Composites Fabrication. Ph.D.Thesis . Massachusetts Institute of Technology.

Hollnagel, E. (2000) Looking for errors of omission and commission or The Hunting of the Snark revisited. Reliability Engineering and System Safety,68 (2:135-145

Holywell, P. 1996 Incorporating human dependent failures in risk assessments to improve estimates of actual risk. Safety Science, 22(1-3) : 177-194.

Horlick-Jones, T. (1998) Meaning and contextualisation in risk assessment. Reliability Engineering and System Safety, 59(1): 79-89.

INERIS 2001 Outils d’aide à la décision pour la gestion des crises (DRA-04).

ISO 12100 2003 Safety of machinery -- Basic concepts, general principles for design.

ISO/TR 14121-2. 2012. Safety of Machinery – Principles of Risk Assessment. Geneva: International Organization for Standardization (ISO).

Jefarian, E., Rezvani, M.A. (2012) Application of fuzzy fault tree analysis for evaluation of railway safety risks: an evaluation of root causes for passenger train derailment. Proc. IMechE Vol. 226 Part F: J. Rail and Rapid Transit:14-25.

Jiang, B. C., O.S.H., Cheng, (1990) A procedure analysis for robot system safety. Int. J. of Industrial Ergonomics, 6 :95-117.

Johnson, C.W. (1996*)* Integrating human factors and systems engineering to reduce the risk of operator «error». *Safety Science* 22(1-3) :195-194.

Kaplan, S. (1997) The words of risk *Risk Analysis* 17 (4): 407-417.

Kaplan, S, & B.J. Garrick (1983) On the quantitative definition of risk. *Risk Analysis* 1(1) : 1-28.

Kariuki, S.G. & K. Löwe (2007) Integrating human factors into process hazard analysis. Reliability Engineering and System Safety 92:1764–1773

Kirwan, B. (1994) A guide to practical human reliability assessment. Bristol, PA: Taylor & Francis.

Kontogiannis, T. (2000) A comparaison of accident analysis techniques for safety-critical man-machine systems. *Int. J. of Industrial Ergonomics*, Vol. 25, p. 327-347.

Krüger, J., T.K. Lien, D.W. Verl (2009) *Cooperation of humans and machines on assembly lines*. CIRP Annals Manufacturing technology, Vol. 58, p. 628-646.

Klir, J. & B. Parviz, (1992) Probability–possibility transformations: a comparison. *International Journal of General Systems* 21 (3): 291–310.

Knol A.B., J. de Hartog, H. Boogaard, P. Slottje, ,J.P. van der Sluijs, E. Lebret, R. Cassee, J. Wardekker, J.G. Ayres, P.J. Borm, B. Brunekreef, K. Donaldson, F. Forastiere, S.T. Holgate, W.G. Kreyling, B. Nemery, J. Pekkanen, V. Stone, H. Wichmann and G. Hoek (2009) Expert elicitation on ultrafine particles: likelihood of health effects and causal pathways**.** *Particle and Fibre Toxicology*, 6, p.19-19

Knol, A.B., P. Slottje, J. P van der Sluijs, and E. Lebret (2010) The use of expert elicitation in environmental health impact assessment: a seven step procedure. *Environmental Health*, 9:19

Komal (2015) Fuzzy fault tree analysis for patient safety risk modeling in healthcare under uncertainty, *Applied Soft Computing* 37: 942-951

Kruger, T. (2012) The role of expert opinion in environmental modelling. *Environmental Modelling & Software* 36: 4-18.

Kumamoto, H., E.J. Henley (1996) Probabilistic Risk Assessment and Management for Engineers and Scientists. New York: IEEE Press.

Lavasini, S.M., A. Zendegania,, M. Celik (2015) An extension to Fuzzy Fault Tree Analysis (FFTA) application in petrochemical process industry. *Process Safety and Environmental Protection* 93 75–88.

Lavasini, S.M., A. Zendegania,, M. Celik (2014) Utilisation of Fuzzy Fault Tree Analysis (FFTA) for quantified risk analysis of leakage in abandoned oil and natural-gas wells, *Ocean Engineering*, 108: 729-737

Lei, X. & C.A. MacKenzie (2019) Assessing risk in different types of supply chains with a dynamic fault tree. *Computers & Industrial Engineering* 137: 106061

Lewis, E.E. (1996) Introduction to reliability engineering. New York, N.Y. : J. Wiley and Sons

Liu, P., L.Yang, Z. Gao, S. Li, Y.Gao (2015) Fault tree analysis combined with quantitative analysis for high-speed railway accidents. *Safety Science* 79 :344 -357

Li YF, Huang HZ, Liu Y, Xiao N, Li H. (2012) A new fault tree analysis method: fuzzy dynamic fault tree analysis. Eksploatacja i Niezawodnosc – Maintenance and Reliability 14 (3): 208-214.

Lindhe, A., T. Norberg, L. Rosen Approximate dynamic fault tree calculations for modelling water supply risks. Reliability Engineering and System Safety 106(10): 61-71

Main, B. (2002) Risk assessment is coming: are you ready? *Professional Safety*, 47(7):32-37.

Mahmood Y. A.,A. Ahmadi, A. K. Verma, A. Srividya, U. Kumar (2013) Fuzzy fault tree analysis: a review of concept and application. *Int J Syst Assur Eng Manag* 4(1):19–32

Markowski, A., M.S. Mannan. Fuzzy risk matrix. J. of Hazardous Materials 159 (2008) 152–157.

Markowski, A. et al. Fuzzy logic for piping risk assessment (pfLOPA) J. of Loss Prevention in the Process Industries 22 (2009) 921–927.

Markowski, A.S. (2010) Uncertainty aspects in process safety analysis. *Journal of Loss Prevention in the Process Industries* 23:446-454.

Markowski, A. S. (2011) Application of fuzzy logic to explosion risk assessment. *Journal of Loss Prevention in the Process Industries* 24:780-790.

Marszal, E., Scharpf, E. (2002) Safety Integrity Level Selection. Research Triangle Park, N.C.: I.S.A

Mechri, W. Simon, Ch. Ben Othman, K. and M. Benrejeb, (2011) Uncertainty evaluation of Safety Instrumented Systems by using Markov chains. 18th IFAC World Congress Milano (Italy) August 28 - September 2, 2011.

Melchers, R.E. & Feutrill, W.R. (2001) Risk assessment of LPG automotive refueling facilities *Reliability and System Safety* 74:283-290

Mentes, A. and I.H. Helvacioglu (2011) An application of fuzzy fault tree analysis for spread mooring systems. *Ocean Engineering* 38:285–294

Moon, J.H., C.S. Kang (1999) Use of fuzzy set theory in the aggregation of expert judgments. *Annals of Nuclear Energy* 26 :461-469

Modarres, M. (2006) Risk Analysis in Engineering. Techniques, Tools, and Trends. Boca Raton: CRC Press. Taylor and Francis.

Montmayeul, R., Mosneron-Dupin, F. (1994) The managerial dilemma between the prescribed task and the real activity of operators: Some trends for research on human factors. *Reliability Engineering and System Safety*, 45: 67-73.

Moriyama, T., H. Ohtani, (2009) Risk assessment tools incorporating human error probabilities in the Japanese small-sized establishment. *Safety Science*, Vol. 47(10):. 1379-1397.

Murata, T. (1989) Petri nets: Properties, Analysis and Applications. *Proceedings of the IEEE*, 77(4):.541-580.

Neoh, E.T. (1995) Adaptive framework for estimating fabrication times. Ph.D.Thesis . Massachusetts Institute of Technology.

Nivon, M. (undated) Sécurité dans la transformation des plastiques. Techniques de l'ingénieur.

Nascimento C.S., R.N. de Mesquita (2012) Human reliability analysis data obtainment through fuzzy logic in nuclear plants. Nuclear Engineering and Design, Vol.250, pp.671-677

Omidvarin, M., Lavasini S.M.R., Mirza S., (2014) Presenting of failure probability assessment pattern by FTA in Fuzzy logic (case study: Distillation tower unit of oilrefinery process) *Journal of Chemical Health & Safety*, November/December .

Onisawa, T. 1988 Subjective analysis of system reliability and its analyzer. *Fuzzy Sets and Systems* 83(2): 249-269

Page, L.B. & V.E. Perry (1994) Standard Deviation As an Alternative to Fuzziness in Fault Tree Models. *IEEE Transactions On Reliability*, 43(3):402-407.

Page, T., A.L. Heathwaite, L.J. Thompson, L. Pope, R. Willows (2012) Eliciting fuzzy distributions from experts for ranking conceptual risk model components. *Environmental Modelling & Software* 36 : 19-34.

Pâques, J-J., Bourbonnière, R. (2002) Appréciation et réduction des risques. Guide de formation. IRSST.

Pérès, F., D. Noyes (2003) Evaluation of a maintenance strategy by the analysis of the rate of repair. Quality and Reliability Engineering International. 19(2):129-148

Poli, C. (2001) Design for Manufacturing : a Structured Approach. Boston: Butterworth–Heinemann.

Pyy, P., B. Wahlstrom, (1988) Modelling the human in PSA studies. *Reliability Engineering and System Safety*, Vol. 22(1-4): 277-294.

Purba, J.H., Tjahyani, A.S.Ekariansyah, H. Tjahjono (2014) A fuzzy reliability assessment of basic events of fault trees through qualitative data processing, *Fuzzy Sets and Systems* 243: 50-69

Purba, J.H., D.T. Tjahyani, A.S.Ekariansyah, H. Tjahjono (2015) Fuzzy probability based fault tree analysis to propagate and quantify epistemic uncertainty. *Annals of Nuclear Energy* 85: 1189-1199

Rajakarunakaran, S., Kumar, M., Prabhu, V.A. (2015) Applications of fuzzy faulty tree analysis and expert elicitation for evaluation of risks in LPG refuelling station. *Journal of Loss Prevention in the Process Industries* 33: 109-123

Ramzali N., M. R. M. Lavasani, J. Ghodousi (2015) Safety barriers analysis of offshore drilling system by employing Fuzzy Event Tree Analysis. *Safety Science*. 78: 49-59

Raafat, H.M.N. (1989) Risk assessment and machinery safety. Journal of occupational accidents, 11(1): 37-50.

Rasmussen, J. (1983) Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance model. IEEE Transactions on Systems, Man, and Cybernetics. Vol.SMC-13(3): 257-266

Rausand, M. (2011) Risk Assessment. New-York:Wiley.

Reason, J. (1990) Human error. Cambridge University Press. Cambridge.

Renjith V.R., G. Madhu, V. Nayagam, A. H. Bhasi, (2010) Two-dimensional fuzzy fault tree analysis for chlorine release from a chlor-alkali industry using expert elicitation. *Journal of Hazardous Materials* 183: 103–110.

Rhee, S.J., K. Ishii (2003) Using cost based FMEA to enhance reliability and serviceability. Advanced Engineering Informatics. 17(3) : 179-188

Rogers, F., J. Younbae, (2009) Fuzzy nonlinear optimization for the linear fuzzy real number system. *International Mathematical Forum* 4 (12): 587-596

Ridley J., R. Pearce (2006) Safety with machinery. Amsterdam; Boston; London: Butterworth-Heinemann.

Ruckart, P.Z., Burgess, P.A. (2007) Human error and time of occurrence in hazardous material events in mining and manufacturing. Journal of Hazardous Materials. 142(3): 747-75

Sabir, S. & Papadopoulos, Y. (2018) A review of applications of fuzzy sets to safety and reliability engineering. *International Journal of Approximate Reasoning* 100:.29–55.

Sa'idi, E., B. Anvaripour, F.Jaderi N. Nabhani (2014) Fuzzy risk modeling of process operations in the oil and gas refineries. *Journal of Loss Prevention in the Process Industries* 30: 63-73.

Sadiq,R, E. Saint-Martin, Y. Kleiner (2008) Predicting risk of water quality failures in distribution networks under uncertainties using fault-tree analysis. *Urban Water Journal* 5(4): 287–304.

Sharma,R.K., P. Sharma (2010). System failure behavior and maintenance decision making using, RCA, FMEA and FM. Journal of Quality in Maintenance Engineering, vol. 16 (1) pp.64-88.

Smith, D.J. (2011) Reliability, maintainability, and risk practical methods for engineers.8th edition. Amsterdam; Boston : Butterworth-Heinemann/Elsevier

Stanton, N., C. Baber, (1996) A systems approach to human error identification Safety Science, 22(1-3): 195-194.

Starr, C. (1969) Social Benefits versus Technological Risks. *Science*, 165(3899): 1232–1238.

Suresh, P.V., A.K. Babur, V. Raj (1996) Uncertainty in fault tree analysis: A fuzzy approach. *Fuzzy Sets and Systems* 83: 135-141.

Tyagi S.K., D. Pandey D., V Kumar., (2011) Fuzzy Fault Tree Analysis for Fault Diagnosis of in *Power Transformer Applied Mathematics* 2:1346-1355

Venditti, T, Tran, N.P.D, Ngô, A.D., 2017 Dynamic Fuzzy Safety Analysis of An Industrial System 2017 8th International Conference on Applied Human Factors and Ergonomics (AHFE) Los Angeles, California, USA July 19th to 21st

Venditti, T, Tran, N.P.D, Ngô, A.D., 2018 Expert elicitation methodology in the risk analysis of an industrial machine 9th International Conference on Applied Human Factors and Ergonomics (AHFE) Orlando, Florida, USA July 21st to 25th 2018.

Venditti, T, Tran, N.P.D, Ngô, A.D., 2018b System Safety Analysis of an Industrial Process Using Fuzzy Methodology 4th International Conference on Fuzzy Systems and Data Mining (FSDM2018) , Bangkok, Thailand November 16-19, 2018

Vernez, D. et al. (2000) Perspectives on the use of coloured Petri nets for risk analysis and accident modelling. *Safety Science*, 41 : 445-463.

Villemeur, A. (1988) Sûreté de fonctionnement des systèmes industriels. Fiabilité - facteurs humains – Informatisation. Paris : Eyrolles.

Wang, Y., Y. Jia, J. Yu, Y. Zheng, S. Yi (1999) Failure probabilistic model of CNC lathes. *Reliability Engineering and System Safety*, 65: 307-314.

Wang D., Zhang P., Chen, C. (2013) Fuzzy fault tree analysis for fire and explosion of crude oil tanks. *Journal of Loss Prevention in the Process Industries* 26: 1390-1398

Winnick, J. (1997) Chemical Engineering Thermodynamics. New York: Wiley.

Whiteley, M. et al .(2016) Failure Mode and Effect Analysis, and Fault Tree Analysis of Polymer Electolytic Membrane Fuel Cells, *International Journal of Hydrogen Energy* 41(2), pp.1187-1202

Yiu, T.W. (2015) Fuzzy Fault Tree Framework of Construction Dispute Negotiation Failure, *IEEE Transactions on Engineering Management*, May 2015, Vol.62(2):171-183

Yunus E. S. et al. (2015) Fault Tree Analysis of chemical cargo contamination by using fuzzy Approach, *Expert Systems with Applications* 42: 5233-5244

Zhang L., Kecojevic, V., Komljenovic, D. (2014) Investigation of haul truck-related fatal accidents in surface mining. using fault tree analysis *Safety Science* 65: 106–117

Zhang L., Skibnrewski M.J., Wu X., Chen Y., Deng Q., (2014) A probabilistic approach for safety risk analysis in metro construction. *Safety Science* 63: 8–17

Yuhua, D. et Datao, Y. (2005) Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis. *Journal of Loss Prevention in the Process Industries*, , Vol.18(2): 83-88

Zadeh, L. A. 1965 Fuzzy sets. *Information and Control*, 8: 338-353.