COPPE

Instituto Alberto Luiz Coimbra de
Pós-Graduação e Pesquisa de Engenharia

UFRJ

QUANTITATIVE RISK ASSESSMENT USING MONTE CARLO AND DYNAMIC PROCESS SIMULATION

Rafael Raoni Lopes de Britto

Tese de Doutorado apresentada ao Programa de Pós-graduação em Engenharia Química, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Doutor em Engenharia Química.

Orientador: Argimiro Resende Secchi

Rio de Janeiro
Fevereiro de 2018

QUANTITATIVE RISK ASSESSMENT USING MONTE CARLO AND DYNAMIC PROCESS SIMULATION

Rafael Raoni Lopes de Britto

TESE SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA (COPPE) DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM ENGENHARIA QUÍMICA.

Examinada por:

Prof. Argimiro Resende Secchi, D.Sc.

Prof. Paulo Fernando Ferreira Frutuoso e Melo, D.Sc.

Prof. Tito Lívio Moitinho Alves, D.Sc.

Prof. André Luiz Hemerly Costa, D.Sc.

Prof. Carlos André Vaz Junior, D.Sc.

RIO DE JANEIRO, RJ - BRASIL
FEVEREIRO DE 2018

Raoni, Rafael Lopes de Britto.

Quantitative Risk Assessment Using Monte Carlo and Dynamic Process Simulation/ Rafael Raoni Lopes de Britto. – Rio de Janeiro: UFRJ/COPPE, 2018.

XIII, 195 p.: il.; 29,7 cm.

Orientador: Argimiro Resende Secchi.

Tese (Doutorado) – UFRJ/COPPE/Programa de Engenharia Química, 2018.

Referências Bibliográficas: p. 9-11; 38-41; 68-70; 105-108; 135-139.

1. Desvios de processo. 2. Análise quantitativa de riscos. 3. Conceito de risco. 4. Simulação dinâmica de processo. 5. Simulação de Monte Carlo. I. Secchi, Argimiro Resende II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Química. III. Título.

Agradecimentos

Ao meu filho Cezar pela motivação.
À minha esposa Ingrid pelo companheirismo.
Ao meu orientador professor Argimiro pela paciência.

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

AVALIAÇÃO QUANTITATIVA DE RISCO USANDO MONTE CARLO E SIMULAÇÃO DE PROCESSOS DINÂMICOS

Rafael Raoni Lopes de Britto

Fevereiro/2018

Orientador: Argimiro Resende Secchi

Programa: Engenharia Química

Atualmente, a preocupação com o risco industrial é um ponto chave para implantação de uma nova tecnologia ou para um melhor posicionamento competitivo. Neste sentido, a ideia de risco pode ser considerada como o principal recurso para antever situações que podem gerar problemas futuros. Considerando a indústria de processos, diferentes técnicas de análise de riscos são utilizadas para identificar eventos perigosos, estimar suas frequências e severidades e caracterizar o risco, sendo essas as principais ferramentas para o aumento da segurança industrial. Sabendo disso, a presente tese aborda tais tópicos e propõe quatro contribuições principais: (i) novo procedimento para identificação de eventos perigosos; (ii) novos procedimentos para quantificação de frequência; (iii) nova definição e representação de risco e (iv) um método para integrar os procedimentos propostos em uma avaliação quantitativa de risco completa. A ideia por trás destas contribuições é utilizar procedimentos computacionais que geram resultados mais acurados sobre o risco de uma operação, ajudando em seu entendimento e na obtenção de seu valor. Assim, baseado em um novo conceito de risco que melhor relaciona as análises desenvolvidas, simulações de processos são utilizadas para identificação de eventos perigosos e simulações de Monte Carlo são utilizadas para estimativa de frequência e gerar uma nova representação de risco caracterizada por uma superfície com eixos *frequência x severidade x tempo*. Apesar de cada contribuição ter sua particularidade e importância para o desenvolvimento das técnicas de análise de risco, como contribuição final, a presente tese aplica todas as técnicas desenvolvidas em um estudo de caso, apresentando assim uma avaliação de risco inovadora.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Doctor of Science (D.Sc.)

QUANTITATIVE RISK ASSESSMENT USING MONTE CARLO AND DYNAMIC PROCESS SIMULATION

Rafael Raoni Lopes de Britto

February/2018

Advisor: Argimiro Resende Secchi

Department: Chemical Engineering

Currently, the concern about the industrial risk is a key issue to implement any technology process or to improve the industry competitiveness. In this sense, the risk concept may be considered as the main tool to anticipate behaviors that can lead to further problems. Considering the process industry, different risk analysis techniques are employed to identify hazardous events, to estimate their frequencies and severities, and to characterize the risk, being such tools the best ones to improve the industrial safety. Knowing that, the present Thesis discusses these risk topics to propose four main contributions: (i) new procedure to identify hazardous events; (ii) new procedures to quantify frequency; (iii) new risk definition and representation; and (iv) a method to integrate the proposed procedures to manage a complete risk assessment management. The idea behind the contributions is to use computational tools in new techniques with improved results about the operational risk, helping its obtainment and understanding. Thus, based on a new risk definition that allow better relation between the developed analysis, process simulations are employed to identify hazardous events and Monte Carlo simulations are employed to estimate frequency and to generate a new risk representation characterized by a *severity x time x frequency* surface. Despite all contributions has its particularity and importance for the risk analyses development, as final contribution, the presented Thesis apply all developed techniques in a case study, proposing an innovative risk assessment procedure.

SUMMARY

LIST OF FIGURES

CHAPTER II - HAZARD IDENTIFICATION...........12 Erro! Indicador não definido.

CHAPTER III - LIKELIHOOD ESTIMATION 42

CHAPTER IV - RISK CONCEPT AND REPRESENTATION............................. 82

CHAPTER V - COMPLETE QUANTITATIVE RISK ASSESSMENT CASE STUDY.......Erro! Indicador não definido.

LIST OF TABLES

LIST OF ABBREVIATIONS

ALARP - As Low As Reasonably Practicable

BSW - Basic Sediments and Water

CDF - Cumulative Distribution Function

DFT - Dynamical Fault Tree

DRBD - Dynamic Reliability Block Diagram

E - Identified event(s)

EMSO - Environment for Modeling, Simulation, and Optimization

ET - Event Tree

F - Frequency of the event occurrence

FMEA - Failure mode and effect analysis

FT - Fault Tree

GBM - Geometric Brownian Motion

HAZOP - Hazard operability

L - Loss to be analyzed

MC - Monte Carlo

OGC - Oil and Grease Content

P&ID - Piping and Instrumentation Diagram/Drawing

PCDS - Probability Consequence Diagrams

PDSPs - Probabilistic Dynamic System Problems

PEQ - Chemical Engineering Program

PFD - Process Flow Diagram

PHA - Preliminary Hazard Analysis

PSA - Probabilistic Safety Assessment

QRA - Quantitative Risk Assessment

ROA - Recursive operability analysis

S - Severity of the event

SHS - Stochastic Hybrid System

SoK - Strength of the Knowledge

U – Uncertain

UFRJ – Universidade Federal do Rio de Janeiro

CHAPTER I - INTRODUCTION

1.1 Introduction of risk analysis for industries

Given the acquired experience of the society on operating the industry of processes, it is known that the process behavior predicted during its project does not match the observed behavior during its operation. Even more, this gap between industry project and operation may lead to undesirable consequences that go from small changes on operational conditions, until major hazards with huge economic impact, loss of life and environmental damages (Crowl and Louvar, 2002). To deal with this misfortune, the idea of risk was incorporated to allow anticipation and fixing of undesirable industrial process behaviors, being an important dimension of any rational decision-making process (Jonkman et al., 2003; Rae et al., 2014; Yang and Haugen, 2015). Actually, the application of the risk concept in industries is on continuous development and tries to mitigate different kind of industrial risks (Crowl and Louvar, 2002).

Despite the lack of consensus, the probability-of-loss risk characterization is the most employed risk metric in industries (Kaplan and Garrick, 1981; Aven and Ylönen, 2016). For this risk characterization, the identification of (i) the possible accident scenarios; and the estimation of (ii) the consequences and (iii) the likelihood of these scenarios are needed (Siu, 1994). In this sense, the term risk analysis is employed to identify different techniques that investigate these three risk dimensions (Crowl and Louvar, 2002). The risk investigation may be used to different risk dimension and a bunch of risk analysis techniques are available (Crowl and Louvar, 2002).

Regarding the steps to identify risks, different techniques are available. In the framework of process hazards, the HAZOP (Hazard Operability study) (Lawley, 1974; Kletz, 1997) is one of the most recognized and probably the most widely used study in the industries (Tyler, 2012). The method examines the plant documentation aiming the identification of hazardous consequences of identified process deviations (Dunjó et al., 2010), being also a source of information for further quantitative risk analysis (Siu, 1994; Demichela et al., 2002). Despite the wide application, some efforts had being made in order to implement computational advances in the HAZOP technique, just as the employment of the so-called expert systems to improve the HAZOP team efficiency, and by considering computational process dynamic simulation to consider the dynamics and non-linearities of the analyzed process (Dunjó et al., 2010).

When the hazard identification is followed by the quantitative calculation of the frequency of the events, several other techniques may be applied. For such estimation, two main classes of evaluations: (i) a static model and (ii) dynamic state-space model (Chiacchio et al., 2011), which are mostly employed to probabilistic risk and reliability/profitability estimation respectively, may be identified. The Event Tree and the Fault Tree are techniques classified as static models (Labeau et al. 2000), while methodologies such as state-space and Markov representations are applied to dynamic process investigation (Chiacchio et al., 2011). Furthermore, when the dynamic probabilistic problem is mixed with the deterministic process behavior problem, the Champman-Kolmogorov equation may be used (Devooght and Smidts, 1996). In the end, the Monte Carlo, classified as a probabilistic resolution method, may be used in order to overcome some difficulties of the analytic resolution procedure of all these introduced techniques (Manno et al., 2012).

Just as the frequency may be computed quantitatively, the severity of events may also be computed quantitatively. For that, different models, which may be classified by the kind of loss to be analyzed, may be employed. To name some, different source models can be used when it is aimed the calculation of the amount of liquid or gas relieved due to a vessel hole; models for gas dispersion may be used to identify how a relived hazardous gas will disperse in the atmosphere (Crow and Louvar, 2002), and also Computational Fluid Dynamics (CFD) may be used in all these cases in order to obtain a more detailed and accurate results.

Despite all these methods for hazard identification and quantitative calculation of frequency and severity, the concept of risk and how it should be used to predict unwanted futures for manage better decisions also lead to some discussions in the literature. Aven (2012) discusses nine different definition of risk that were applied in the risk analysis of industries and Villa et al. (2016) grouped the particularities of all nine definitions in a consequence versus probability perspective, which is in accordance with the probability-of-loss risk perspective that has been dominant for more than 30 years in the industry (Kaplan and Garrick, 1981; Aven and Ylönen, 2016). All these discussions highlight the importance of understanding the risk concept before manage a risk assessment in order to better understand the risk results. Furthermore, a bunch of criticisms are associated with quantitative risk assessment, such as its subjectivity (Aven, 2016) and the errors and superficiality in frequency estimations (Aven 2010, Creed, 2011), to name some. These all reflects on how the industry treats risk and, trying to overcome these drawbacks, the tendency is the improvement of the safety culture guided by an industry dynamic risk management (Aven, 2011; Aven and Krohn, 2014).

Given that, it can be noted that the complementary use of different risk analyses is essential to manage a risk assessment to be monitored by a risk management program. All the existing risk analysis techniques may be used according with different purposes of risk investigation, despite that, all of them have the main goal to improve the understanding of industry abnormal process behaviors (Mannan, 2005). Furthermore, the interaction among these different techniques enables to improve the risk understanding and visualization. Thus, some proposals to combine risks analyses, such as HAZOP and FT, are widely employed (Bendixen and O'Neill, 1984), being the ROA (Recursive Operability Analysis) (Demichela et al., 2002) a detailed procedure to manage such complementarity.

Finally, it is understood that the development of the knowledge about all risk dimensions is one of the most important issues for any kind of scientific and industry development (Jonkman et al., 2003, Yang and Haugen, 2015), being such worry the foundation for the obtainment and maintenance of any kind of industry goal.

1.2 Motivation

This Thesis embraces several steps of the risk assessment framework, going from hazard identification to risk visualization and interpretation. The first contribution is about risk analysis for hazard identification of industrial process. Actually, the most employed technique for such analysis is the HAZOP study, being it responsible to verify the operational security of hazardous chemical process (Crowl and Louvar, 2002). The study is followed without any computational engineering tools during long time meeting with a multidisciplinary group of specialists, requiring a large amount of time and work (Swann and Preston, 1995; Khan and Abbasi, 1997). For sure, given the importance of the study and the available advanced computational tools developed in the last decades, there is the need and a room for the improvements of this investigative work. In fact, the literature reports (Dunjó, 2010) several contribution for the improvement of the technique. However, none of then goes deeper on the main objective of the method, which is to identify process hazards based on process deviations, making only improvements using computational tools on the methodological steps. In this sense, it was visualized a room for developing a new hazard identification analysis that uses process simulation for an improved process abnormal behavior understanding based on process simulation, helping also the approximation between the process simulation and risk analysis area, which seems to be the right path for the processes safety future.

Considering the quantitative risk assessment, it was observed that one of the main difficulties to quantify risk is how to combine the empirical analysis to build a representative model of the analyzed process and its mathematical resolution that leads to the suitable quantitative frequency value of the aimed events occurrence. For that purpose, several methods are available (Crowl and Louvar, 2002, Mannan, 2005) and it was not identified one that combines process model building with wide-applicable mathematical problem resolution that allow to obtain a time representative and process variable dependence frequency result. Given that, it was clear the need of new procedures that combine such highlighted points in a wider risk assessment framework.

Furthermore, considerations about the risk interpretation and visualization are important issues in the framework of risk result usage since it helps to manage the best decision-making. In this framework, the topic uncertainty is one of the most discussed in the literature, being highlighted that its perspective is not fully integrated in the risk analyses methodologies (Aven, 2010). Actually, it is understood that the biggest and most important nowadays discussion about risk and how to use its result is about uncertainties. Such discussions highlight the lack of accuracy of the risk analyses results, demanding on the perspective of risk understanding (Amundrud and Aven, 2015) in order to allow risk-informed decisions instead of risk-based decisions (Apostolakis, 2004; Aven, 2016a). In this sense, the consideration of such ideas about uncertainties in the framework of the quantitative and dynamic risk assessment presented in this thesis was a necessary issue to improve the presented contributions.

Finally, it was observed the need for the integration of the necessary procedures described above in order to allow their complementary usage. In fact, one of the biggest difficulties on manage a complete quantitative risk assessment is to combine different procedures in a well-connected way. Some researches already have considered the integration of risk analysis techniques, being the HAZOP and FT integration the most common employed (Bendixen and O’Neill, 1984) having the ROA (Demichela et al., 2002) as one kind of this integrated procedure. In this sense, it was visualized the need for a procedure that integrates all these methodologies in order to enable an improved and complete quantitative dynamic risk assessment.

1.3 Objective

In the present thesis, the main objective is to propose new procedures (i) to identify hazardous events of process industries, (ii) to estimate frequency of occurrence of hazardous events, (iii) to introduce a new risk definition and visualization that incorporates process simulations and (iv) to integrate all the proposed procedures for manage a quantitative risk assessment. All of these proposals aim to mitigate some of the existing risk analysis drawbacks and criticisms. The idea behind these proposals is to show how different steps of a quantitative risk assessment may be improved by the use of computational tools (as the employed dynamic and stationary process and Monte Carlo simulations) and how these improved methods may interact among each other in order to lead to better risk identification and visualization. It is understood that these improvements are really important for developing the risk concept and to improve the quality of any decision making based on risk information.

The purpose of this thesis is related to the industrial process risk investigation, which was exemplified in a case study where economic risk was investigated. However, given the wide application of the risk concepts, which covers different areas of scientific or human interest, the proposed reasoning and ideas may be employed for different objectives, allowing the improvement of any kind of decision making.

1.4 Text structure

The main contributions of this thesis are presented in four articles structure. Each article is presented in one chapter, which includes all the information needed to introduce the subject matter, the proposals, the case studies, the conclusions and the used references. The three first articles (Chapter II, Chapter III and Chapter IV) present new structured ideas for hazard analysis that are supported by simulation. Despite the separation on different articles, the three first discussed topics are related with each other in a wider risk framework, which is exemplified in the last article (Chapter V). These chapters are presented as follow.

In CHAPTER II, a new procedure to identify and analyze hazards is presented. The method aims to overcome some of the drawbacks of traditional hazard analysis techniques applied on process industries. It is proposed a procedure that is based on (i) devices malfunction identification; (ii) process simulation of the devices malfunctions, in order to identify their dependent process variable deviations; and (iii) a heuristic consequence identification and hazard analysis of the identified abnormal process behaviors. The proposed procedure follows the correct order of cause and consequences events (a device malfunction causes process variable deviations), investigating then real process behaviors. Furthermore, the use of process simulation enables the analysis of any modeled system, allowing the understanding of its dynamic hazard and non-linear behaviors. The heuristic analysis enables the use of expert opinion in order to consider hazards that are not possible to be simulated. In order to exemplify the proposals, the procedure is applied on a startup pump system and compared with the HAZOP process hazard deviation analysis. The comparison has shown that the proposed procedure presents better system interpretation and results, being also better suitable for automation. In the second case study, it is shown the application of the procedure on a dynamic process simulation of an offshore oil production process, where it was possible to identify and quantify the magnitude of the consequences on downstream systems caused by a device malfunction.

In CHAPTER III, a procedure of Probabilistic Safety Assessment (PSA) that aims to overcome some existing difficulties of quantitative frequency estimation of a dynamic and stochastic process is presented. In this procedure, the problem modeling and resolution must: characterize events; build a continuous process based on discrete state-space events; connect the events based on both discrete and continuous random variables; use Monte Carlo simulation to solve the modeled system; and interpret the results to obtain the probability of an event occurrence in a specific length of time. To obtain these results, all problem modeling were built to answer two main questions: (i) what is the probability of a specific process event to occur? (ii) What is the time distribution of the event occurrence? In order to explain the proposal, one Probabilistic Dynamic System Problems with deterministic behaviors was solved. In the problem, the overpressure in a vessel caused by possible failures of two valves was investigated.

In CHAPTER IV, a new risk definition and representations are presented. The proposals aim to provide new tools for improving the risk concept understanding to enable better decisions making. Basically, the risk is a probabilistic representation of the prediction of the loss of undesirable futures. Despite the lack of wide consensus about the risk concept, the term is applied in different areas to manage different kind of decisions, and the perspective of probability-of-loss is the most employed. Furthermore, several criticisms about risk are highlighted in the literature, what may reduce the importance of it for decision-making. In this sense, the proposals aim to organize the ideas needed to investigate undesirable futures. For that, a new risk concept is proposed, where the risk is characterized by function that is dependent of five variables: the loss to be analyzed (L), the identified event(s) (E), the frequency of the event occurrence (F), the severity of the event (S) and the uncertain (U). The uncertainties deserve some attention because it is the source of the most discussions in the literature. It was defined that uncertain is not related to the frequency of events, being defined as the lack of technical quality plus the unknown of the risk analysis. Furthermore, given that both frequency and severity may be represented by a fixes value or a probabilistic function, where the time and the magnitude of the severity is the continuous random variable, the risk might be represented by three different manners: (i) expected value; (ii) probabilistic risk curve; and (i) risk surface. Finally, the new risk definition and surface risk representation were applied in two case studies: a pressurized vessel and a holdup tank.

In CHAPTER V, it is presented how the three proposed risk analysis methods, described in the previous chapters, may be used together in order to manage a complete quantitative risk assessment. The main contribution of this chapter is the proposal of a procedure to manage such risk analyses integration in order to reduce uncertainties of the quantitative risk assessment. In order to exemplify the procedure, the risk of economic loss of a freeze-drying process was investigated. In this case study, the hazard identification based on device failures and dynamic process simulation was applied, making it possible to identify that all simulated devices malfunctions leaded to three harmful consequences and one possibility of operational improvements. Aiming to investigate only the harmful consequences and following the next step of the proposals, the process state space based on the results of the hazard identification analysis was built in order to obtain the frequency of occurrence of the analyzed events. Furthermore, specifying the probabilistic information and the severity magnitude of all events, which were represented by probabilistic functions, the risk surface with *"time x frequency x severity"* dimensions was obtained solving a unique state space problem. In this sense, the proposals enable to obtain a three-dimensional quantitative risk representation by solving the state space obtained directly from the hazard identification analysis. Such risk representation enables the visualization of the relation among the probability of occurrence, the severity magnitude and the time, being possible to identify when an unacceptable pair of severity and frequency, or risk, starts to occur.

In CHAPTER VI, the conclusion of this thesis is presented. The wide risk perspective followed in this thesis has allowed the development of different and complementary approaches for different steps of a complete risk assessment framework. The main contribution of each work are presented and discussed in order to highlight the insights and advantages of their employment. Furthermore, some important topics that were not fully investigated in this thesis are introduced in order to enable the continuous development of the proposals and the risk usefulness for better decision-making.

1.5 References

Amundrud, Ø., Aven, T., 2015, On how to understand and acknowledge risk, Reliability Engineering and System Safety 142 (2015) 42–47

Apostolakis, G. E., 2004, How Useful Is Quantitative Risk Assessment?, Risk Analysis, Vol. 24, No. 3, 2004.

Aven, T., 2010, On how to define, understand and describe risk, Reliability Engineering and System Safety 95 (2010) 623–631

Aven, T., 2011, On the new ISO guide on risk management terminology, Reliability Engineering and System Safety 96 (2011) 719–726

Aven, T., 2012, The risk concept - historical and recent development trends, Reliability Engineering and System Safety 99 33–44.

Aven, T., 2016, Supplementing quantitative risk assessments with a stage addressing the risk understanding of the decision maker, Reliability Engineering and System Safety 152 51–57.

Aven, T., Krohn, B. S., 2014, A new perspective on how to understand, assess and manage risk and the unforeseen, Reliability Engineering and System Safety 121 (2014) 1–10

Aven, T., Ylönen, M., 2016, Safety regulations: Implications of the new risk perspectives, Reliability Engineering and System Safety 149 (2016) 164–171

Bendixen, L., O'Neill, J.K., Chemical plant risk assessment using HAZOP and fault tree methods, Plant/Operations Progress 3 (3) (1984) 179–184.

Chiacchio, F.; Compagno, L.; D'Urso, D.; Manno, G.; Trapani, N., 2011, *Dynamic fault tree resolution: A conscious trade-off between analytical and simulative approach*, Reliability Engineering and System Safety, 96, 1515-1526.

Creed, G. D., 2011, Quantitative risk assessment: How realistic are those frequency assumptions?, Journal of Loss Prevention in the Process Industries 24 (2011) 203e207

Crowl D. A., Louvar J. F., Chemical Process Safety Fundamentals with Applications. (2th ed.). New Jersey, 2002. Prentice Hall International Series in the Physical and Chemical Engineering Sciences.

Demichela M., Marmo L., Piccinini N.,Recursive operability analysis of a complex plant with multiple protection devices, Reliab. Eng. Syst. Saf. 77 (2002) 301–308.

Devooght, J.; Smidts, C.; 1996, *Probabilistic dynamics as a tool for dynamic PSA*, Reliability and System Safety, 52, 185-196.

Dunjó J., Fthenakis V., Vílchez J. A., Arnaldos J., Hazard and operability (HAZOP) analysis. A literature review. J. of Hazard. Mater. 173 (2010) 19-32.

Jonkman, S. N., van Gelder, P.H.A.J.M., Vrijling, J.K., 2003, An overview of quantitative risk measures for loss of life and economic damage, Journal of Hazardous Materials A99 (2003) 1–30

Kaplan, S., Garrick, B. J., 1981, On the quantitative definition of risk, Risk Analysis, Vol. I, No. I, 1981.

Khan F. I., Abbasi S. A., Mathematical model for HAZOP study time estimation. J Loss Prev Process Ind 10(4) (1997) 249–57.

Kletz T. A., Hazop-past and future. Reliab. Eng. Syst. Saf. 55 (1997) 263-266.

Labeau, P. E.; Smidts, C.; Swamaiathan, S., 2000, *Dynamic reliability: Towards an integrated platform for probabilistic risk assessment.* Reliability Engineering and System Safety, 68, 219-254.

Lawley H. G., Operability studies and hazard analysis, Chem. Eng. Prog. 70 (4) (1974) 45-56.

Mannam, S., 2005, Lee’s Loss Prevention in the Process Industries - Hazard Identification, Assessment and Control, Volume 1, Third edition. Elsevier Butterworth-Heinemann.

Manno, G; Chiacchio, F.; Compagno, L.; D’Urso, D.; Trapani, N., 2012, *MatCarloRe: An integrated FT and Monte Carlo Simulink tool for the reliability assessment of dynamic fault tree*, Expert System with Applications, 39, 10334-10342.

Rae, A., Alexander R., McDermid, J., 2014, Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment, Reliability Engineering and System Safety 125 (2014) 67–81

Siu, N., 1994, *Risk assessment for dynamic systems: An overview. Reliability*, Engineering and System Safety 43, 43-*73.*

Swann C. D., Preston M. L., Twenty-five years of HAZOPs. J. Loss Prev. Process Ind. 8(6) (1995) 349–53.

Tyler B. J., HAZOP study training from the 1970s to today. Process Saf. Environ. Prot. 90 (2012) 419-423.

Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016, Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry, Safety Science 89 77–93.

Yang, X., Haugen, S., 2016, Risk information for operational decision-making in the offshore oil and gas industry, Safety Science 86 (2016) 98–109

CHAPTER II - HAZARD IDENTIFICATION

Article accepted in Safety Science 101 (2018) 209-2019 at 19/09/2017
http://dx.doi.org/10.1016/j.ssci.2017.09.014

EMPLOYING PROCESS SIMULATION FOR HAZARD PROCESS DEVIATION IDENTIFICATION AND ANALYSIS

Rafael Raoni[a,b], Argimiro R. Secchi[a], Micaela Demichela[b]

[a] Chemical Engineering Program-COPPE, Universidade Federal do Rio de Janeiro, Cidade Universitária, Centro de Tecnologia, 21941-914 Rio de Janeiro-RJ, Brasil
[b] Department of Applied Science and Technology, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italia
E-mail addresses: rbritto@peq.coppe.ufrj.br (R. Raoni), arge@peq.coppe.ufrj.br (A. R. Secchi), micaela.demichela@polito.it (M. Demichela)
Corresponding author. Tel: +55 21 98488-4057
E-mail address: rbritto@peq.coppe.ufrj.br (R. Raoni)

Abstract: To improve industrial safety, several hazard analyses of processes are available. The HAZOP is one of the most frequently employed and analyzes hazardous process deviations based on heuristic knowledge. Despite the wide application of the technique, new developments are especially important to enhance industrial safety. In this sense a systematic procedure is proposed for hazardous process deviation identification and analysis that employs process simulation and heuristic evaluation. Process simulation enables the analysis of process behaviors caused by device malfunctions and the performance of deviation analysis that considers the process non-linearities and dynamics. A comparison between the HAZOP and the proposed procedure is presented using a pump startup system case study, wherein the better system interpretation and results regarding abnormal process conditions are highlighted. A second case study applies the procedures to an offshore oil production process, showing the advantages of employing process simulation for studying deviation during a dynamic process's abnormal behavior.

Keywords: Hazard analysis; Process simulation; Process deviation; Systematic procedure; Heuristic analysis.

1. INTRODUCTION

Several techniques are available to identify and analyze hazardous conditions. A rigorous and systematic procedure followed by a multidisciplinary team of experts is widely employed in different methods of hazard identification (Crowl and Louvar, 2002; Mannan, 2005). In the framework of process hazards, the HAZOP (*hazard operability*) study (Kletz, 1997; Lawley, 1974; Swann and Preston, 1995; Tayler, 2012) is one of the most recognized and widely used studies in industries (Tyler, 2012), and techniques such as FMEA (*failure mode and effect analysis*) (Kenneth, 2004; McDermott et al., 2009) are also widely used for the identification of hazards caused by failure modes of equipment and processes. Furthermore, in terms of probabilistic risk assessment, several other techniques are available, of which the fault tree (FT) is one of the most often employed (Chiacchio et al., 2011; Siu, 1994).

Given the importance of identifying and analyzing industry hazards, it seems reasonable to improve the quality of hazard assessment by mixing the concepts of different risk analyses, such as the Recursive Operability Analysis (ROA) (Demichela et al., 2002), which integrates the concepts of the HAZOP for hazard identification and the FT for frequency assessment. Furthermore, considering the HAZOP as one of the most important hazard analyses in process industries, some of its insights and improvements are introduced.

1.1. Description of traditional HAZOP

Basically speaking, the method examines the plant documentation with the aim of identifying the hazardous consequences of recognized process deviations (Dunjó et al., 2010) as well as being a source of information for further quantitative risk analysis (Demichela et al., 2002; Siu, 1994). The technique's power lies in its procedure for generating process deviations (e.g. high pressure), which combines guide words (high, less, none, etc.) and process variables (pressure, temperature, etc.). The analysis is carried out considering deviations at the identified nodes, referred to as plant sections, in which the process variables' behavior is analyzed to allow the identification of the causes, consequences and safeguards of the deviation. Furthermore, following some reference tables, the qualification of the scenario risk may be made for a certain risk focus (e.g. the environment, people, image and assets) and, when necessary, some observations or recommendations may be offered (Dunjó et al., 2010) to improve the process's safety concerning the identified hazard.

The systematic procedure enables the identification of all the possible deviations of the system (Crowl and Louvar, 2002), which, depending on its dimension, may be divided into smaller subsystems to facilitate a manageable analysis. The method is employed during long-time meetings with a multidisciplinary group of specialists and requires a large amount of time and work (Khan and Abbasi, 1997; Swann and Preston, 1995). Its quality strongly depends on the capability of the safety specialist who guides the study, on the expertise of the multidisciplinary group and on the group's capability to maintain accuracy until the end of the study.

1.2. Computational advances in hazard analysis

Despite the wide application of heuristic hazard analyses, some efforts have been made to make computational advances in hazard assessment techniques. Aiming to improve the HAZOP team efficiency, so-called expert systems have been studied widely (Dunjó et al., 2010) and implemented in many commercial tools. The main idea of the proposals is to analyze the propagation of the deviation throughout an empirical model of the system (Bartolozzi et al., 2000; Boonthum et al., 2014; Cocchiara et al., 2001; Cui et al., 2010; Leone, 1996; Wang and Gao, 2012), generating an "automatic HAZOP" requiring less time (Boonthum et al., 2014) and providing constant quality during the whole analysis and improved consequence identification due to the deviation propagation throughout the system model (Bartolozzi et al., 2000). Accordingly, the deviation propagation may use, among others, a petri network (Chung and Chang, 2011; Srinivasan and Venkatasubramanian, 1998a, 1998b) or fuzzy logic (Guimarães and Lapa, 2005).

Other works have considered computational process dynamic simulation for hazard study to investigate the emergency process conditions (Shacham et al., 2004), for operators training in emergency situations (Eizenberg et al., 2006b) and to identify the conditions in which safeguard activation occurs (Demichela and Camuncoli, 2013). The use of dynamic simulation for deviation analysis has been employed in an extended HAZOP approach (Ramzan et al., 2006), making possible the identification of non-trivial consequences and better system safeguards (Li et al., 2010). Furthermore, the importance of simulation has been highlighted for hazard analysis of non-linear processes with multiple steady states (Labovsky et al., 2007; Svandova et al., 2005), in which an improved quantitative and sensitive deviation analysis is required. In these latter works, it was exemplified that a small deviation can cause substantial process disturbance, highlighting the advantages of quantitative versus qualitative deviation analysis.

Both expert system and process simulation aim to overcome some of the difficulties faced during a heuristic hazard analysis. Given the complexity of process plants, it seems logical to use process simulations to understand hazardous process conditions and to implement computational advances to automate a known systematic approach. On the other hand, since not all anomalous process behaviors can be predicted or implemented in computational software, the importance of expert opinion for hazard analysis is highlighted. In this sense a procedure that groups both computational advances and expert opinion seems important to improve the process safety.

In this work a systematic procedure that uses process simulation is proposed for the identification and analysis of hazardous process deviation. The procedure presents steps that can be automatized computationally and is concluded in multidisciplinary meetings. The hazard scenario is defined as one possible malfunction of devices (process units), which must be simulated to identify the group of its dependent process deviations. Such information is grouped and feeds a further heuristic process hazard analysis that aims to overcome the limitations of the computational tools. In Section 2 the proposed procedure is described; in Section 3 two case studies that aim to exemplify the procedure's application, results and technical improvements are provided; and in Section 4 the conclusion of the work is presented.

2. PROPOSED PROCEDURE

2.1. Procedure description and process boundaries

During normal operation, with proper action of the process devices, no problems arise. Then an abnormal system condition occurs when a particular device does not operate as originally expected. To give an example, the inappropriate opening of a control valve is an abnormal system condition that could be caused by previous events and leads to several further undesirable consequences, including some process deviations. Such an example, shown in Figure 1, represents a sequence of process behaviors in terms of cause–consequence assumptions, which could be extended by previous causes and further consequences until the desired level of detail is reached. Therefore, to propose a manageable procedure, it is necessary to determine the boundaries of the process to be analyzed.

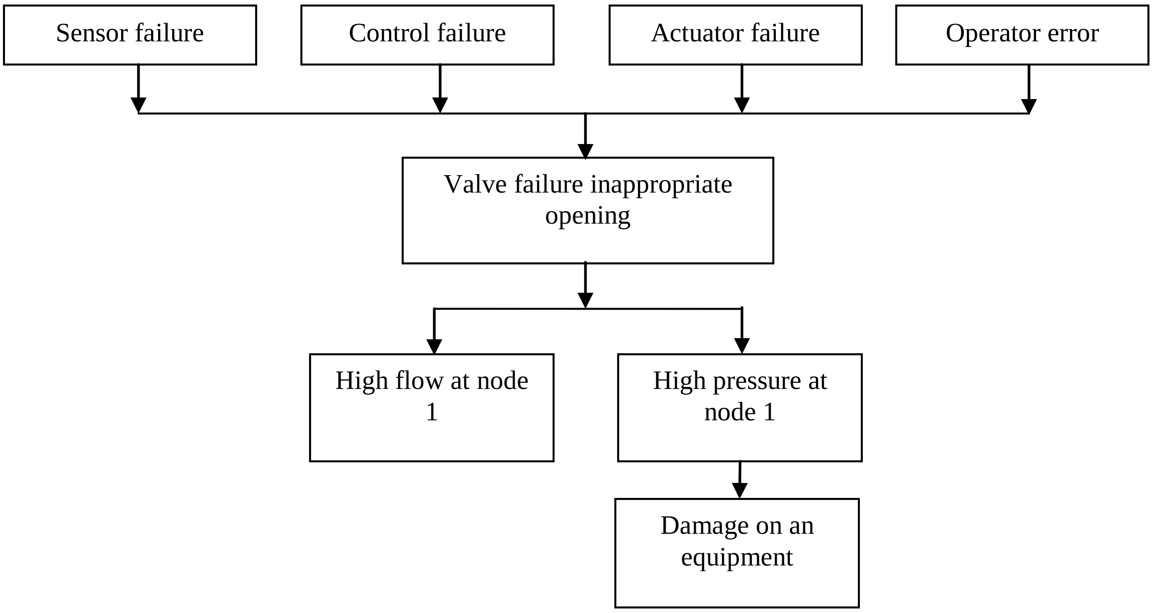


Figure II 1: Sequence of undesired events caused by a valve failure.

Aiming to identify process deviations, the identification of their causes is defined as the starting point of the proposed analysis, and, the inappropriate manipulation of devices being the major cause of process deviations, a study of the devices' malfunction is needed. In this sense, despite the possibility of using any kind of procedure, the FMEA could be understood as a good choice to identify devices' inappropriate manipulation. Moreover, during this identification attention must be paid to identifying device malfunctions that change the normal process condition, which must include the identification of common cause failures. Furthermore, the analysis of these changes during the normal process condition enables the identification of process deviations and further consequences. In addition, after an inappropriate device malfunction, the transient behavior of the process determines the necessary time until the occurrence of the process deviations and their further consequences, leaving room for interventions from the system safeguards.

Therefore, each device malfunction must be identified as one hazard scenario to be analyzed. By this definition, which follows the natural order of sequenced cause and consequence events, all the deviations that are dependent on the scenario device malfunction are grouped together for further consequence and system safeguard identification. The structure of the proposed procedure, using the previous example (inappropriate valve opening), is illustrated in Figure 2.

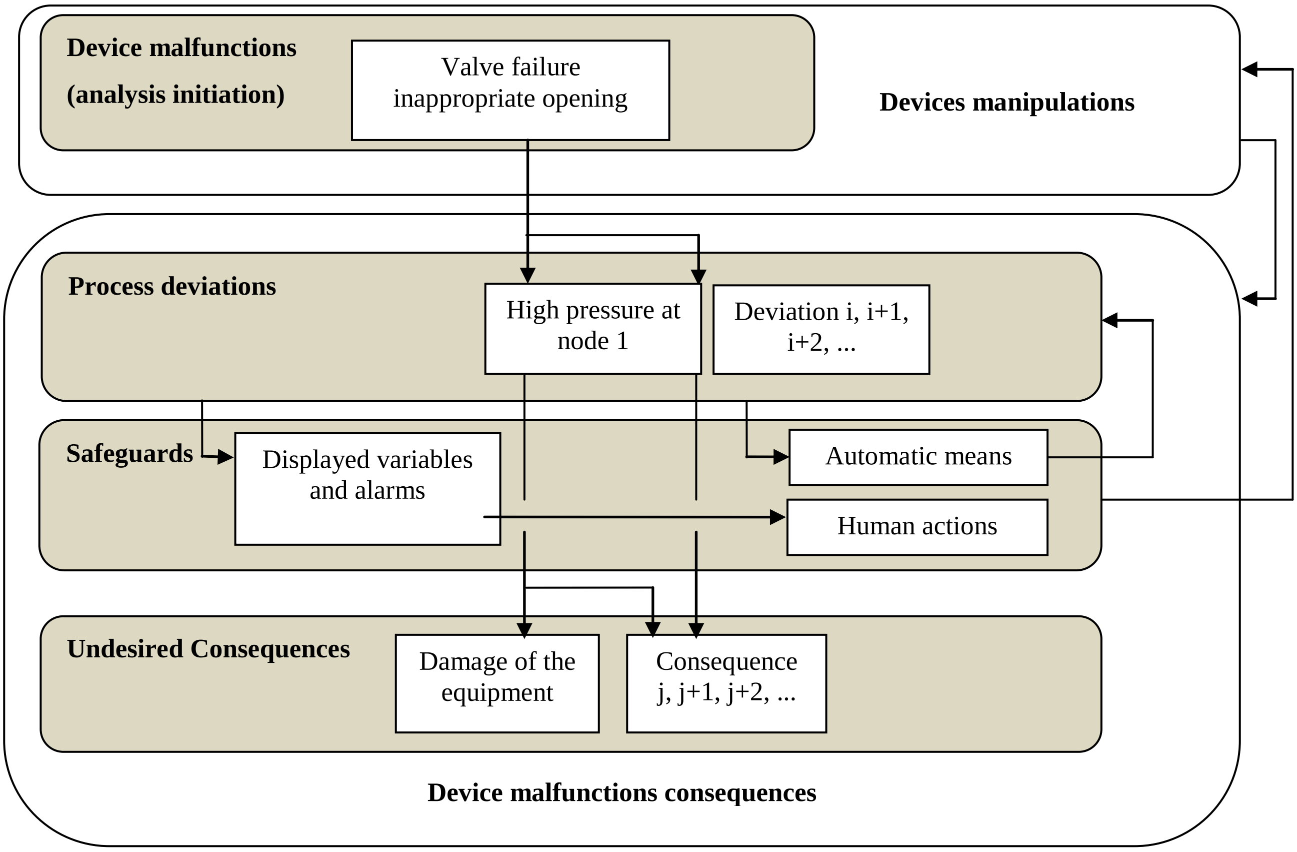


Figure II 2: Proposed procedure structure.

2.2. The use and importance of process simulation

The cause–consequence relationship between device malfunctions and process deviations may be described by heuristic analysis (HAZOP), by heuristic assumptions with computational advances (expert systems) or by phenomenological models in a process simulator. Heuristic considerations and their qualitative approach cannot handle transient and non-linear process behaviors, and, when such process characteristics cannot be neglected, process simulation and its quantitative investigation are the most suitable tool. In this sense the process simulation can improve the results of a hazardous deviation analysis by quantifying the deviations and reducing the process interpretation mistakes. Furthermore, the procedure steps that employ process simulation are presented to be automatized computationally to reduce the required time for the identification of the process deviation. Finally, given the importance of expert opinion for hazard investigation, the hazard analysis is finished by considering expert opinion to identify further consequences of the process deviations identified by the process simulation.

2.3. Steps of the proposed procedure

The following steps constitute the proposed procedure:

- 1. System knowledge: This step aims to introduce the system to be analyzed, which must be fed with the system documents (P&ID, PFDs, data sheets, etc.);
- 2. System modeling: A phenomenological model of the system is implemented in an appropriate process simulator. To build the model for such an application, the variables that represent device configurations need to be assigned as input variables while all the other process variables are dependent variables. As such a model is helpful for the process design, its development may already have been undertaken during a previous design step.
- 3. Simulations:

-*3.1 Simulation 1*: This is carried out to verify whether the model correctly represents the normal system condition, obtaining the values of all the process variables in the normal operational condition.

-*3.2 Simulation 2*: The identified device malfunctions are simulated one by one to identify the behavior of the system in terms of process deviations.

- 4. Scenario analysis: The proposed method separates the deviation analysis obtained from the simulation results from the further consequence analysis, which needs to be performed heuristically:

- *4.1 Simulation result analysis*: This step aims to compare the normal operation simulation with the device malfunction simulations. The process deviations are quantitatively identified, and the activations of the system safeguards are verified.

-*4.2 Hazard heuristic analysis*: With the *simulation result analysis*, the search for further consequences of the deviations, which requires a meeting with a multidisciplinary group, may be undertaken. Each listed consequence may activate further system safeguards that must be identified, and a risk qualification for each identified consequence may be made. Furthermore, when needed, observations or recommendations for the identified hazard should be proposed.

- 5. Result presentation: The proposed table, shown in Table 1, groups all the important information obtained from the proposed procedure.

Table II 1: Proposed table for hazardous process deviation and identification analysis.

<table>
<tr><td colspan="7"><b>System under study:</b></td></tr>
<tr><td colspan="7"><b>Device:</b></td></tr>
<tr><td colspan="7"><b>Scenario number:</b></td></tr>
<tr><td rowspan="3"><b>Device malfunction</b></td><td colspan="6"><b><i>Simulation results analysis</i></b></td></tr>
<tr><td colspan="2"><b>Variable deviation information</b></td><td colspan="4"><b>Deviation safeguards</b></td></tr>
<tr><td><b>Variable identification and normal value</b></td><td><b>Value under deviation</b></td><td><b>Displayed variable</b></td><td><b>Alarms</b></td><td><b>Automatic means</b></td><td><b>Possibility of human actions</b></td></tr>
<tr><td rowspan="7"></td><td></td><td></td><td></td><td></td><td></td><td rowspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6"><b><i>Hazard heuristic analysis</i></b></td></tr>
<tr><td rowspan="2"><b>Further consequences</b></td><td rowspan="2"><b>Consequence safeguards</b></td><td colspan="3"><b>Risk assessment:</b></td><td rowspan="2"><b>Notes, observations, recommendations</b></td></tr>
<tr><td><b>Frequency</b></td><td><b>Severity</b></td><td><b>Risk</b></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

- **System under study**: Refers to the system that is undergoing analysis.
- **Device**: Refers to the analyzed device.
- **Scenario number**: A sequential number for computing all analyzed scenarios.
- **Device malfunction**: Identifies which device malfunction is analyzed in the scenario.
- **Simulation result analysis**: Covers all the analyses to be performed based on the simulation results.

- *Variable identification and normal value*: Identifies and lists the variables analyzed in the simulation, pointing out their system location and their value in normal process conditions;

- *Variable under deviation*: Points out the value of the relevant variable in the abnormal condition (variable deviation value);

- *Displayed variable*: Indicates whether the relevant variable is displayed, on a supervision screen or in the field, for monitoring by plant operators;

- *Alarms*: Identify the activated alarms for the relevant variable deviation;

- *Automatic means*: Identify the activated automatic means for the relevant variable deviation;

- *Possibility of human actions*: Since the abnormal process condition is an unexpected and not easily identifiable event, this information aims to determine whether, in the case of a real occurrence of the hazard scenario, the plant operators would be able to identify that the process is experiencing an abnormal condition. Such identification enables human actions to seek the cause of the abnormal condition to avoid further undesirable consequences. The “possibility of human action” is positive if there is at least one displayed variable under deviation or if there is at least one activated alarm in the scenario;

- **Hazard heuristic analysis**: Covers all the analyses to be performed by the group of specialists based on the obtained *simulation result analysis*.

- *Further consequences*: Identify the possible further consequences based on one variable deviation or on the group of variable deviations analyzed in the scenario;

- *Consequence safeguards*: Identify the safeguards that can avoid the spreading of the relevant consequence, avoiding even more undesirable events;

- *Risk assessment*: Qualifies the risk based on the frequency and severity of the consequence;

- *Notes, observations and recommendations*: Space destined for some relevant notes, observations or recommendations proposed by the group of specialists.

Figure 3 shows the flow chart for the execution of the proposed procedure.

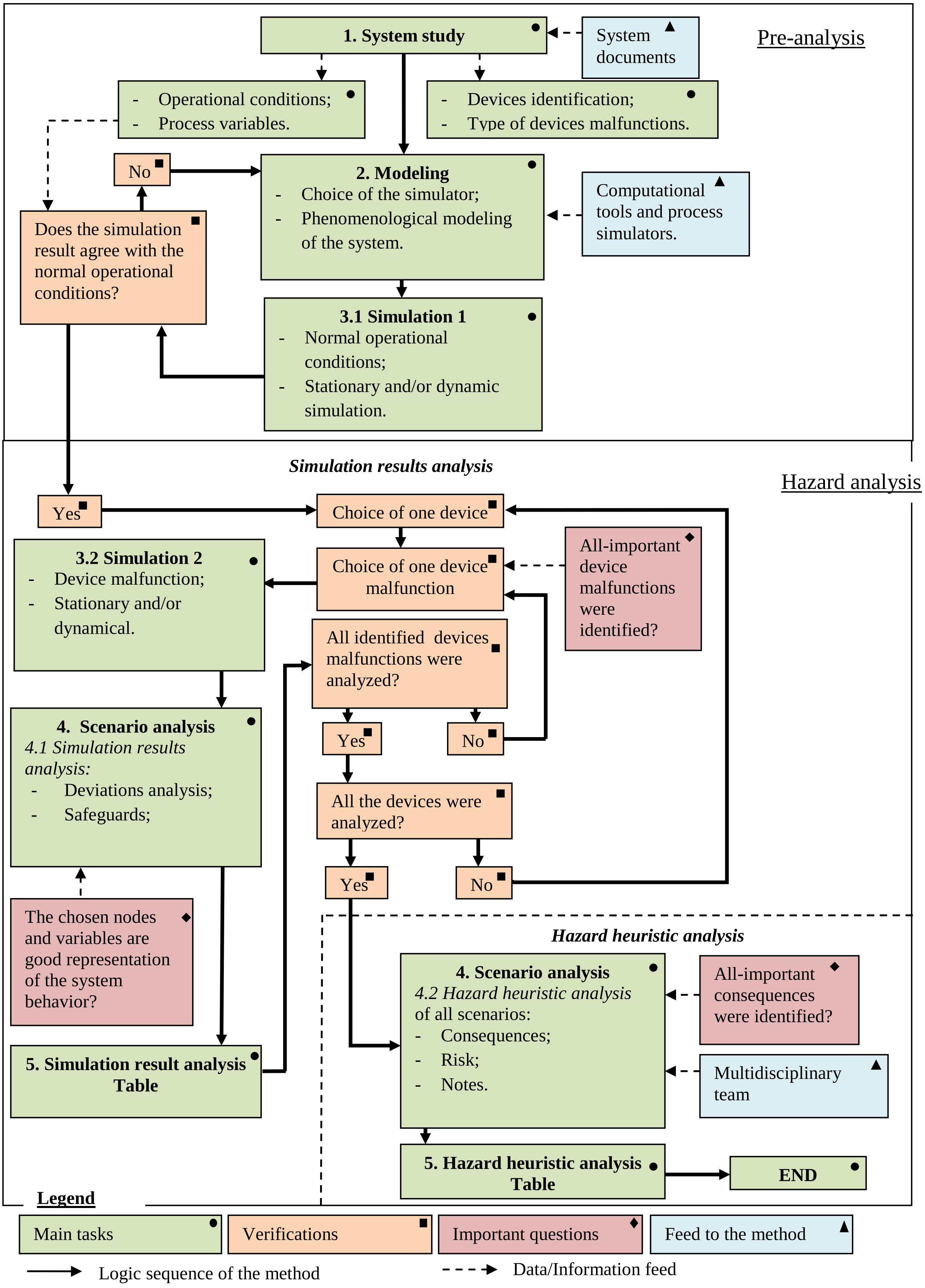

Pre-analysis
1. System study ●
System documents ▲
- Operational conditions; ●
- Process variables.
- Devices identification; ●
- Type of devices malfunctions.
No ■
2. Modeling ●
- Choice of the simulator;
- Phenomenological modeling of the system.
Computational tools and process simulators. ▲
Does the simulation result agree with the normal operational conditions? ■
3.1 Simulation 1 ●
- Normal operational conditions;
- Stationary and/or dynamic simulation.
Simulation results analysis
Hazard analysis
Yes ■
Choice of one device ■
3.2 Simulation 2 ●
- Device malfunction;
- Stationary and/or dynamical.
Choice of one device malfunction ■
All-important device malfunctions were identified? ◆
All identified devices malfunctions were analyzed? ■
Yes ■
No ■
4. Scenario analysis ●
4.1 Simulation results analysis:
- Deviations analysis;
- Safeguards;
All the devices were analyzed? ■
Yes ■
No ■
The chosen nodes and variables are good representation of the system behavior? ◆
Hazard heuristic analysis
4. Scenario analysis ●
4.2 Hazard heuristic analysis of all scenarios:
- Consequences;
- Risk;
- Notes.
All-important consequences were identified? ◆
Multidisciplinary team ▲
5. Simulation result analysis Table ●
5. Hazard heuristic analysis Table ●
END ●
Legend
Main tasks ●
Verifications ■
Important questions ◆
Feed to the method ▲
Logic sequence of the method
Data/Information feed

Figure II 3: Proposed procedure flow chart.

]

2.4. Further observation

The proposed procedure aims to improve the identification and analysis of hazardous process deviations by: (i) respecting the normal sequence of cause and consequence events; (ii) employing process simulation to improve the understanding of process abnormal behavior; and (iii) ascertaining the expert opinion for consequence identification and risk assessment during the final heuristic analysis. The proposed Table 1 separates the deviation from the consequence analysis to make a distinction between the simulation and the heuristic results. Furthermore, given that the simulation result groups a set of deviations that can occur simultaneously during real abnormal system behaviors, they are valuable information for seeking the root cause of real-time abnormal process behaviors.

However, the difficult task of developing a phenomenological model for large-scale processes could raise doubts about its application for safety purposes. To mitigate such a drawback, as reported by Eizenberg et al. (2006a), the idea of dividing the entire system into minor subsystems, just as performed in the HAZOP, could be used to facilitate the modeling process. In addition, to take into account the device malfunction perturbation between subsystems, simultaneous process deviations at the intersection are required. Despite the modeling process drawbacks, process simulation has already been applied widely during several process designs, and the obtained results more than compensate for the labor involved. Therefore, it does not make sense not to apply such technology for safety purposes, even if it requires the development of new procedures, with new requirements, such as those proposed in this work.

Furthermore, given that a non-identified scenario is a non-studied scenario (AIChE, 2000), attention must be paid to the identification of the device malfunctions to be simulated. Since some devices are manipulated by continuous variables, just like the opening of a control valve, a large spectrum of possibilities is faced to identify the device magnitude malfunctions to be simulated. Such identification could be guided by understanding how the device is manipulated normally or the limit at which the magnitude of the device change may cause an undesirable consequence.

Finally, knowing that one device malfunction may generate several process deviations, and since not every deviation is significant in the hazard framework, not every deviation needs to be identified and analyzed. As the process simulation enables every process variable to be monitored, the definition of the variables to be analyzed has great importance for the proposed procedure. One recommendation is to select the variables that are already monitored in the system project, which were already identified as being important in the process design. Furthermore, in any case, process variables may be chosen in identified nodes, just as performed in the traditional HAZOP.

3. CASE STUDIES

The proposed procedure was applied in two case studies: a pump recirculation system and an offshore oil treatment unit. In the first case study, a risk assessment of the consequences of undesirable process deviations was carried out. This case aims to illustrate the step-by-step application of the proposals and to compare the results with those of the HAZOP approach. In the second case study, a hazard scenario was dynamically investigated, and undesirable consequences for the production were found. Tables 2, 3 and 4 were employed for the hazard assessment of both examples (Bureal Veritas, 2007).

Table II 2: Severity classification.

Severity		
1	Negligible	Process is not stopped; repair costs < 10,000 Euros.
2	Low	Process is stopped briefly without following-up costs; repair costs < 50,000 Euros
3	Moderate	Partial shut-off of the facility (max. 1 day), process can (possibly) be continued; repair costs < 500,000 Euros
4	High	Partial shut-off of the facility from 2 days to max 2 weeks; repair and following-up costs < 5 million Euros
5	Critical	Complete shut-off of the facility; repair and follow-up costs > 5 million Euros

Table II 3: Frequency classification.

Frequency classification		
1	Remote	Any occurrence in industry is unknown or appears unlikely
2	Unlikely	Has occurred in the industry
3	Likely	Has occurred within the company sector
4	Several	Has occurred within the operating company
5	Many	Can occur in the company several times a year

Table II 4: Risk matrix.

Consequence	Frequency				
	1	2	3	4	5
1	🟩	🟩	🟩	🟩	🟨
2	🟩	🟩	🟩	🟨	🟨
3	🟩	🟩	🟨	🟨	🟨
4	🟩	🟨	🟨	🟨	🟥
5	🟨	🟨	🟥	🟥	🟥
🟥	Unacceptable risk	Is required project modifications or at the operational procedures.			
🟨	Marginal risk	Should be considered the risk reduction.			
🟩	Negligible risk	Without the need of risk reduction.			

3.1. Pump startup system

3.1.1. System description

A pump startup system is found in installations with high-capacity pumps (large flow and high discharge pressure), commonly used for long-distance transportation of petroleum through ducts, for example. It consists of an arrangement of pipes that connect the pump discharge to its suction, allowing the recirculation of the product, and a pipe accident (i.e. restriction orifice ISO-5167-2 (2003)), required to stabilize the pump discharge and suction pressures. The recirculation procedure is required at pump startup to minimize the required power and avoid possible electrical damage, which could cause fire or other undesirable consequences.

The system under analysis is composed of two recirculation systems of two different groups of pumps (“main pumps” and “booster pumps”) that are connected in series and suctioning from a petroleum tank. The recirculation system of each group of pumps was designed to operate with only one pump at a time using an arrangement with two restriction orifices in series. For each group of pumps, there are two orifice arrangements, one used normally and another as backup.

A simplified flow chart of the described system is shown in Figure 4, where “Pi” refers to the pipes, “Ai” refers to the restriction orifice arrangements and “Ni” refers to the nodes where the process variables will be analyzed. HVs means hand valves, XVs automatic on–off valves and UV the control valve. The indicators PIs and FIs allow the monitoring of the pressure and flow rate at the indicated point, and the FIs also activate alarms and automatic means, as presented in Table 5.

Table II 5: Alarms and automatic means of the FIs.

	Value	*Alarm*	*Automatic means**
FI1	250 m^3/h	FAL1	FSL1 - Shut down BP
FI2	600 m^3/h	FAL2	FSL2 - Shut down MP

* BP = booster pumps and MP = main pumps

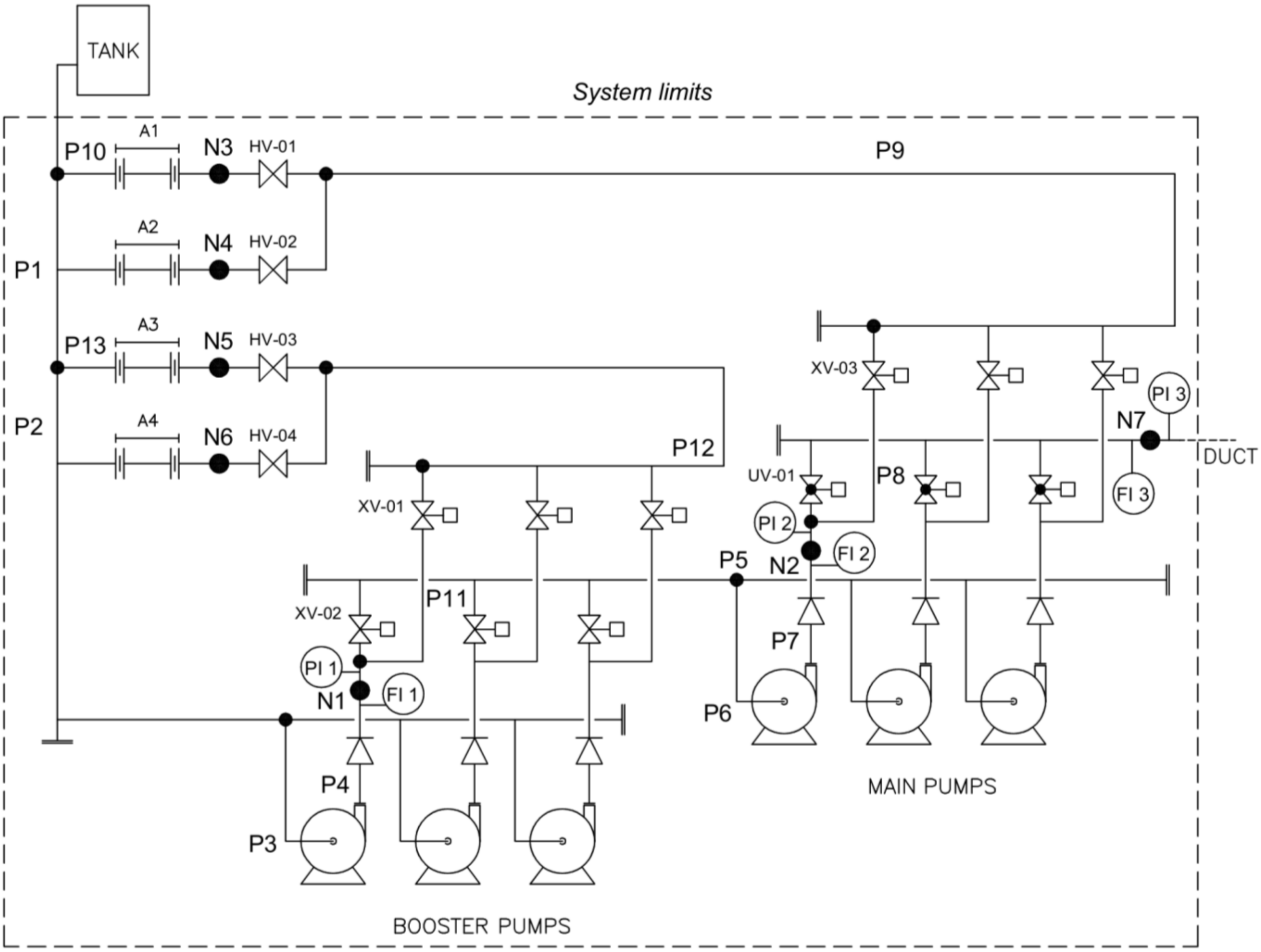


Figure II 4: Recirculation pump system.

In this work the procedure is applied after the booster pump startup, which does not need a low flow rate, and during the startup of the main pump, which does need a low flow rate.

3.1.2. Mathematical modeling

As showed by Raoni et al. (2016), the system needs to be modeled as a looped pipeline network problem and may be solved by simultaneous modular simulation. The specifications of the model are shown in Table 6, and the steady-state assumption was applied. The model was built in Matlab, and the *fsolve* function was used to solve its non-linear system of equations.

Table II 6: Specification of the simulation

P_0 (petroleum column)	110.2 kPa
Pressure drop equation	Darcy-Weisbach
Roughness	4.572×10^{-5} m
Straight length of the pipes (for the 13 pipes)	[20 30 10 10 70 16.5 6 15.9 80 10 10 20 10] m
Diameter of the pipes (for the 13 pipes)	[1.40 1.407 0.74 0.58 1.04 0.58 0.48 0.23 0.58 0.23 0.18 0.38 0.18] m
Density	937 kg/m^3
Viscosity	206.14 cP
Main pump ΔP equation (F [=] m^3/h)	$(-1.8\times10^{-8}\ F^3 + 1.8\times10^{-4}\ F^2 - 0.28\ F + 8456.53)$ kPa
Booster pump ΔP equation (F [=] m^3/h)	$(2.8\times10^{-8}\ F^3 - 8.3\times10^{-5}\ F^2 + 0.051\ F + 1303.1)$ kPa
Restriction condition of the main pump flow	$F_{main.pump} > 720$ m^3/h (0.20 m^3/s)
Restriction condition of the booster pump flow	$F_{booster.pump} > 320$ m^3/h (0.09 m^3/s)
Orifice diameter of all four orifices at A1 and A2	2.6 in (0.0660 m)
Orifice diameter of all four orifices at A3 and A4	2.8 in (0.0711 m)
Static head of the duct	600 m
Straight length of the duct	200000 m
Diameter of the duct	36 in (0.91 m)

3.1.3. Simulations: Normal operation

The normal operation includes the startup of one main pump with a low flow rate (between 5% and 10% higher than the minimum flow rate) aligned with A1 and one booster pump with no flow rate restriction aligned with A3. To understand the system behavior, the pressure and flow rate at the discharge of the booster pump (P_{N1} and F_{N1}, respectively, at node N1), the pressure and flow rate at the discharge of the main pump in operation (P_{N2} and F_{N2}, respectively, at node N2), the flow rate through the four orifice arrangements (F_{N3} for A1, F_{N4} for A2, F_{N5} for A3 and F_{N6} for A4, respectively, at nodes N3, N4, N5 and N6) and the flow rate at the duct (F_{N7} at node N7) were chosen as the process variables to be analyzed. The valve conditions are shown in Table 7 and the operating values of the analyzed variables in Table 8.

Table II 7: Normal valve positions.

Valve	*Position*
UV-01	Close
XV-01	Open
XV-02	Open
XV-03	Open
HV-01	Open
HV-02	Close
HV-03	Open
HV-04	Close

Table II 8: Process variables' values.

Process variables	*Variable location**	*Normal condition*
P_{N1}	N1 - BP discharge	13.9×10^5 Pa
F_{N1}	N1 - BP discharge	0.31 m^3/s
P_{N2}	N2 - MP discharge	96.5×10^5 Pa
F_{N2}	N2 - MP discharge	0.21 m^3/s
F_{N3}	N3 - A1	0.21 m^3/s
F_{N4}	N4 - A2	0 m^3/s
F_{N5}	N5 - A3	0.10 m^3/s
F_{N6}	N6 - A4	0 m^3/s
F_{N7}	N7 - Duct	0 m^3/s

* BP = booster pumps and MP = main pumps

3.1.4. HAZOP results

To apply the HAZOP method, the nodes proposed in Figure 4 may be employed. Here the method was applied only at nodes N1, N2 and N7, which were enough for the purpose of the present work. Choosing "pressure" and "flow" as process variables and "high," "low" and "none" as guide words ("none" only for "flow"), 15 scenarios may be analyzed. In Table 9 the result for the deviation "low pressure" at node N2 is shown.

Table II 9: HAZOP analysis: "low pressure" at node N2.

System under study: Pump recirculation system							
Node: N2							
Scenario number: 1							
Process deviation	**Causes**	**Consequences**	**Safeguards**	**Assets equipment supplies**			**Notes, observations, recommendations**
				Freq.	**Sev.**	**Risk**	
Low pressure	1-HV-01 opened	*Damage to the pump; *Low flow, for the causes 3, 4 and 5 *High flow, for the causes 1 and 2.	*FSL2 (Shut of the main pump by low flow)	5	3	Marginal	It is possible to forecast a low pressure interlock for the system, but is needed better study for set the instrument.
	2-UV-01 opened						
	3-XV-02 closed						
	4-Booster pump stop						
	5-Principal pump stop						

3.1.5. Proposed hazard analysis results

Having identified the system devices and their malfunctions, presented in Table 10, the steps shown in Figure 3 were applied.

Table II 10: Studied device malfunctions.

Device	*Device malfunction*	*Scenario number*
XV-01	Valve closed	1
XV-02	Valve closed	2
XV-03 or HV-01	Valve closed	3
HV-02	Valve opened	4
UV-01	To early opening	5
Main pump	Stop	6
Booster pump	Stop	7

Regarding the identified scenarios (Table 10), as it was considered that the booster pump recirculation system was correctly aligned, it was not necessary to consider malfunctions of HV-03 and HV-04; given that the wrong position of XV-03 and HV-01 would lead to the same deviations, their malfunction analyses are listed together in a single scenario (scenario 3). Furthermore, since the normal system operation must be maintained during a minimal period of time to stabilize the startup of the main pump, an analysis of the early pump alignment with the duct was needed (scenario 5).

Simulating the entire device malfunctions presented in Table 10, all the information required for the *simulation result analysis* may be obtained. Given the employment of the simulation, the identification of the deviations in all the nodes presented in Figure 4 does not make the analysis larger. With the simulation results, the heuristic analysis can be performed to conclude the proposed procedure. The results of scenario 4 are shown in Table 11, and its recommendation and note are presented in Table 12.

Table II 11: Scenario 4 results: Pump recirculation system.

System under study: Pump recirculation system						
Device: HV-02						
Scenario number: 4						
Device Malfunction	***Simulation results analysis***					
	Variable deviation information		**Deviation safeguards**			
	Variable identification and normal value	**Value under deviation**	**Displayed variable**	**Alarms**	**Automatic means**	**Possibility of human actions**
Valve open	P_{N1}: $13.9x10^{5}$ Pa	$13.1x10^{5}$ Pa	Yes	No	No	Yes: By the understanding of the abnormal condition of the displayed process variables PI1, FI1, PI2 and FI2.
	F_{N1}: 0.31 m^{3}/s	0.50 m^{3}/s	Yes	No	No	
	P_{N2}: $96.5x10^{5}$ Pa	$90.1x10^{5}$ Pa	Yes	No	No	
	F_{N2}: 0.21 m^{3}/s	0.40 m^{3}/s	Yes	No	No	
	F_{N3}: 0.21 m^{3}/s	0.20 m^{3}/s	No	No	No	
	F_{N4}: 0 m^{3}/s	0.20 m^{3}/s	No	No	No	
	F_{N5}: 0.10 m^{3}/s	0.097 m^{3}/s	No	No	No	
	F_{N6}: 0 m^{3}/s	0 m^{3}/s	No	No	No	
	F_{N7}: 0 m^{3}/s	0 m^{3}/s	Yes	No	No	
	Hazard heuristic analysis					
	Further consequences	**Consequence safeguards**	**Risk assessment:** Assets equipment supplies			**Notes, observations, recommendations**
			Frequency	**Severity**	**Risk**	
	High potency -Damage to the main pump	No safeguards	5	3	Marginal	Recommendation 1
	Focus of fire	Fire-fighting system	3	4	Marginal	Note 1

Table II 12: Note and recommendation.

Note 1
As the "focus of fire" is a further consequence of the "high potency" and not necessarily the "high potency" lead to focus of fire, it was considered the frequency of the "focus of fire" lower than the frequency of the "high potency".
Recommendation 1
Given the marginal risk, it is needed forecast some system safeguard, such as new alarms or automatic means, for the monitored variables (FI1, PI1, FI2, PI2).

3.1.6. Comparison between the results of the HAZOP and the proposed procedure

The results of the HAZOP (Table 9) show that "low pressure" at N2 is a consequence of several causes, including the inappropriate opening of HV-02 analyzed by the proposed procedure (Table 11). However, due to the difference in the scenario characterization, the consequences of the two scenarios are not the same. Furthermore, analyzing the results of the other scenarios investigated by the proposed procedure, it was possible to note that the further consequences of the HV-02 malfunction are not the same as all the other analyzed device malfunctions that also cause low pressure at N2. Table 13 shows the relations between the cause and the further consequences, obtained by the proposed procedures, which have "low pressure" at node N2 as one of the process deviations.

Table II 13: Cause–consequence with “low pressure” deviations

Cause	*Further consequences*
HV-02 opened and UV-01 to earlier opening	*Damage to the main pump (high potency); *Focus of fire.
XV-02 closed	*Damage to the main pump (no suction flow).
Booster pump stop	*Damage to the main pump (flow lower than the minimum).
Main pump stop	*No further undesirable process consequences.

The analysis of Table 13 provides an understanding that different causes can lead to different consequences, even if they have the same process deviation. Such a conclusion highlights the HAZOP’s difficulty in identifying the scenario consequences given a unique deviation. Understanding that this same reasoning can be applied to safeguard identification, the employment of the natural sequence of cause and consequence events for hazard and safeguard identification is highlighted, since it is an important improvement for deviation hazard analysis.

3.2. Offshore oil production

In this example the proposed procedure is applied to a unique device malfunction (scenario) of a dynamic process of offshore oil production. The risk assessment focused on the capacity and quality of the production, and therefore only some of the process deviations were analyzed.

3.2.1. System description

During offshore oil production, the platform separates the produced water, oil and gas (the primary treatment) and controls the oil production by injecting produced gas (gas-lift) into its wells. The representative flow chart of the process referred to is shown in Figure 5.

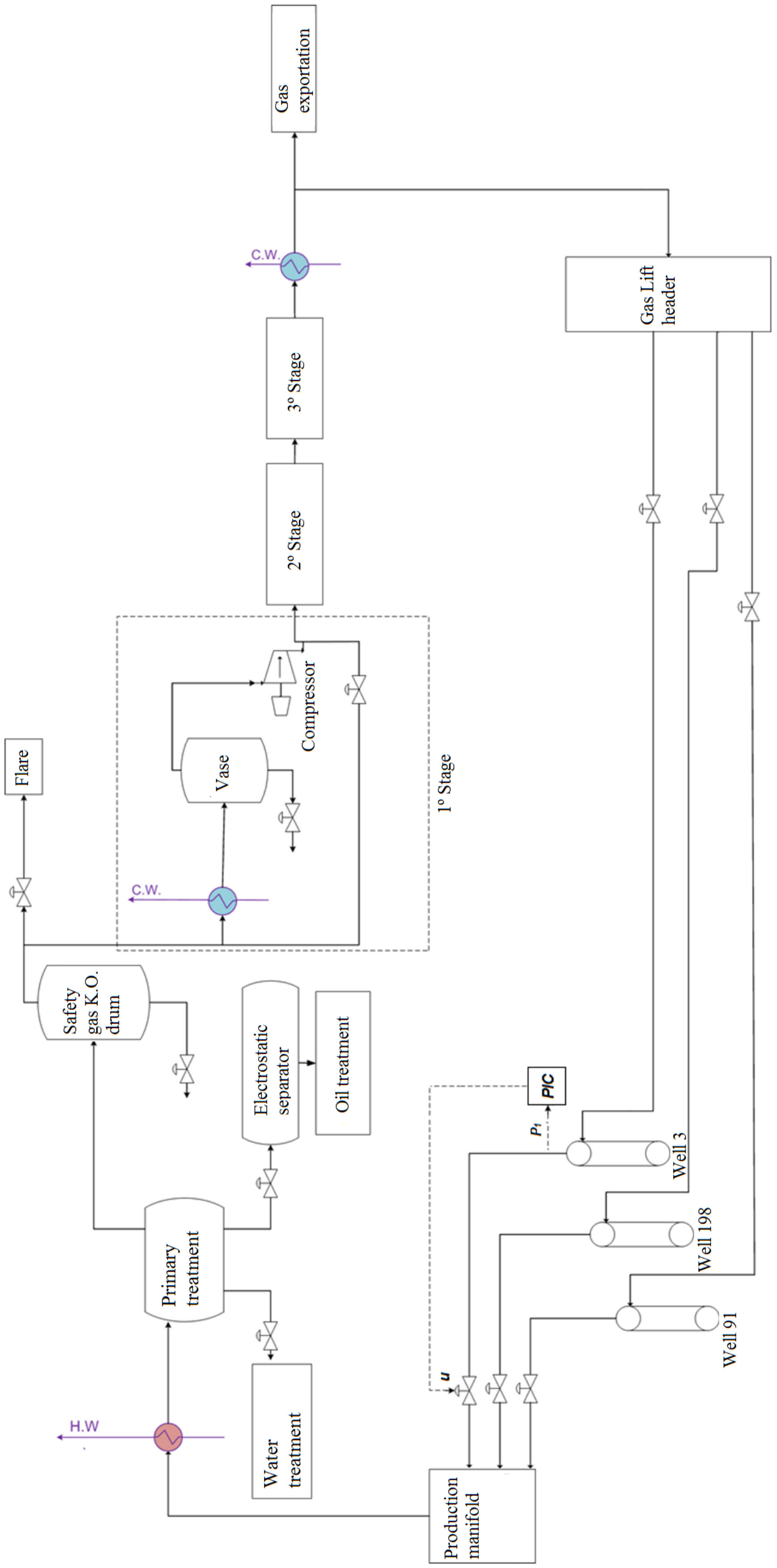


Figure II 5: Offshore oil production flow chart.

To operate the system, a set of equipment and instruments is controlled to maintain the needed pressures, flows, temperatures and levels. If some of the process devices do not operate as expected, the process starts to operate in an abnormal condition and its deviations may lead to undesirable consequences, such as out-of-specification oil, out-of-specification water, changes in the production capacity and so on.

3.2.2. Mathematical modeling

The building of a phenomenological model to represent the process presented in Figure 5 requires hard work. Just as referred latter, the process simulation is widely applied for different process design purposes, it being possible to employ the same built model for safety analysis. In this case the phenomenological model of the described process was built with the contributions of several studies (Ribeiro, 2012) for different purposes, which include the evaluation of the economic benefits of employing slugging flow advanced control (Bendia, 2013). Thus, there was no need to build a new phenomenological model, since it had already been implemented in the EMSO (Soares and Secchi, 2013), a dynamic process simulator with simultaneous resolution.

The process model was built to allow the analysis of the process dynamic and can be divided on subgroups that embrace high detailed models just as the production well, the production line (riser), the three-phase separator, the compression cycle, among others complementary models. Different controls in closed loop (the pressure in the risers, the level of water and oil in the three-phase separator, to name some) were implemented in order to simulate the real process behavior in normal condition. Given that, the simulation of the abnormal condition could be made considering the most accurate model to represent the normal operation condition. For more information about the process model see Thomaz (2017), Bendia (2013) and Ribeiro (2012).

It is important to note that widely used commercial process simulators present some restrictions on process modeling, as the sequential procedure or the “closed box” that assembles some generic phenomenological model to be used to different kind of applications. In fact, these drawbacks may lead to some difficulties during process modeling and resolution with traditional simulators. At this point, the features of the EMSO process simulator should be highlighted, since it provides a framework with open code in which the modeler can change or model the specificity process characteristic according to his/her analysis goal. Then, in fact, despite the suitable tools for the process simulation of abnormal process behaviors are already available for the industrial community, this information should be fomented in order to turn the proposed procedure widespread applied.

3.2.3. Simulations: Normal operation

For the normal operation, the study considered the dynamic behavior of all the equipment and devices, the continuum production of the three wells and an efficient quality control of the produced oil, analyzed by the BSW (basic sediments and water), and of the produced water, analyzed by the OGC (oil and grease content). To understand the process's abnormal behavior, the process variables presented in Table 14 were chosen to be analyzed, and Figure 6 shows their normal values.

Table II 14: Chosen process variables.

Process variables	*Variables description*
F_{gas}	Total gas flowrate production
F_{water}	Total water flowrate production
F_{oil}	Total oil flowrate production
P_{header}	Pressure at the production manifold header
OGC	Oil and grease content
BSW	Basic sediments and water
$F_{flaregas}$	Total gas flowrate relieved to the flare

3.2.4. Proposed hazard analysis

In this example the inappropriate opening of the flare relief valve, located just after the safety gas K.O. drum and before the flare system, was chosen as the device malfunction to be analyzed. The valve is designed to relief gas to the flare to maintain the downstream pressure lower than 10.1×10^5 Pa (10 atm). In the normal condition, the valve downstream pressure is lower than 10 atm, and then the valve is closed normally. The dynamic simulation considered the normal operation until 1000 seconds, when a 40% inappropriate opening of the flare relief valve was imposed. The dynamic simulation was continued until 3600 seconds to identify the consequent dynamic process behavior. The behavior of the chosen process variables (Table 14) is shown in Figure 6.

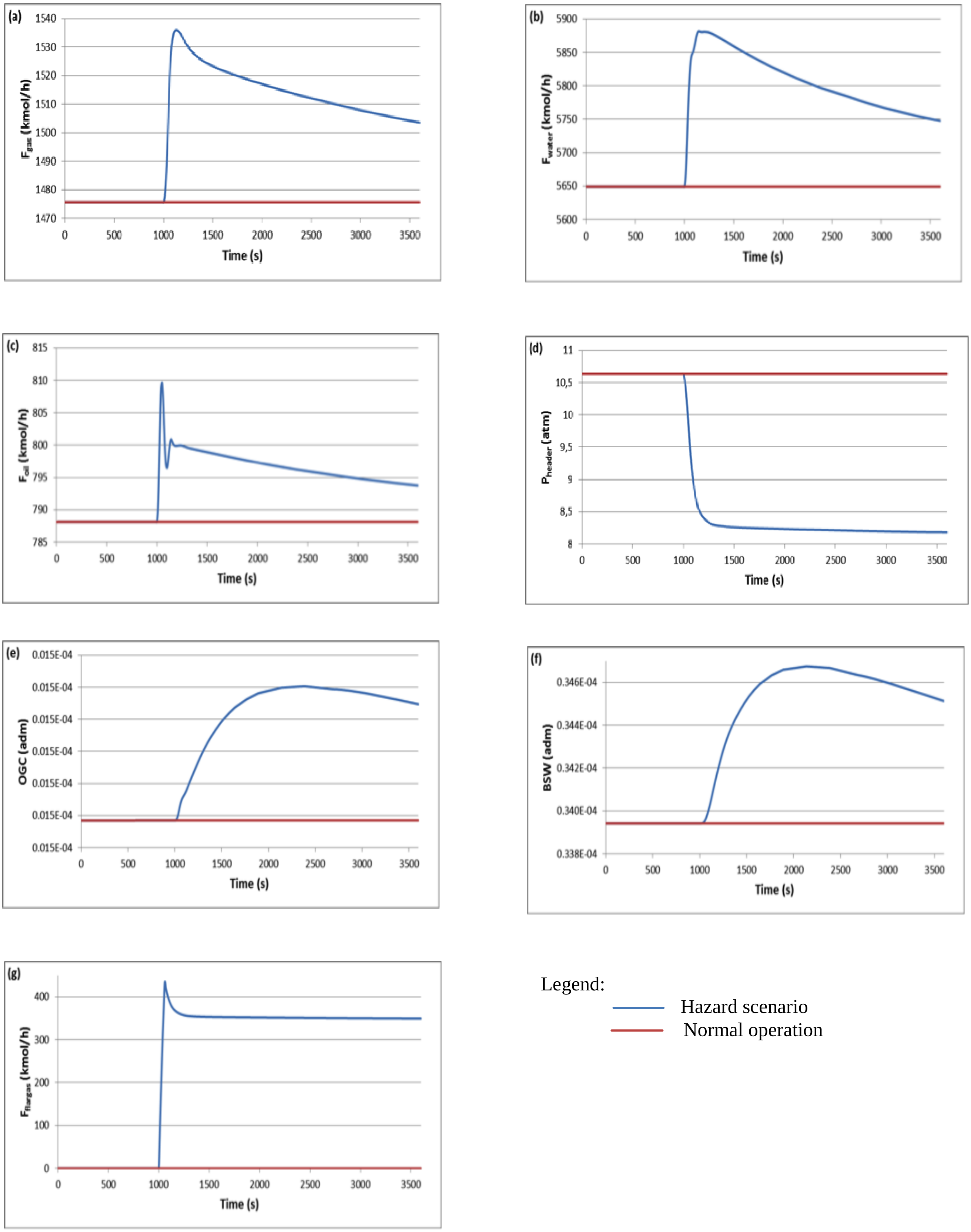


Figure II 6: (a) F_{gas} (kmol/h) – total gas flow rate production; (b) F_{water} (kmol/h) – total water flow rate production; (c) F_{oil} (kmol/h) – total oil flow rate production; (d) P_{header} (atm) – pressure at the production inlet header; (e) OGC (adm) – oil and grease content; (f) BSW (atm) – basic sediments and water; (g) $F_{flaregas}$ (kmol/h) – total gas flow rate relieved to the flare.

It can be noted in Figure 6 that all the analyzed variables suffered deviation with dynamic behavior given the simulated device malfunction, and some of them did not reach their steady-state condition is 3600 seconds. The analyzed scenario reduces the manifold pressure (Figure 6 (d)), increases the production of gas, water and oil (Figure 6 (a), (b) and (c)) and increases the oil (BSW) and water (OGC) contamination (Figure 6 (e) and (f)); such oil and water contamination could be even greater without the control system. The quantitative and time-dependent deviation analysis identified a large amount of out-of-specification oil and water delivered to their downstream system, which could not be designed to handle such a scenario. Table 15 shows the results of this scenario simulation and heuristic analysis, in which the deviation values were picked at 2000 seconds of the simulation.

Table II 15: Offshore oil production – Flare valve malfunction.

<table>
<tr><td colspan="11"><b>System under study:</b> Off shore oil production</td></tr>
<tr><td colspan="11"><b>Device:</b> Flare valve</td></tr>
<tr><td rowspan="3"><b>Device malfunction</b></td><td colspan="10"><b><i>Simulation results analysis</i></b></td></tr>
<tr><td colspan="3"><b>Variable deviation information</b></td><td colspan="7"><b>Deviation safeguards</b></td></tr>
<tr><td colspan="2"><b>Variable identification and normal value</b></td><td><b>Value under deviation</b></td><td><b>Displayed variable</b></td><td colspan="2"><b>Ala rms</b></td><td colspan="2"><b>Automatic means</b></td><td colspan="2"><b>Possibility of human actions</b></td></tr>
<tr><td rowspan="11">Valve open (40%)</td><td colspan="2">F_{gas} = 1475.68 kmol/h</td><td>1517.02 kmol/h</td><td>Yes</td><td colspan="2">No</td><td colspan="2">No</td><td colspan="2" rowspan="7">Yes. The displayed variables allow the identification of hazard behavior.</td></tr>
<tr><td colspan="2">F_{water} = 5649.03 kmol/h</td><td>5820.40 kmol/h</td><td>Yes</td><td colspan="2">No</td><td colspan="2">No</td></tr>
<tr><td colspan="2">F_{oil} = 788.12 kmol/h</td><td>797.32 kmol/h</td><td>Yes</td><td colspan="2">No</td><td colspan="2">No</td></tr>
<tr><td colspan="2">P_{header} =10.63 atm</td><td>8.23 atm</td><td>Yes</td><td colspan="2">No</td><td colspan="2">No</td></tr>
<tr><td colspan="2">OGC = 0.00151</td><td>0.00153</td><td>No</td><td colspan="2">No</td><td colspan="2">No</td></tr>
<tr><td colspan="2">BSW = 0.03394</td><td>0.03466</td><td>No</td><td colspan="2">No</td><td colspan="2">No</td></tr>
<tr><td colspan="2">$F_{flaregas}$ = 0.0 kmol/h</td><td>351.81 kmol/h</td><td>Yes</td><td colspan="2">No</td><td colspan="2">No</td></tr>
<tr><td colspan="10"><b><i>Hazard heuristic analysis</i></b></td></tr>
<tr><td rowspan="2"><b>Further consequences</b></td><td colspan="2" rowspan="2"><b>Consequence safeguards</b></td><td colspan="6"><b>Risk assessment:</b> Production</td><td rowspan="2"><b>Notes, observations, recommendations</b></td></tr>
<tr><td colspan="2"><b>Frequency</b></td><td colspan="2"><b>Severity</b></td><td colspan="2"><b>Risk</b></td></tr>
<tr><td>High production of oil and water out of specification</td><td colspan="2">Advanced process control system</td><td colspan="2">3</td><td colspan="2">4</td><td colspan="2">Marginal</td><td>Obs.: Further consequences to the downstream systems.</td></tr>
</table>

4. CONCLUSIONS

In this work a new procedure for the identification and analysis of hazardous process deviation based on process simulation was proposed, resulting in the following main achievements:

- The employment of an adequate sequence of cause and consequence events to manage hazard deviation analysis, which requires the characterization of a hazard scenario as device malfunctions;

- The analysis of the process abnormal behaviors caused by all possible system device malfunctions leads to a complete study of the process deviations;
- The employment of process simulation is necessary to understand the non-linearities and dynamic behaviors of the process and to allow the quantification of the deviations, improving the quality of the process deviation analysis results;
- The separation of the computer-aided and heuristic consequence analysis. The "simulation result analysis" identifies and analyzes deviations with advanced computational tools, and the "hazard heuristic analysis" identifies and analyzes further consequences of the deviations with expert opinion to cover hazard identification and risk analysis that cannot be modeled computationally;
- A unique device malfunction can lead to several deviations; consequently, several undesirable consequences can be identified and undergo risk assessment;
- The process hazard behaviors presented in the proposed table can be used for real-time failure diagnosis in real plants, enhancing the safety of their daily operation.

The main characteristics of the proposed procedure consist of: (i) identifying the hazard scenario as a device malfunction, (ii) using process simulation to identify and analyze process deviations and (iii) analyzing the results of the simulation with a multidisciplinary group of specialists.

Comparing the proposed procedure with the traditional HAZOP, which also analyzes process deviations, (i) the steps followed are more coherent with real process abnormal behavior; (ii) the understanding of the process deviations is more accurate; (iii) the time required for heuristic analysis is shorter; and (iv) the results assemble a wider range of abnormal conditions with a lower number of scenarios.

Furthermore, given the current importance of the process simulation research area, its employment for safety purposes is the future of PHAs. In addition, given the proposed procedure, the use of computational software enables the automation of the "simulation result analysis," which is the main objective of "expert system" HAZOP research.

5. ACKNOWLEDGMENTS

The present work was accomplished with the support of CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brasil and CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil.

6. REFERENCES

AIChE, Guidelines for chemical process quantitative risk analysis (2th ed.). New York, 2000. Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Bartolozzi V., Castiglione L., Picciotto A., Galluzzo M., Qualitative models of equipment units & their use in automatic HAZOP analysis. Reliability Engineering & System Safety 70 (2000) 49–87.

Bendia, R. M., Economic evaluation of control strategies for slug flow in the separation process of offshore platforms, Master dissertation (in Portuguese). Electrical Engineering Program – COPPE, Universidade Federal do Rio de Janeiro, Brazil, 2013.

Boonthum N., Mulalee U., Srinophakun, T., A systematic formulation for HAZOP analysis based on structural model. Reliab. Eng. Syst. Saf. 121 (2014) 152-163.

Bureal Veritas, 2007, Quantified Risk Assessment Training Course Manual (Offshore Oil & Gas).

Chiacchio, F.; Compagno, L.; D'Urso, D.; Manno, G.; Trapani, N., 2011, Dynamic fault tree resolution: A conscious trade-off between analytical and simulative approach, Reliability Engineering and System Safety, 96, 1515-1526.

Chung L., Chang C., Petri-net models for comprehensive hazard analysis of MOCVD processes. Computers and Chemical Eng. (2011) 35, 356-371.

Cocchiara M., Bartolozzi V, Picciotto A, Galluzzo M., Integration of interlocks system analysis with automated HAZOP analysis. Reliability Engineering & System Safety 74 (2001) 99-105.

Crowl D. A., Louvar J. F., Chemical Process Safety Fundamentals with Applications. (2th ed.). New Jersey, 2002. Prentice Hall International Series in the Physical and Chemical Engineering Sciences.

Cui L., Zhao J., Zhang R., The integration of HAZOP expert system and piping and instrumentation diagrams. Process Saf. Environ. Prot. 88 (2010) 327–334.

Demichela M., Camuncoli G., Risk based decision making. Discussion on two methodological milestones. J. of Loss Prevention Ind. 28 (2013) 101-108.

Demichela M., Marmo L., Piccinini N.,Recursive operability analysis of a complex plant with multiple protection devices, Reliab. Eng. Syst. Saf. 77 (2002) 301–308.

Dunjó J., Fthenakis V., Vílchez J. A., Arnaldos J., Hazard and operability (HAZOP) analysis. A literature review. J. of Hazard. Mater. 173 (2010) 19-32.

Eizenberg S., Shacham M., Brauner N., Combining HAZOP with Dynamic Process Model Development for Safety Analysis. 16th European Symposiumon Computer Aided Process Engineering and 9th International Symposium on Process Systems Engineering (2006a) 389-384.

Eizenberg S., Shacham M., Brauner N., Combining HAZOP with dynamic simulation - Applications for safety education. J. Loss Prev. Process Ind. 19 (2006b) 754–761.

Guimarães A. C. F., Lapa C. M. F., Hazard and operability study using approximate reasoning in light-water reactors passive systems. Nucl. Eng. Des. 236 (2005) 1256-1263.

ISO-5167-2. Measurement of fluid flow by means of pressure differential devices inserted in circular-cross section conduits running full. Part 2: Orifice Plates. Brussels, 2003. European Committee For Standardization.

Kenneth W. D. The FMEA Pocket Handbook. (1th ed.). USA, 2004. Kenneth W. Dailey.

Khan F. I., Abbasi S. A., Mathematical model for HAZOP study time estimation. J Loss Prev Process Ind 10(4) (1997) 249–57.

Kletz T. A., Hazop-past and future. Reliab. Eng. Syst. Saf. 55 (1997) 263-266.

Labovsky J., Svandova Z., Markos J., Jelemensky L., Model-based HAZOP study of a real MTBE plant. J. of Loss Prevention Ind. 20 (3) (2007) 230-237.

Lawley H. G., Operability studies and hazard analysis, Chem. Eng. Prog. 70 (4) (1974) 45-56.

Leone H., A knowledge-based system for hazard studies – The Knowledge representation structure. Computers & Chemical Eng. 20 (1996) 269-274.

Li S., Bahroun S., Valentin C., Jallut C., De Panthou F., Dynamic model based safety analysis of a three-phase catalytic slurry intensified continuous reactor J. of Loss Prevention Ind. 23 (2010) 437-445.

Mannan, S., Lee's Lost Prevention in the Process Industries – Hazard Identification, Assessment and Control, Vol. 1, 3rd ed., Oxford: Elsevier Butterworth–Heinemann;, 2005.

McDermott R. E., Mikulak R. J., Beauregard M. R., The basic of FMEA (2nd ed.). New York ,Usa (2009). CRC Press Taylor & Francis Group.

Ramzan N., Compart F., Witt W., Methodology for the Generation and Evaluation of Safety System Alternatives Based on Extended Hazop. AlChe 26 (1) (2006) 35-42.

Raoni R., Secchi A. R., Biscaia E. C., *Novel method for looped pipeline network resolution*. Computers and Chemical Engineering http://dx.doi.org/10.1016/j.compchemeng.2016.10.001.

Ribeiro, C. H. P., Multivariable predictive control on platforms for production of oil with quality constrains, Master dissertation (in Portuguese). Electrical Engineering Program – COPPE, Universidade Federal do Rio de Janeiro, Brazil, 2012.

Shacham M., Brauner N., Cutlip M. B., Open architecture modelling and simulation in process hazard assessment. Computer & Chemical Engineering 24 (2004) 415–421.

Siu, N., Risk assessment for dynamic systems: An overview. Reliability Engineering and System Safety 43 (1994) 43-73.

Soares, R. P., Secchi, A. R., EMSO: A new environment for modelling, simulation and optimization, Computer Aided Chemical Engineering, 14 (C) (2003), 947-952.

Srinivasan R., Venkatasubramanian V., Automatic HAZOP analysis of batch chemical plants Part I: the knowledge representation framework. Computer & Chemical Engineering 22(9) (1998a) 1345–55.

Srinivasan R., Venkatasubramanian V., Automatic HAZOP analysis of batch chemical plants Part II: Algorithms and application. Computer & Chemical Engineering 22(9) (1998b) 1357–70.

Svandova Z., Jelemensky L., Markos J., Molnar A., Steady states analysis and dynamic simulation as a complement in the HAZOP study of chemical reactors. Process Saf. Environ. Prot. 83(B5) (2005) 463-471.

Swann C. D., Preston M. L., Twenty-five years of HAZOPs. J. Loss Prev. Process Ind. 8(6) (1995) 349–53.

Thomaz, D. M., Multivariable Predictive Controller Strategy In Pre-Salt Gas Compression System, Master dissertation (in Portuguese). Chemical Engineering Program – COPPE, Universidade Federal do Rio de Janeiro, Brazil, 2017.

Tyler B. J., HAZOP study training from the 1970s to today. Process Saf. Environ. Prot. 90 (2012) 419-423.

Wang F., Gao J., A novel knowledge database construction method for operation guidance expert system based on HAZOP analysis and accident analysis. J Loss Prev Process Ind 25 (2012) 905-915.

CHAPTER III - LIKELIHOOD ESTIMATION

Article submitted to Reliability Engineering and System Safety at 19/01/2018.

PROCEDURES TO MODEL AND SOLVE PROBABILISTIC DYNAMIC SYSTEM PROBLEMS

Rafael Raoni[a], Argimiro R. Secchi[a]

[a] Chemical Engineering Program-COPPE, Universidade Federal do Rio de Janeiro, Cidade Universitária, Centro de Tecnologia, 21941-914 Rio de Janeiro-RJ, Brasil
E-mail addresses: rbritto@peq.coppe.ufrj.br (R. Raoni), arge@peq.coppe.ufrj.br (A. R. Secchi),
Corresponding author e-mail address: rbritto@peq.coppe.ufrj.br (R. Raoni)

Abstract: Probabilistic Safety Assessment (PSA), characterized by process-behaviours modelling and event likelihood calculation, has great importance for quantitative risk evaluation. PSA presents some difficulties for implementation, mainly when the analysis of a dynamic process is required. In this work, a set of procedures to formulate and solve Probabilistic Dynamic System Problems (PDSPs) is presented. Such procedures explain how events should be modelled and connected with each other to build a process model that makes it possible to answer two main questions: (i) What is the discrete probability of occurrence of a specific process event? And, given its occurrence (ii) What is the distribution of event time to occurrence? After answering these questions, the event-occurrence probability in a specific length of time, which is the main goal of PSA, is easily calculated. To explain the proposals, one PDSP is solved: the pressure change in a vessel caused by failure of two valves.

Keywords: Probabilistic Safety Assessment (PSA); Probabilistic Dynamic System Problem (PDSP); Monte Carlo simulation; Deterministic and stochastic modeling; Risk assessment.

1. INTRODUCTION

Risk assessment can be characterized as identifying (i) the possible accident scenarios, (ii) the consequences, and (iii) the likelihood of these scenarios [25]. After the identification of scenarios, a quantitative likelihood analysis normally requires analysis of a dynamic system with stochastic behaviour, which can be modelled and solved by several different techniques [12]. Nevertheless, Probabilistic Safety Assessment (PSA) has gained importance in several technological areas, strongly influencing the design and operation of complex systems [21]. Amendola (1981) [3], studying nuclear reactors, was the first to propose accident-sequences likelihood analysis using a system dynamic model [2]. Roughly described, PSA aims to estimate the probability of occurrence of undesired process events. For such an estimation, two main evaluation classes may be identified: (i) the static model and (ii) the dynamic state-space model [10], which are mostly employed for probabilistic risk and reliability/profitability estimation, respectively.

Event Tree (ET) and Fault Tree (FT) are techniques classified as static models that represent scenarios or systems under study using, respectively, basic probability theory and Boolean algebra [19]. Despite not be suitable for dynamic system behaviour [25], FT is the most frequently used quantitative technique for accident-scenario likelihood assessment in industry [10, 17, 25]. To deal with dynamic systems, dynamical Fault Tree (DFT) has introduced dynamic gates to compute the dependence of occurrence time between events and has gained attention for solving safety-critical systems [14]. Currently, the procedure is employed when deterministic and stochastic system behaviours are mixed into the problem [7, 16, 24], requiring great efforts in modelling [20].

Unlike static model procedures, methodologies applied to dynamic reliability do not model systems or scenarios by a generic representation scheme [19]. Such methodologies use state-space evaluation, which allows modelling of system transitions whose time dependency behaviours are important [25]. Among several representations, state transition diagrams, based on Markov models [10], have been popular for many decades. The representation employs diagrams of the evolution of the system’s state transition, with nodes denoting states and arrows denoting transitions to formulate the state equations [19]. Time is an explicit variable, making it possible to cover time-dependent parameters, and the problem is solved by analytical resolution, making it possible to calculate the probabilities of rare event sequences [25]. Despite that, the unpractical identification of states, transitions and probabilities, and also the problem of dealing with complex systems and the exponential explosion of states lead to unmanageable problems [12, 19, 25]. Furthermore, all of the techniques introduced generate models based on description of the qualitative behaviour of the system, making them an inadequate model for some system behaviours [8].

As described by Devooght and Smidts (1996) [12], the Champman-Kolmogorov equation can also be used to mix probabilistic and deterministic dynamic analyses through to solve PSA problems. The state equations, which represent the temporal evolution of physical variables and their links with reliability parameters [5], are solved analytically, and the human and control error can be included [12]. Despite wide applicability and useful results, difficulties are faced when trying to solve high-dimensional problems based on realistic circumstances, making the application hard to use for probabilistic dynamic system problems (PDSPs) [18].

To overcome these analytical problem resolution difficulties to solve PDSP, probabilistic methods, such as the Monte Carlo (MC) procedure [20], may be employed to solve the same problem [5, 18]. The application of MC to solve PDSP leads to the highest freedom for problem modelling and resolution, and does not require any specific representation of the system. Furthermore, MC is insensitive to the system complexity and dimension, allowing the use of any probability density function, non-fixed failure rate, interactions between components, and so on. These characteristics make MC the best approach for solving realistic systems [9], being limited by the analyst's ability to model the possible behaviours of the system [25]. Normally, applying MC requires, beside the system model and state specifications, the system mission time (maximum history time), the definition of the system failure model, and the number of histories to be simulated in order to obtain a representative statistical result [20, 21]. Difficulties arise in MC when the system under study is very reliable, since, to obtain meaningful results, a large number of system histories and consequent large computational effort are needed [2, 26]. However, biasing techniques may be applying to deal with the difficulty of solving very reliable problems [18, 21].

Other probabilistic techniques have been developed and are in widespread use for PSA, such as Dynamic Reliability Block Diagram (DRBDs), Bayesian Network, Stochastic Petri Network, GO-FLOW, and DYLAN, among others [1, 19, 20, 22]. This large number of techniques highlights the wide range of possibilities for modelling and solving scenario-likelihood problems. As reported at NUREG-0492 (1981) [23], in the scenario likelihood problem, the greatest emphasis should be placed on assuring that the system model provides the most accurate representation of reality. In this sense, it is observed that one difficulty in obtaining the most representative model is the restrictions imposed by the problem resolution procedures of existing methods, such as FT and ET static pictures, DFT state space explosion, difficulty in solving the formulated high-dimensional problem for some realistic application of the Champman-Kolmogorov equation, the large number of MC histories needed for the resolution of very reliable system, and so on. Thus, the model-resolution relation is one of the most important features that must be analysed during the use of these existing techniques and, in this sense, procedures to solve PDSP should be improved in order to consider, from a unique perspective, (i) building the model of the system's behaviour, (ii) the problem resolution, and (iii) the representativeness of the obtained results, which must meet the expectations of the solution.

In the present work, a procedure to understand and model dynamic system behaviour is proposed with the aim of achieving better model building, problem resolution, and interpretation of results. To introduce the proposals, two main questions to be answered are highlighted:

(i) What is the probability of occurrence of a specific process event (disregarding any time dependence)?

(ii) Given that the event has occur, what is the time distribution of its occurrence?

To answer these questions, the following procedures are introduced:

- Modelling a continuous dynamic process based on discrete events (state-spaces) that embrace a set of deterministic behaviours, focusing on the desired results for simpler process modelling and resolution
- Representing each event connection by a discrete random variable that defines whether the connection will or will not occur combined with a continuous random variable time dependence;
- Application of the deepness concept, to identify the set of process behaviours in the events, combined with logics to represent the relationship between these identified events;
- The application of MC to allow the highest modelling freedom and the probabilistic problem resolution, setting the absorbing events as a unique process feature that ends the simulated MC history.

In Section 2, procedures for event identification, system modelling, and problem resolution are introduced to obtain answers to both of the abovementioned questions about discrete probability and time distribution of the events occurrence. In Section 3, a case study is modelled and solved to illustrate the proposals and, in Section 4, the conclusions of the work are presented.

2. PROCEDURES

2.1. Event characterization and its interactions

The discretization of real-world continuous behaviour makes in linked events is one of the biggest difficulties for any modelling process. In this work, an event is defined as a state space in which some process behaviour is identified, and making it possible to separate the system’s deterministic from the system’s stochastic behaviours. Due to the fact that, in many domains, system dynamics may be described by deterministic behaviours punctuated by stochastic transitions [6, 8, 13, 19], the idea that a dynamic deterministic behaviour does not needs to be separated into different events should be followed. Therefore, all sequenced deterministic behaviours should be grouped into a unique state space limited by stochastic transitions.

For these event limits, which are points of connection of events, both discrete and continuous random variables must be considered. Continuous random variables, which are characterized by continuous probability distribution functions, should represent the stochastic time to the event occurrence. Furthermore, this time dependency of the event occurrence must be computed already considering the certainty that the event will occur, representing only the randomness of the time to the event occurrence. On the other hand, the discrete random variable of event occurrence is employed to forecast process paths, identifying whether some downstream event will or will not occur in the simulated history. In other words, the discrete random variables lead to process behaviour “instantaneous decisions” determining the path that the process goes, while continuous random variables consider the time dependency of an event occurrence given the defined path.

To link the identified events and build the target process model, some logics may be employed to describe how these events interact with each other. Logics should be understood as a feature that allows the modelling of process behaviour based on interactions between more than two events. Figure 1 shows features for the identification of the events and their connections.

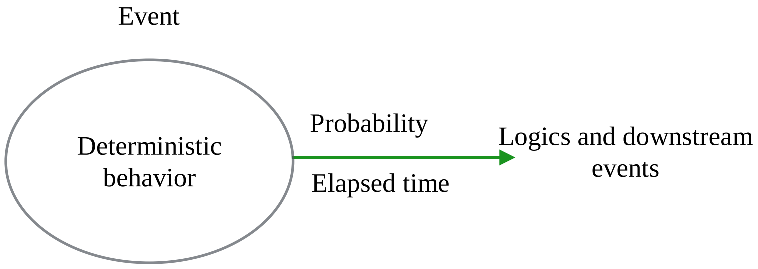


Figure III 1: Process event and connection features.

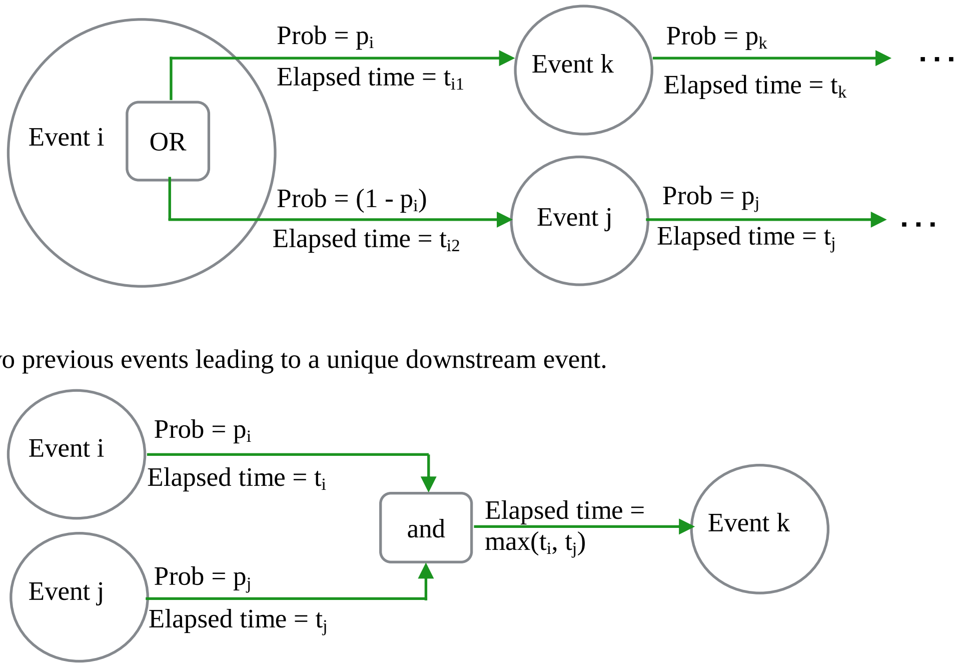
Then, discretization of a continuous probabilistic process based on events that embraces deterministic behaviour limited by continuous and discrete stochastic behaviours, as well as logics relationships, is proposed.

2.2. Process model

To build a process model that characterizes a sequence of events that occurs in continuous time, definitions of: (i) initial and final boundaries of the process (initial and absorbing event), (ii) intermediary events, and (iii) how such events are connected with each other are required. Knowing that this modelling process is subjective, attention should be paid to its representativeness and accuracy.

2.2.1. Event connections and logics

During a process history, time computation is started at the initial event, in which the connections with its downstream events are analysed. Such connections must take into account both cause–consequence instantaneous probability assumptions (how probable it is that the previous event will cause the consequent downstream event?), by employment of discrete random variables; and the time to event transition, which can be a continuous random variable. If, for an intermediate event occurrence, two or more events need to interact, logic should be employed to build their relationship. This proposal makes it possible to build any dynamic and stochastic system behaviour that can also be supported by graphic representation. Figure 2 shows examples of representation of the graphical connections.


Ex.1: Unique event leading to two downstream events.

Ex.2: Two previous events leading to a unique downstream event.

Figure III 2: Examples of graphical representation of event connections.

2.2.2. The deepness concept

To provide more flexibility for modelling, the deepness concept is introduced. Deepness can be understood as the difference between choosing unique data to represent process behaviour and of carrying out deep analysis considering all conditions that could lead to this behaviour. In this sense, the deepness aims to define the level of detail of the event description in front of whole analysed process. The concept is very important for PSA since it directly changes the model size and complexity. When employing deepness to embrace process behaviour in some discrete event, the adequate use of continuous and discrete random variables is needed. In Figure 3, a graphical example to manage discrete and continuous random variables in the deepness concept for PSA model building is shown.

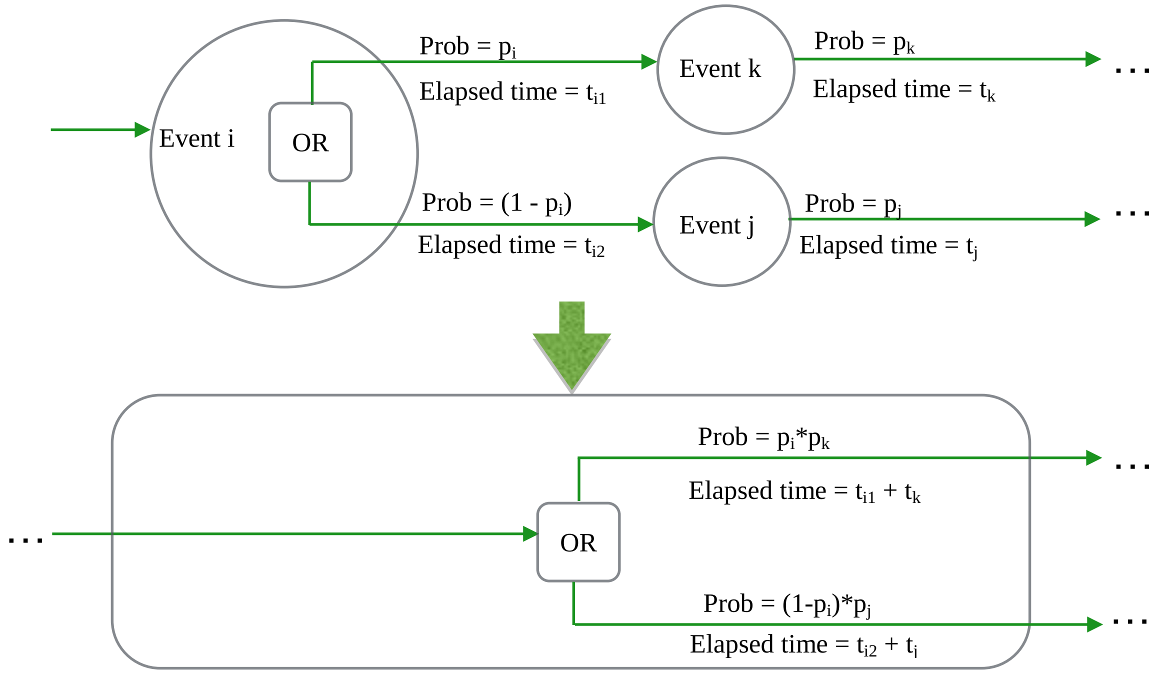


Figure III 3: Example of how to simplify a model by using the deepness concept.

In this sense, after understanding the system to be analysed, the level of detail of the model classifies its deepness. The deepness concept may be related to the level of detail obtained by the *bottom-up* approach for model building, where the system is superficially modelled as detailed until it reaches the desired *deepness*, or by the *top-down* approach, where system modelling starts with highly detailed models of subsystems, or high *deepness*, which will be joined to build the model of the entire system [5]. To allow the better use of the idea, the proposed model deepness can be based on the targeted problem result, available data, or analyst's technical capacity, making no sense to define the best approach (*bottom-up* or *top-down*) to manage model building.

2.2.3. Proposed steps for model building

The system model can be understood as a space in which dynamic behaviours are connected by stochastic connections and detailed according to the desired deepness. The proposed model resembles the state space of the *stochastic hybrid system* (SHS), which comprises discrete and stochastic event transitions based on continuous and dynamic behaviour [13]. Differently from a system model comprising a unique deterministic model connected with a stochastic model [11], the proposals make it possible to build different deterministic models, with occurrences and behaviours dependent on their stochastic inputs, and then to evaluate the variability of their behaviours not only due to the variability of the initial system condition [16, 26] but also due to the system's intrinsic stochasticity. Figure 4 presents the steps for model building.

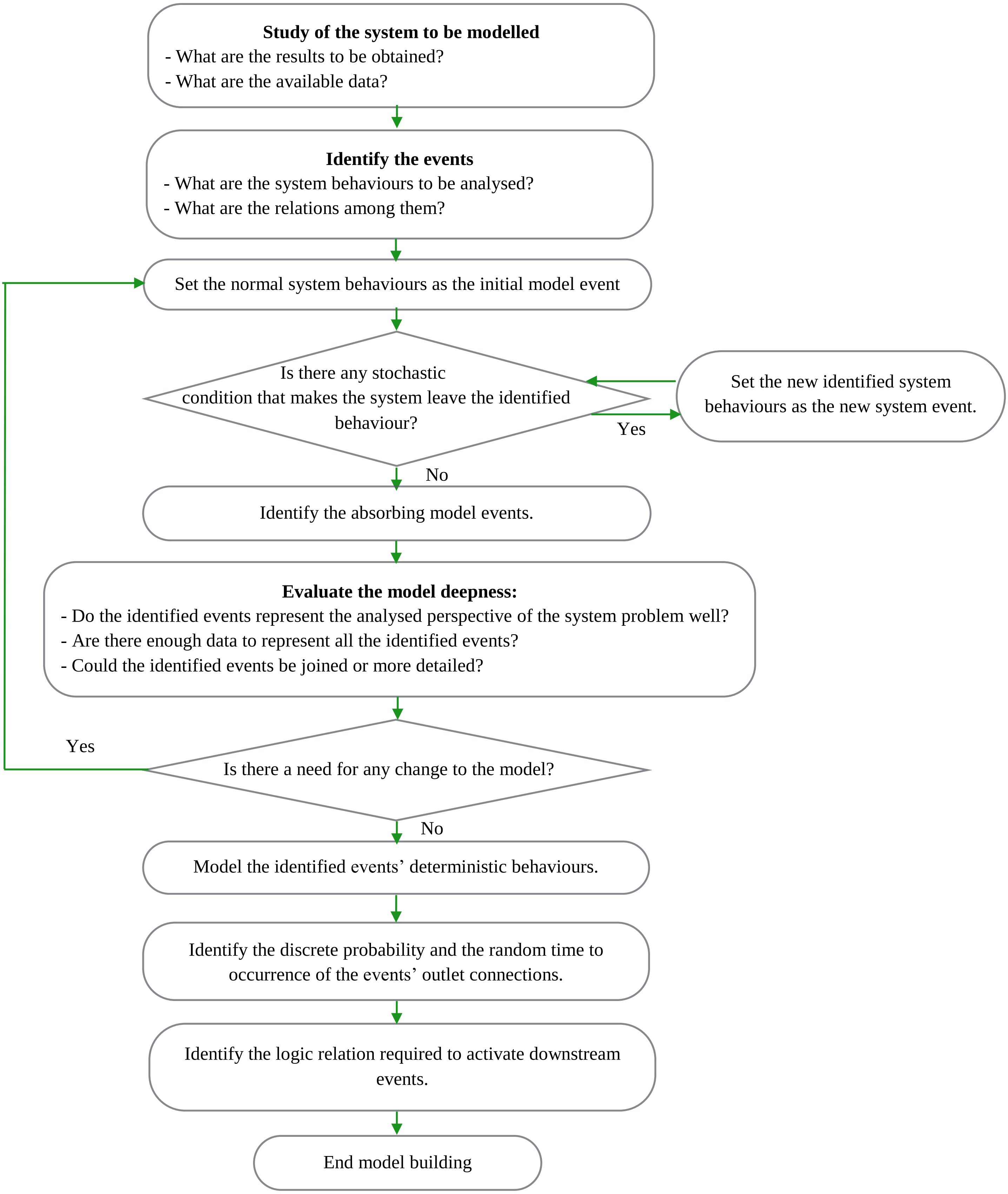

Study of the system to be modelled
- What are the results to be obtained?
- What are the available data?
Identify the events
- What are the system behaviours to be analysed?
- What are the relations among them?
Set the normal system behaviours as the initial model event
Is there any stochastic condition that makes the system leave the identified behaviour?
Yes
Set the new identified system behaviours as the new system event.
No
Identify the absorbing model events.
Evaluate the model deepness:
- Do the identified events represent the analysed perspective of the system problem well?
- Are there enough data to represent all the identified events?
- Could the identified events be joined or more detailed?
Yes
Is there a need for any change to the model?
No
Model the identified events' deterministic behaviours.
Identify the discrete probability and the random time to occurrence of the events' outlet connections.
Identify the logic relation required to activate downstream events.
End model building

Figure III 4: Steps for model building.

Differently from most application of state space representation, the proposal enhances the importance in building the state space from the perspective of process conditions rather than device conditions. Using the deepness concept with discrete and continuous random variables at event connections makes it possible to link detailed subsystem models to form a representation of a complex system as well as simplifications for model representation and resolution based on the process behaviour.

2.3. Problem solving

A difficulty is faced when trying to develop an analytical method capable of obtaining all event times and the number of occurrences of a model based on the proposed assumptions. In this sense, a probabilistic approach, such as the MC procedure, is the most suitable option for resolution. To obtain the random time of the event connection, a non-tendentious random number between 0 and 1 is obtained and the event occurrence time is calculated employing its continuous probability distribution. To obtain the occurrence of the connection based on the discrete random variable, another non-tendentious random number between 0 and 1 is obtained to identify whether or not the downstream event will occur. Furthermore, sometimes, the discrete random connections may be dependent on the process elapsed time, requiring the use of a continuous probability distribution function. The difference between employing a continuous probability distribution to obtain the time as a continuous random variable and the occurrence of a discrete random connection based on process elapsed time is shown in Figure 5, in which the exponential distribution was used.

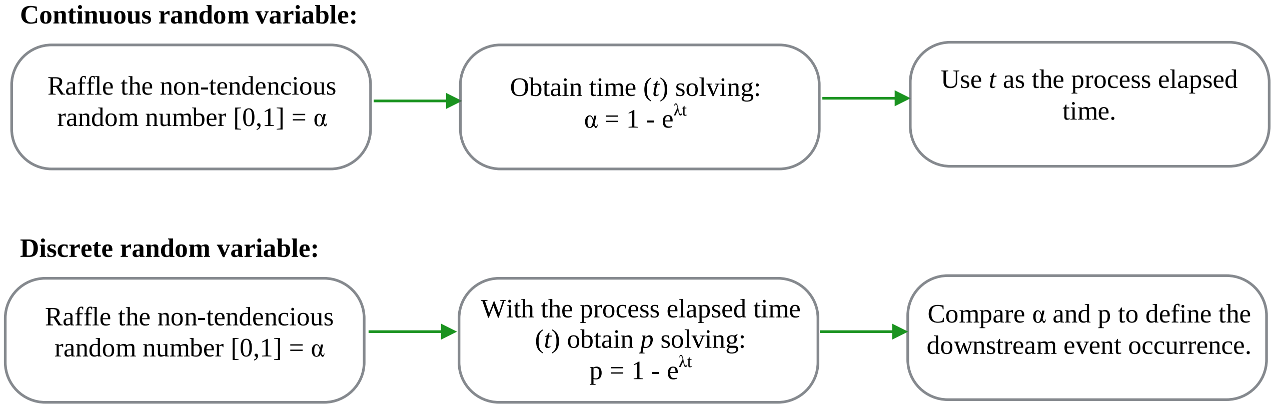

Continuous random variable:
Raffle the non-tendencious random number [0,1] = α
Obtain time (*t*) solving: $\alpha = 1 - e^{\lambda t}$
Use *t* as the process elapsed time.
Discrete random variable:
Raffle the non-tendencious random number [0,1] = α
With the process elapsed time (*t*) obtain *p* solving: $p = 1 - e^{\lambda t}$
Compare α and p to define the downstream event occurrence.

Figure III 5: Application of the continuous probability distribution to solve continuous and discrete random events.

Unlike the usually procedure for solving PDSP by MC, the proposed procedure does not ends the simulated history based on a pre-defined mission time. It is proposed that the unique way to end a simulated history is when an absorbing event occurs. For example, the simulation starts with the system at its initial event, obtaining its entire deterministic behaviour and identifying its outlets that will occur given the discrete probability. Knowing the initial event outlets, the connections that will occur, given related discrete probability, and their times to occurrence, the problem resolution is continued by solving the downstream events. If these downstream events are dependent on more than one event that has previously occurred, their inlet logics should be analysed to evaluate whether and when the event activation will occur to continue the history simulation. The same procedure as already described to solve the first event should be repeated for the activated ones, computing the total elapsed time and which events have occurred. On continuing this procedure until no more events can be solved, which means that absorbing events occur, one process simulation, or history, is finished. To obtain the probabilistic number of occurrence and time to occurrence of all modelled events, the procedure should be repeated as many times as necessary to obtain an accurate result. Figure 6 shows the flow chart that explains how to solve the model built by the proposed procedure.

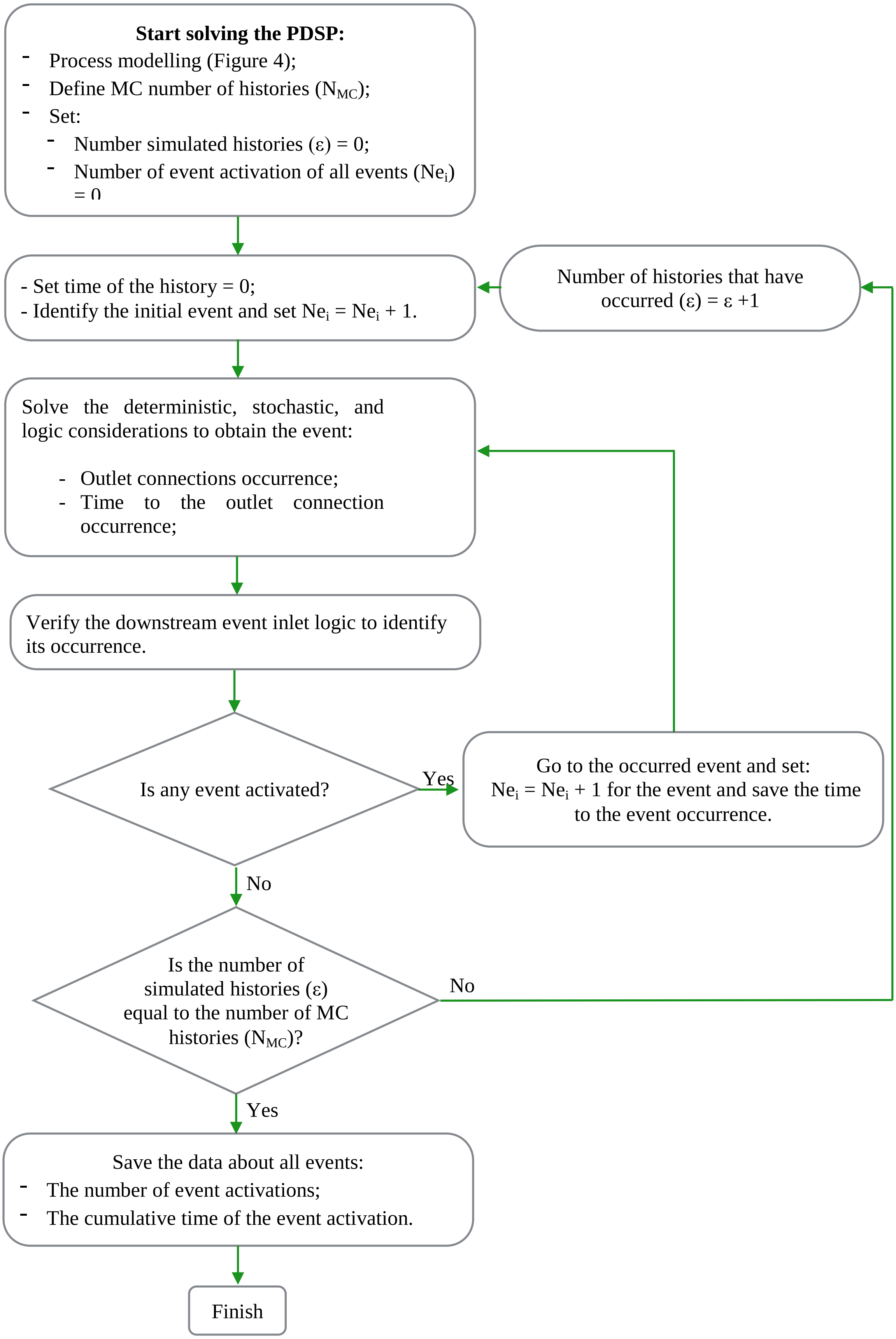

Start solving the PDSP:
- Process modelling (Figure 4);
- Define MC number of histories (N_{MC});
- Set:
- Number simulated histories (ε) = 0;
- Number of event activation of all events (Ne_i) = 0
- Set time of the history = 0;
- Identify the initial event and set $Ne_i = Ne_i + 1$.
Number of histories that have occurred (ε) = ε +1
Solve the deterministic, stochastic, and logic considerations to obtain the event:
- Outlet connections occurrence;
- Time to the outlet connection occurrence;
Verify the downstream event inlet logic to identify its occurrence.
Is any event activated?
Yes
Go to the occurred event and set: $Ne_i = Ne_i + 1$ for the event and save the time to the event occurrence.
No
Is the number of simulated histories (ε) equal to the number of MC histories (N_{MC})?
No
Yes
Save the data about all events:
- The number of event activations;
- The cumulative time of the event activation.
Finish

Figure III 6: Procedure for solving the PDSP.

In Figure 6, the inner loop represents the modelled process behaviour simulation while the outer loop represents the MC iterations. After solving the problem, the most important information to be obtained is the number of activations and the required time of all activation of all evens.

As probabilistic resolutions demand high computational effort, not solving the same computationally expensive deterministic problem repetitively is important to save computational work in problem resolution. In this sense, after the first resolution of the event deterministic behaviour, the results may be further obtained by using a table of data, simplified mathematical model, or process control transfer functions [8]. However, if an deterministic process behaviour in an event is too sensitive with respect to the previously elapsed time of the process and its initial conditions, the study should be done with repetitive resolution of the original deterministic model, together with the stochastic behaviour, to ensure the highest accuracy of the results.

2.4. Interpretation of Results

The proposal mixes different existing probabilistic system analysis procedures, such as logics and discrete probability data employed in FT and ET, and state-space and continuous random time employed in reliability problems. The main objective of that is making it possible to answer two questions posed about: (i) the probability and (ii) time to event occurrence.

Analysing the *i-th* event, its probability of occurrence can be estimated by Equation (1).

$$Pe_i = \frac{Ne_i}{N_{MC}} \tag{1}$$

where Pe_i is the probability of occurrence of event *i*; N_{MC} is the number of process simulations in MC; and Ne_i is the number of times that event *i* has occurred, considering all N_{MC} histories.

After the consideration that an analysed event has already occurred, the obtained elapsed times for the event occurrences can be used to identify a cumulative probability distribution function of its time to occurrence. As shown in Equation (2), by computing cumulatively the number of event occurrences in time intervals, a cumulative distribution equation that best fits these data can be identified.

$$CFD(t_j)_i = \frac{Ne_i\big|_{t=0}^{t=t_j}}{Ne_i} \tag{2}$$

where $CDF(t_j)_i$ is the cumulative distribution value of event *i*, which defines the probability of occurrence of the event *i* between the time 0 and t_j; $Ne_i\big|_{t=0}^{t=t_j}$ is the number of occurrences of event *i* between the times 0 and t_j.

It is important to note that the continuous probability function for an event time to occur, obtained using the Equation (2), does not depend on the probability of occurrence of the event, obtained using the Equation (1). Using these two independent results, the probability of occurrence of the event given a specified time is obtained using Equation (3).

$$Pe(t_j)_i = \frac{Ne_i\big|_{t=0}^{t=t_j}}{N_{MC}} = Pe_i \quad CDF(t_j)_i \tag{3}$$

where $Pe(t_j)_i$ is the probability of occurrence of event *i* in the interval t = [0, t_j].

2.5. Further comments

The constant development of new techniques to solve PDSP shows the importance of the problem and the desire to improve its resolution. When dealing with dynamic behaviours, some methods such as FT and ET are incipient, when dealing with any kind of data, the Markov method presents some restrictions, and when simultaneously dealing with deterministic and stochastic behaviours, the analytical resolution of the Champman-Kolmogorov equation problem is limited and can be unmanageable for some systems. These drawbacks of the existing methods and the need for better interaction between model building and resolution pose the main difficulties in solving PDSP to which the current work proposes a solution. In this sense, an approach with different procedures to formulate and solve PDSP is proposed. However, as the use of an existing method with its restriction is sufficient to solve some kind of problems, the proposal enables the simplification of the analysis by employing just some of the presented procedures. As an example, employing the proposed procedures to solve a PDSP with only discrete random variable at the connections, and without deterministic process behaviour in the events, already makes it possible the obtainment of the probability of occurrence of the modelled events, being it an adequate result for some specific scope. In this sense, the proposals aim to presents procedures to help with PSA problem modelling and resolution being flexible in such way that may or may not be used all together.

It is also important to note that the proposed procedures make the stochastic discrete process behaviour the unique feature that changes the number of the occurrence of the events in all MC histories while the probabilistic distribution of the event time to occurrence represents the probability of occurrence of the event in all time space. With these two separated results, Equation (3) can be used to obtain the probability of occurrence of the event in any time interval, reducing the required number of MC histories for calculation of the probability of rare events. As an example, using $Pe_i = 0.5$ and an exponential probability distribution with $\lambda = 10^{-5}$ failures per year to represent its time to occur, according to Equation (3), the probability of occurrence of the event in one year is 5×10^{-6}. If those data are unknown and the proposed procedure, with 10^5 MC histories, is employed to their obtainment, since only $Pe_i = 0.5$ influences the occurrence of the specified event, probably half of the MC histories (5×10^4) would end in the discussed event, given enough data to fit the exponential probability distribution function of the time to occur with $\lambda = 10^{-5}$ failures per year. However, when employing a probabilistic resolution with a mission time equal to one year, no event occurrence would be expected in all 10^5 MC histories.

It is important to note that, given the probabilistic resolution of the MC, any result present error that is reduced proportionally with the increase of the number of MC histories. In other words, as higher is the MC number of histories lower is the error of the probabilistic MC result. In this sense, given that the discrete probability of occurrence is the unique feature that changes the number of the occurrence of the events in all MC histories, the feature is the unique source of error in the MC resolution.

In the end, the major proposed steps are: (i) identifying events characterized by deterministic behaviours and limited by stochastic connections; (ii) connecting events, employing both discrete and continuous random variables, logics, and the deepness concept; and (iii) solving the model by the MC procedure to obtain the probability of occurrence and the probabilistic distribution curve of the time to occurrence of all events.

3. CASE STUDY: PRESSURIZED VESSEL

A benchmark reliability problem is presented. The problem is related to a pressurized vessel in which the failure of two valves that contributes to a change in the vessel pressure is investigated.

3.1. Problem description

The pressurized vessel problem presented in Labeau et al. (2000) [19] was modelled and solved. The vessel is continuously pressurized from its initial pressure condition (P_0) until it reaches the high-pressure condition (P_h), when valve V1 must be opened to relieve the vessel pressure. The valve V1 has a probability of failure on demand equal to ρ, and its failure leads to a continuous elevation of the vessel pressure until it reaches the critical pressure condition (P_c). The system also contains a second valve (V2), which can eventually open inadvertently, contributing to the elevation of the vessel pressure. Failure of V2 occurs only when the vessel pressure is between the initial and the high-pressure conditions ($P_0 < P < P_h$). When valve V2 is opened and the vessel pressure reaches P_h, even with the V1 is opened, the pressure will rise until the critical condition (P_c). With the V1 opens, the vessel pressure is reduced until it reaches its initial condition (P_0), when V1 is closed without failure. Then, the unique problem-absorbing event is when the vessel reaches its critical pressure, which can occur if V1 fails to open; V2 opens inadvertently; or V2 opens inadvertently and V1 fails to open successively. Figure 7 presents the described process.

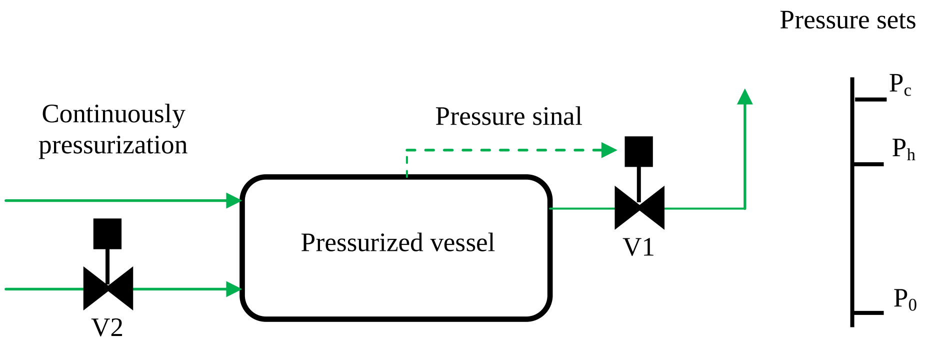


Figure III 7: Pressurized vessel process.

3.2. Problem modelling

The model was built to obtain the probabilities of the absorbing state and its prior events, which are as follows: (E2) V1 fails to open; (E3) V2 opens inadvertently; (E4) V2 opens inadvertently and V1 fails to open successively; and (E5) critical pressure is reached in the vessel. Considering the system's start point as the vessel being pressurized from P_0, the initial event E1 is characterized by the state space in which no failure has occurred, including the deterministic oscillation of the vessel pressure in its normal condition ($P_0 < P < P_h$). Combining stochastic behaviour and logics, the system may remain in the initial event or reach some failure event (E2 or E3) that leads to the absorbing event E5. With failure of V2 (E3) followed by failure of V1 to open when the vessel pressure reaches P_h, the system reaches E4. Such a system model embraces one probabilistic discrete event (failure on demand of V1), one continuous random variable (time to failure of V2), and deterministic behaviour (a change in vessel pressure).

The normal pressurization and the pressure change due to the failures of valves V1 and V2 were modelled as shown in Equation (4), with the parameters shown in Table 1.

$$P(t) = P_i \quad e^{\alpha t} \tag{4}$$

where *P(t)* is the time-dependent pressure in the vessel; P_i is the pressure in the vessel at the moment of the change in the vessel pressurization behaviour; α is the relative vessel pressurization parameter (normal condition, V1 open, or V2 open); and *t* is the time.

Table III 1: Parameters of the pressurized vessel problem.

Parameters	**Value**	**Parameters**	**Value**
P_0 (MPa)	10	Number of MC histories	10000
P_h (MPa)	20	λ (V2 failure rate – failure per hour)	4×10^{-3}
P_c (MPa)	30	ρ (probability of V1 fail to open)	0.05
Parameter of normal vessel pressurization (α)			0.05
Parameter of V1 pressurization (α)			-0.10
Parameter of V2 pressurization (α)			0.06

A graphic representation of the described model is shown in Figure 8 and the descriptions of the discrete and random variables of the model connections are listed in Table 2.

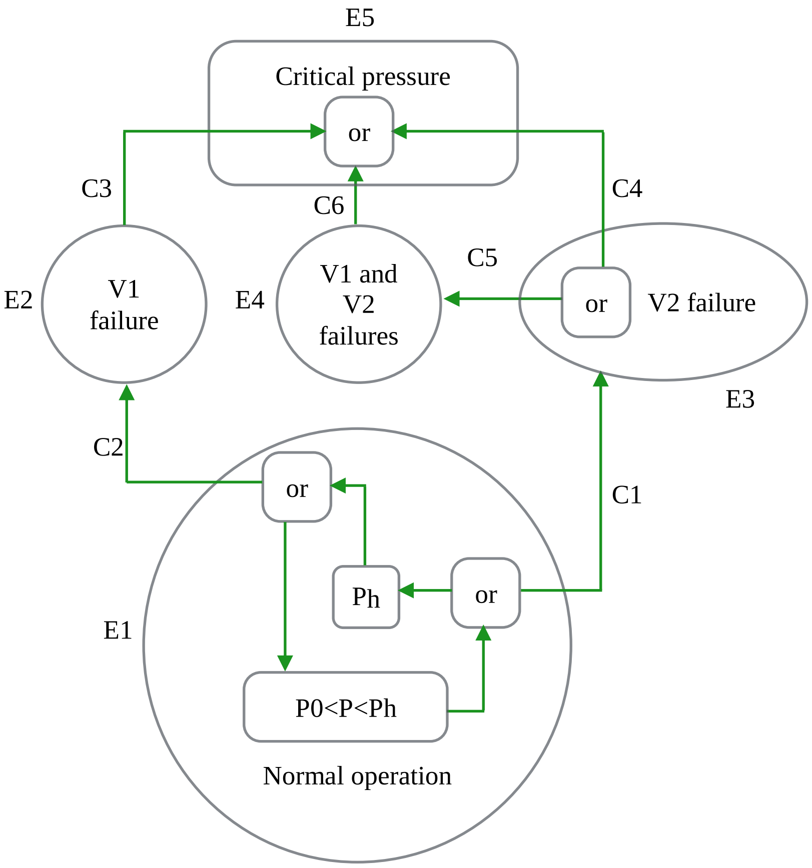


Figure III 8: Graphic representation of the pressurized vessel problem.

Table III 2: Descriptions of the discrete and random variables of the model connections of the pressurized vessel problem.

Connection	**Variable dependence**		**Connection**	**Variable dependence**	
	Continuous	**Discrete**		**Continuous**	**Discrete**
C1	Time (λ) - Random	1**	C4	Time - Deterministic*	$(1-\rho)$
C2	Time - Deterministic*	ρ	C5	Time - Deterministic*	ρ
C3	Time - Deterministic*	1	C6	Time - Deterministic*	1

* Time and pressure as deterministic values.
** Probability equal to one for no random discrete occurrence.

3.3. Problem resolution

The system was modelled and solved in MATLAB® software assuming that the particles are walking through the state spaces according to the MC procedure that follows the steps described in Figure 6. Figure 9 shows examples of the process behaviours, passing through E2, E3, and E4, which lead to the critical pressure E5, in which the points in the Figures 9 (a), (b) and (c) represent the point when the V2 fail (red point in Figure 9 (b) and (c)), the V1 fail (blue point in Figure 9 (a) and (c)) and V1 do not fail after the failure of V2 (green point in Figure 9 (b)). Figure 10 shows the cumulative probability distribution curves of the time to occur of all four events, and Table 3 shows the discrete probabilistic results.

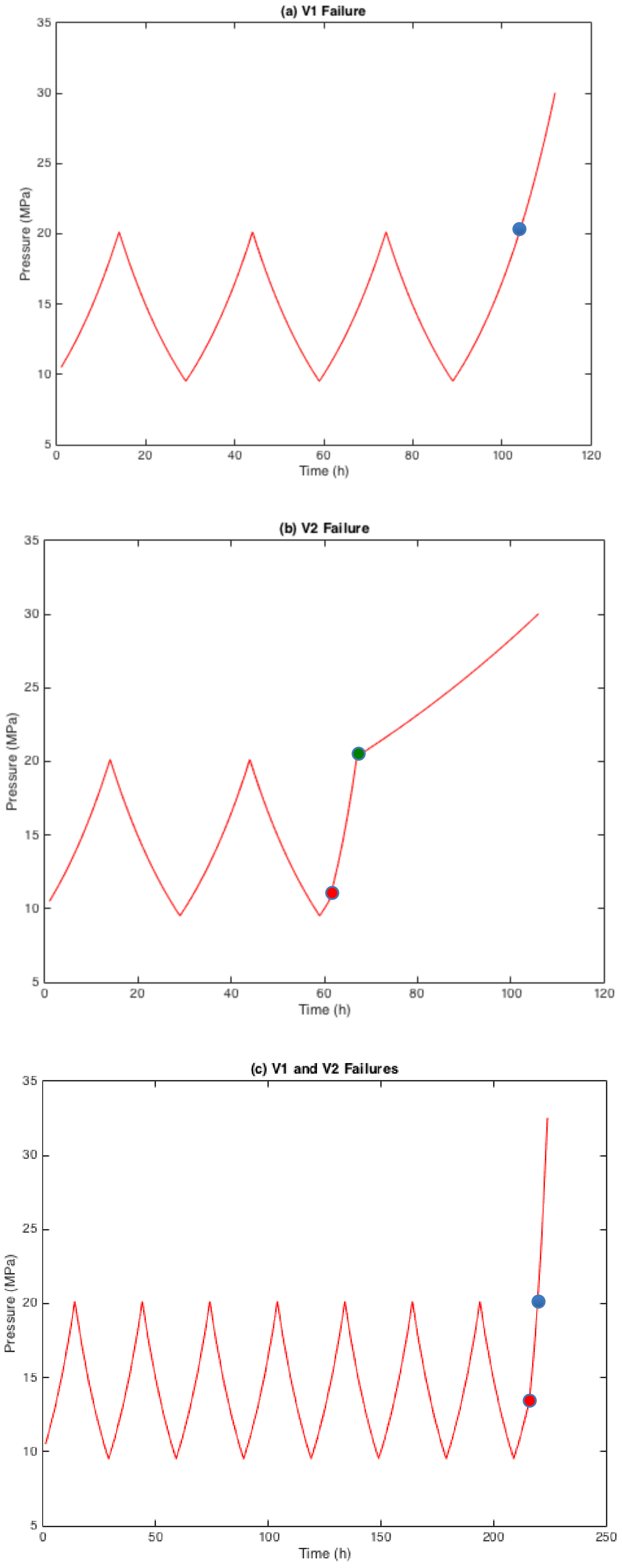
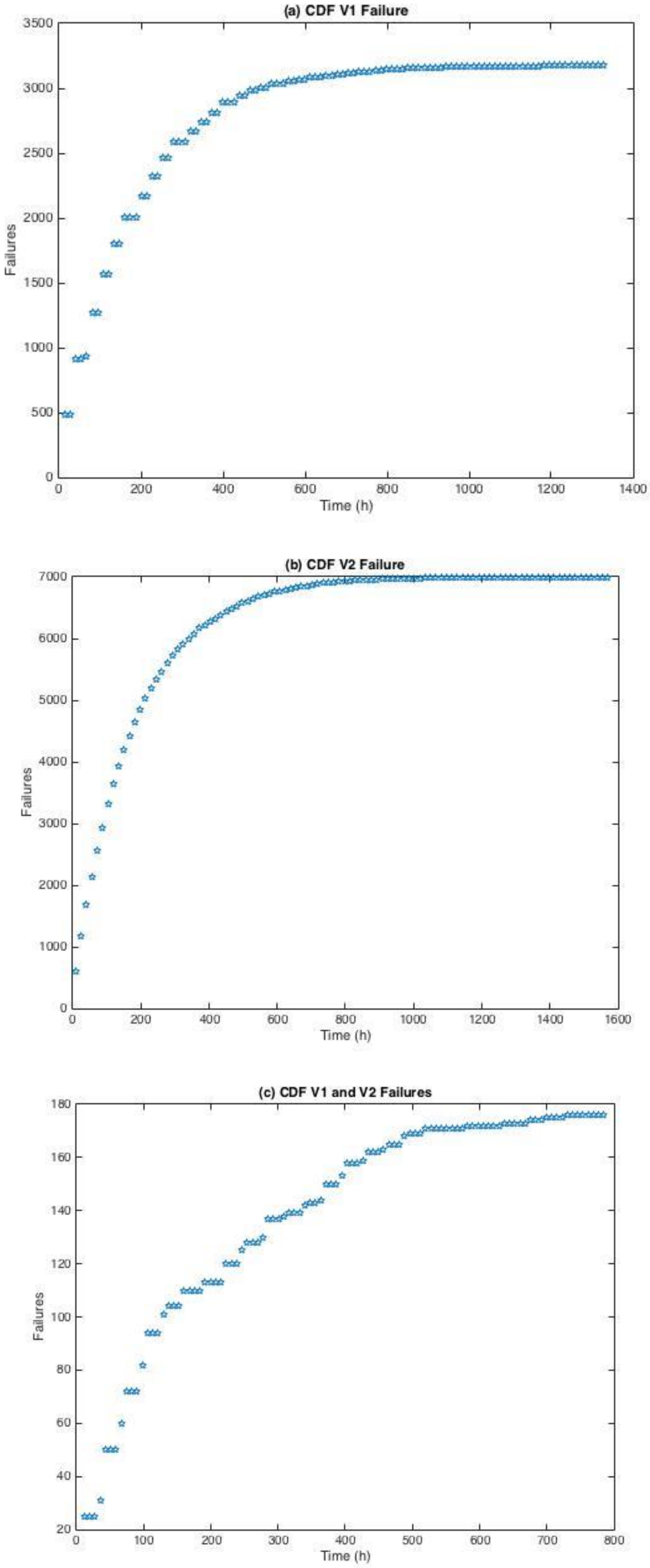


Figure III 9: Possible process behaviours of the pressurized vessel: (a) failure of V1; (b) failure of V2; (c) failures of V2 and V1.



(a) CDF V1 Failure

(b) CDF V2 Failure

(c) CDF V1 and V2 Failures

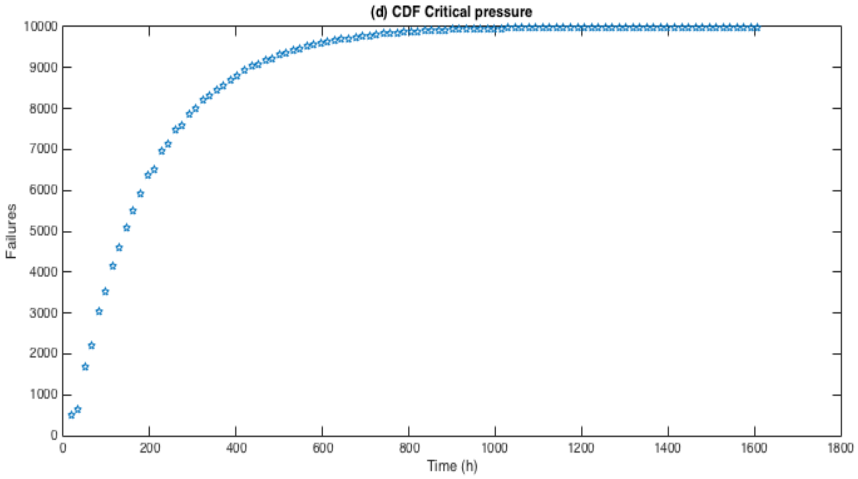


Figure III 10: Cumulative distribution functions of the pressurized vessel: (a) E2: V1 failure event; (b) E3: V2 failure event; (c) E4: V2 and V1 failure event; (d) E5: critical vessel pressure.

Table III 3: Discrete probabilistic results.

MC histories = 10000			
(E2) Number of failure of V1 *	3001	Probability of failure of V1 (%)	30.01
(E3) Number of failure of V2	6999	Probability of failure of V2 (%)	69.99
(E4) Number of failure of V1 and V2	177	Probability of failure of V2 and V1 (%)**	2.53
(E5) Number of critical pressure	10000	Probability of critical pressure (%)	100.00

* Number of failures of V1given the previous non-occurrence of failure of V2.
**Probability of failure of V1 given the occurrence of failure of V2.

3.4. Problem observations and discussion

The graphic representation (Figure 8) makes it possible to visualize the possible paths of the MC histories, helping to understand how the probabilistic information of the events E2, E3, E4, and E5 is calculated. Exemplifying deepness, all the simulated behaviours of the process may be summarized by the cumulative distribution function obtained from Figure 10(d). In this sense, if the problem goal doing a further PSA that aims to obtain the consequent probability of explosion of the vessel, which may be followed by dead of an operator for example, the cumulative distribution function obtained from Figure 10(d) should be employed in the state space presented in Figure 11.

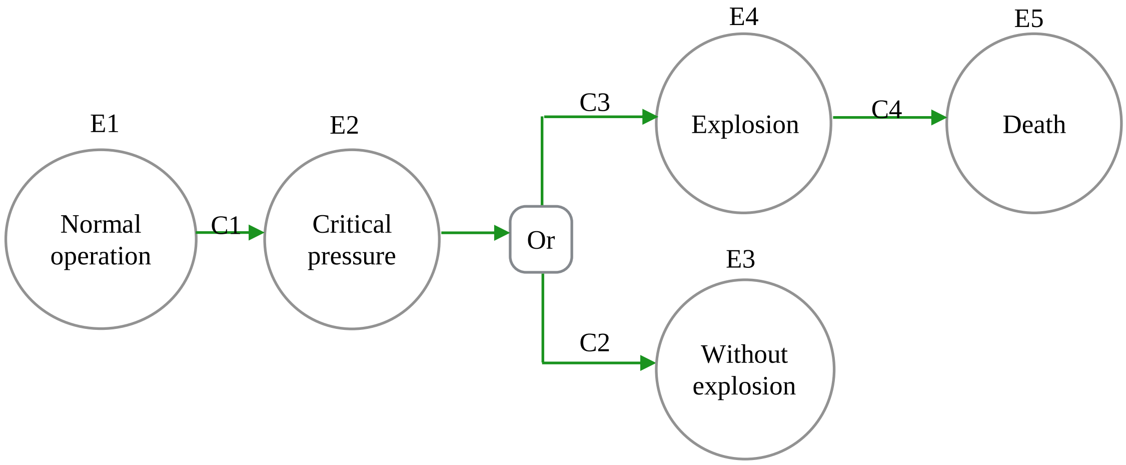


Figure III 11: Further PSA problem with critical pressure as one of its events.

As the critical pressure does not depends on discrete probability of occurrence, the connection C1 is represented by only the cumulative function distribution obtained from Figure 11(d), while the others connections may be estimated or even be obtained by other deeper analysis just as the one used to obtain de specifications of C1. This example shows how a wider problem can be divided in small and manageable deeper pieces that lead to suitable result to be used in the further resolution of the wider and less deeper problem.

In Labeau et al. (2000) [19], the pressurized vessel problem was modelled by different representation schemes (state graph, Petri net, event sequence diagram, DFM, and GO-FLOW). On comparing the results, a more intuitive method for model building and a better representation of the real system behaviour may be highlighted. Such features are mainly due to the modelling freedom, which is enabled by the proposed combination of problem modelling and resolution. The problem resolutions presented in Labeau et al. (2000) [19] start with the mathematical modelling of the problem by the Chapman–Kolmogorov equation to describe the analytic and probabilistic resolution procedures. In the presented example, the deterministic behaviours are expressed by phenomenological equations, the stochastic behaviours are located in the event connections, and the problem resolution follows a MC procedure that simulates a particle walking through the events. Given that, no further mathematical worries were needed to obtain the probability of occurrence and the probabilistic distribution curve of the time to occurrence of all events.

4. CONCLUSION

A procedure that deals with the drawbacks of methods for solving probabilistic dynamic system problems that consider deterministic behaviours was introduced. The procedure is capable of simplifying the system model building, combining it with an adequate probabilistic resolution. Due to the complex interactions among events and the required level of detail of some system models, the proposed way of identifying deterministic behaviours separated by stochastic connections, combined with the event deepness to characterize the model representativeness, introduces a new way to solve PDSP.

Furthermore, use of the procedure allows the following questions to be answered:

(i) What is the probability of occurrence of a specific process event (disregarding any time dependence)?

(ii) Given that the event has occur, what is the time distribution of its occurrence?

Using these answers in Equation (3), the probability of occurrence of the event in a specific length of time may be obtained, which is the main objective of most PSA problems.

The drawback in employing probabilistic problem resolution, which requires a large number of histories to obtain a representative result of a rare event, was partially solved by using absorbing events as the unique way to end a simulated history. Such a procedure makes discrete random behaviours the unique feature that prevents the occurrence of any modelled event. Thus, the number of MC histories required to obtain a meaningful result is naturally reduced without needing mathematical procedures or approximations such as biased techniques.

The case study was modelled and solved while respecting its system characteristics, which was possible due to the use of MC procedure that impose no restriction for modelling the problem. Although not exemplified, this freedom makes it possible to solve problems with specific system behaviours such as the dependence of the probability on previous events and/or past history time and the employment of any continuous probability distribution.

The proposed ideas also allow building of simplified model to obtain specific aimed results by using only some of the procedures presented. Furthermore, the deepness concept allows simplification of the model representation, grouping events throughout the discrete probability and the cumulative time distribution function data in event connections. Such features make it possible to build models that may be gradually updated given newly acquired information without the need to increase the model size, helping to mitigate uncertainties that are identified through dynamic knowledge development [4,15].

Finally, given that PDSP is a multidisciplinary problem, the proposed procedures to build the model, solve the problem, and analyse the results may be employed in different areas. For that, it is important to highlight that the event must embrace deterministic behaviours to allow model building from a system perspective instead of from the perspective of the status of devices or subsystem failures. The case study presented is an example in which the model presents a unique event for the normal operation (pressure in the normal range), instead of different events for the different status of each valve.

5. ACKNOWLEDGMENTS

The present work was accomplished with the CNPq support, Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brasil and CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil.

6. REFERENCES

[1] Aldemir, T., 2013, *A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants*, Annals of Nuclear Energy 52, 113–124

[2] Alejandro, D., D., G.; John, G., K.; Joel, E., S.; Jefferey, J., Z., 2008, *An integrated methodology for the dynamic performance and reliability evaluation of fault-tolerant systems*, Reliability and System Safety, 93, 1628-1649.

[3] Amendola, A., 1981, *Event sequence and consequence spectrum: a methodology for probabilistic transient analysis*. Nucl Sci Eng 77(3), 297-315.

[4] Aven, T., Krohn, B. S., 2014, *A new perspective on how to understand, assess and manage risk and the unforeseen*, Reliability Engineering and System Safety 121, 1–10

[5] Babykina, G; Brînzei, N., Aubry, JF.; Deleuze, G., 2016, *Modeling and simulation of a controlled steam generator in the context of dynamic reliability using a Stochastic Hybrid Automaton*, Reliability Engineering and System Safety 152, 115–136

[6] Berner, C., Flage, R., 2016, *Strengthening quantitative risk assessments by systematic treatment of uncertain assumptions*, Reliability Engineering and System Safety 151, 46–59

[7] Di Maio, F.; Rai, A.; Zio, E., 2016, *A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis,* Reliability Engineering and System Safety 145, 9–18

[8] Domínguez-García, A. D.; Kassakianb, J. G.; Schindallb, J. E.; Zinchukc, J. J., 2008, *An integrated methodology for the dynamic performance and reliability evaluation of fault-tolerant systems,* Reliability Engineering and System Safety 93,1628–1649

[9] Dubi, A., 1998, *Analytic approach and Monte Carlo methods for realistic system analysis,* Mathematic and Computers in Simulation, 47, 243-269.

[10] Chiacchio, F.; Compagno, L.; D'Urso, D.; Manno, G.; Trapani, N., 2011, *Dynamic fault tree resolution: A conscious trade-off between analytical and simulative approach*, Reliability Engineering and System Safety, 96, 1515-1526.

[11] Chiacchio, F.; D'Urso, D.; Manno, G.; Compagno, L., 2016, *Stochastic hybrid automaton model of a multi-state system with aging: Reliability assessment and design consequences*, Reliability Engineering and System Safety 149, 1–13

[12] Devooght, J.; Smidts, C.; 1996, *Probabilistic dynamics as a tool for dynamic PSA,* Reliability and System Safety, 52, 185-196.

[13] Dhople, S.V.; DeVille, L.; Domínguez-García, A.D., 2014, *A Stochastic Hybrid Systems framework for analysis of Markov reward models*, Reliability Engineering and System Safety 123 158–170

[14] Durga Rao, K.; Gopika, V.; Sanyasi Rao, V.V.S.; Kushwaha, H.S.; Verma, A.K.; Srividya, A., 2009, *Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment*, Reliability Engineering and System Safety, 94, 872-883.

[15] Flage, R.; Aven, T., 2015, *Emerging risk – Conceptual definition and a relation to black swan type of events*, Reliability Engineering and System Safety 144, 61–67

[16] Karanki, D.R.; Rahman, S.; Dang, V.N.; Zerkak, O., 2017, *Epistemic and aleatory uncertainties in integrated deterministic and probabilistic safety assessment: Tradeoff between accuracy and accident simulations*, Reliability Engineering and System Safety 162, 91–102

[17] Khakzad, N.; Khan, F.; Amyotte, P.. 2013, *Risk-based design of process systems using discrete-time Bayesian networks*, Reliability Engineering and System Safety 109, 5–17.

[18] Labeau, P. E., 1996, *A Monte Carlo estimation of the marginal distributions in a problem of probabilistic dynamics*, Reliability Engineering and System Safety, 53, 65-75.

[19] Labeau, P. E.; Smidts, C.; Swamaiathan, S., 2000, *Dynamic reliability: Towards an integrated platform for probabilistic risk assessment.* Reliability Engineering and System Safety, 68, 219-254.

[20] Manno, G; Chiacchio, F.; Compagno, L.; D'Urso, D.; Trapani, N., 2012, *MatCarloRe: An integrated FT and Monte Carlo Simulink tool for the reliability assessment of dynamic fault tree*, Expert System with Applications, 39, 10334-10342.

[21] Marseguerra, M.; Zio, E., 1996, *Monte Carlo approach to PSA for dynamics process systems*, Reliability Engineering and system safety, 52, 227-241.

[22] Nývlt, O.; Haugen, S.; Ferkl, L., 2015, *Complex accident scenarios modelled and analysed by Stochastic Petri Nets*, Reliability Engineering and System Safety 142, 539–555

[23] NUREG-0492, Fault Tree Handbook, U.S. Nuclear Regulatory Commission Washington D.C. 20555, January 1981.

[24] Roy, A.; Srivastava, P; Sinha, S., 2015, *Dynamic failure assessment of an ammonia storage unit: A case study*, Process Safety and Environmental Protection 9 4, 385–401

[25] Siu, N., 1994, *Risk assessment for dynamic systems: An overview. Reliability*, Engineering and System Safety 43, 43-*73.*

[26] Zio, E., 2014, *Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions*, Nuclear Engineering and Design 280, 413–419.

CHAPTER IV - RISK CONCEPT AND REPRESENTATION

Article submitted to Reliability Engineering and System Safety at 19/01/2018.

BETTER RISK UNDERSTANDING FOR A QUANTITATIVE RISK SURFACE ASSESSMENT

Rafael Raoni[a], Argimiro R. Secchi[a]

[a] Chemical Engineering Program-COPPE, Universidade Federal do Rio de Janeiro, Cidade Universitária, Centro de Tecnologia, 21941-914 Rio de Janeiro-RJ, Brasil
E-mail addresses: rbritto@peq.coppe.ufrj.br (R. Raoni), arge@peq.coppe.ufrj.br (A. R. Secchi),
Corresponding author e-mail address: rbritto@peq.coppe.ufrj.br (R. Raoni)

Abstract: The term risk is used in different areas for supporting different kinds of decisions. In essence, risk assessment tries to represent or improve the understanding of undesired and uncertain futures. Despite being widely used, there is no consensus on the risk concept in the scientific community, and this leads to different risk approaches and representations. In this work, new ideas about risk and risk characterization are discussed, characterizing the risk as a function of five variables. Furthermore, given that frequencies and severities (two risk variables) may be represented by static values or probabilistic functions, three risk representations may be obtained: (i) expected value; (ii) risk curve and (iii) risk surface. The proposed risk characterization was used to investigate the risk in two case studies, a pressurized vessel problem and a holdup tank problem. In both cases risk surfaces were built in order to visualize the frequency and severity variation of the economic loss over the analyzed time.

Keywords: Quantitative Risk Assessment (QRA); Risk concept; Risk representation; Dynamic risk assessment; Risk surface.

1. INTRODUCTION

Every day, everyone makes decisions, and the capacity to understand and correctly predict the outcomes is very important to making the right ones. When such predictions are based on stochasticity, risk shows up as an important concept. For an overall perspective, the risk has to accommodate both undesirable and desirable outcomes [11, 18], but the focuses on understanding and measuring only the undesirable future to support decision making that avoids, controls or mitigates losses is widespread applied. For that, in order to understand the situation that precedes the decision, draw good conclusions and carry out good actions, strong knowledge and adequate information about the true risk is needed [3, 44]. Thus, the risk is an important dimension of any rational decision-making process [30, 37, 43] and is applied in different areas, e.g., health, safety, environment, adverse and catastrophic scenery [40], from different perspectives, e.g., loss of life, environmental and economic damages [30], and covering a wide range of decisions, e.g., technical, operational or organizational issues [43].

Even with the importance and wide application of the risk idea, there is no consensus on its concept in the scientific field. According to Aven (2012) [9], nine different perspectives of risk (e.g., risk is: an event; the combination of scenario, consequence and probability; a future event, consequence and uncertainties, etc.) have been applied to identify and manage undesirable futures. Despite these perspectives, Villa et al. (2016) [41] grouped the particularities of all nine definitions in a consequence versus probability perspective, which is in accordance with the probability-of-loss risk perspective that has been dominant for more than 30 years in the industry [31, 13]. For a risk assessment in this consequence versus probability perspective, a sequence of steps is employed, which includes, for example, qualitative analysis, quantitative analysis, risk evaluation, risk reduction measures and risk control [30]. Finally, in order to express risk, a risk matrix, employing qualitative or quantitative information, or QRA (Quantitative Risk Assessment) may be used [43].

Regarding QRA, Apostolakis (2004) [5] had observed that, initially, the safety community was very skeptical about its usefulness, but as it was acquiring familiarity with the technology, the decision makers begun to pay attention to its insights, and several important risk measures were developed [15]. Today, the QRA, defined by acquiring and incorporating all possible knowledge for making decisions [19], allowing the relaxation and cost benefit evaluation of safety requirements [5]. The use of QRA is also fundamental for numerical goals/criteria, which is the common type of criterion adopted in the Norwegian oil and Gas industry [11], for example.

Despite the accomplishments and importance, given the need of empirical judgment for the model building and lack of fit between the probabilistic results and the real world behavior, several criticisms are still associated with QRA [13], such as its subjectivity [12]; the ambiguity and lack of accuracy to estimate consequences, probability and human judgment [29, 41]; the errors and superficiality in frequency estimations [7, 18]; its static picture of a moment by a frozen time risk estimation [9, 28, 41]; the difficulty of dealing with the black swan sort of events [10, 21, 23]; the way of the risk information is used for decision making and its influence in risk estimation [43]; the strength of the knowledge (SoK) of the decision maker [12]; the suitability of using acceptance criteria [13]; the difficulty in dealing with human errors during accident conditions [5]; its limitation in operational planning decisions [44]; the usefulness of the analysis and theories of past accident and disaster [36]; the accuracy of the assumptions made [14] and so on. Thus, the QRA analysis is not a perfect tool and should not be used only to produce numbers [5].

In order to overcome the most of these criticisms, the consideration of the uncertainties rather than probabilities [13] is highlighted. In this sense, the risk description can be either built on quantitative estimates and/or uncertainty knowledge-based [7]. This supports the view that integrates the hard QRA data with subjective judgment [9], allowing risk-informed decisions instead of criteria or risk-based decisions [5, 12].

Furthermore, to better handle uncertainties, the focus on risk management has recently increased [8]. Risk management, which complements the traditional rule-compliance [24], aims to assure better daily decisions that consider the interaction between technologic and organizational failures, employing patterns of thinking that anticipate correct actions for well-understood hazards [36]. For that, standards [4, 26, 27], procedures such as the risk barometer [22, 34], ALARP principle (ALARP: *As Low As Reasonably Practicable*) [11] and other ideas [6, 20, 28, 39] have been developed.

In fact, the main concern in risk management is to provide the continuous improvement of the understanding of risk and uncertainties [11] in order to overcome some process unpredicted behavior. These concerns require continuous monitoring of the risk picture in order to update the risk assessment based on new acquired data and on the dynamic development of the knowledge [21], aiming to improve the *operational learning* for higher organizational reliability [11, 36]. Furthermore, in terms of risk assessment, Flage and Aven (2015) [21] stated the "need for reflecting the knowledge dimension in risk assessment as well as for development of dynamic risk assessment methods", which is related with the uncertainty topic and with the need of suitable risk characterization that combines with the continuous monitoring of the risk picture in a risk management program.

Thus, it is understood that all these discussions are related with the uncertainties, how does it changes over the time and how the risk may be updated in order to maintain its value as much accurate as possible. Therefore, one of the main questions to be answered that aids the development of better risk avoidance and mitigation strategy is:

- How to deal with all criticism of QRA and deliver adequate information for a continuous update of risk information that allows good risk perception and management?

In order to deal with a risk definition that answers the introduced question, some proposals are made in this work. Furthermore, it is understood that the risk estimate must be based on the probability-of-loss perspective and the idea that the quantified risk is a probability distribution [37] must be employed. Thus, to start the risk estimation, the identification of: (i) the kind of loss to be analyzed, (ii) the event(s) that identifies the states of a process that lead to the undesirable loss, (iii) the frequency of the event occurrence and (iv) the severity of the analyzed event loss are needed. Such risk estimation steps, despite being in accordance with the major employed risk definition, are not an adequate risk description [7] due to the uncertainties in risk estimate. Therefore, the uncertainties must be considered as a separate dimension of the risk definition and then should not replace, be considered as a part of, or be an interpretation of the frequency of an event occurrence, as widely discussed [7, 8, 9, 11, 35]. Thus, in this work, the characterization of the risk as the combination of five variables: (i) L – the losses to be analyzed, (ii) E – the identified event, (iii) F – the frequency of the event occurrence, (iv) S - severity of the loss due to the event occurrence and (v) U – the uncertainties is proposed.

In Section 2, the five risk variables are defined, their common interpretations are discussed and new ideas are introduced. Furthermore, three different risk representations: the expected value, the probabilistic risk curve, and the probabilistic risk surface are presented, and some important aspects about the proposed method are discussed in order to highlight how risk may be represented to improve its understanding. In Section 3, two case studies are introduced and the probabilistic risk surfaces of the cases are obtained.

2. DEFINING RISK

One of the reasons for employing different risk concepts is the lack of the capacity to understand a wider risk perspective. In order to fix this misunderstanding, a risk function (R=f(L, E, F, C, U)), as depicted in Figure 1, is presented.

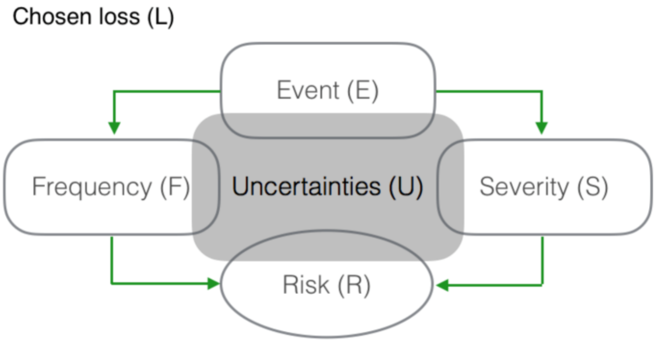


Figure IV 1: Risk dependencies.

2.1. The five risk dimensions

In this section, the role of each risk variable is discussed.

- **Losses to be analyzed (L)**

First of all, in order to improve the understanding of the proposed risk definition, the use of the word "consequence" was avoided since it may be understood as "everything that happens due to some previous occurrence," describing, for example, a hazard scenario, harmful effects, losses, etc. Then, the variable L defines the kind of loss to be analyzed in a risk framework, which needs to be, necessarily, a measurable loss, e.g., financial losses, human losses, amount of spilled oil, etc. If aiming for the analysis of an intangible outcome such as "Company Image," a measurable scale for the degree of loss may be employed to turn it into a measurable outcome.

The risk variable L is required since a unique hazard scenario can lead to different kinds of losses, which must be analyzed separately in order to obtain different risk estimates. This specification aims to lead to risk visualization in the loss perspective instead of the accident perspective. Despite not being normally identified as a risk variable, the loss (L) is normally required to manage industry risk analysis, where, for example, it is considered as the objective of the analysis [27] or as a type of consequence with human value [8, 43] that should characterize the risk measure [30].

- **Identified Event (E)**

It is understood that the event cannot be defined only as a hazard scenario or as its effects, which usually occur in risk analyses, but require a wider definition that embraces any event that causes the analyzed loss. In this sense, the event (E) is defined as an occurrence in the process that leads to the losses to be analyzed (L). For example, if the quantification of the risk of financial loss of an explosion is needed, the prior damage in the plant and several further consequences of the explosion must be identified as events in the risk analysis. It is important to note that, because of the uncertainties in risk analysis and also because of hazard identification techniques need restricted scope in order to keep the analysis within reasonable bounds [18], the employment of one risk analysis for hazard identification does not guarantee that all the events that lead to the analyzed losses were identified. In this sense, since a non-identified event leads to a non-analyzed risk [1], a great attention must be paid in the event identification step. Furthermore, this step is often the most important part of QRA and contributes to both risk generation information and identification of actions [3].

- **Frequency of the event occurrence (F)**

This variable is a known risk dimension and may be nominated as frequency, probability, likelihood or uncertainty. In this work, the term frequency (F) is employed to identify the average number of occurrences of an event in a unit of time, which could be represented by single value (e.g., failure per year), or by a probabilistic function with time as a continuous random variable to represent the variation of the frequency value in time. For the major community risk specialists, such frequency variation is considered as uncertainty, however, since uncertainty also involves other issues, e.g., reliability of the data, human epistemic uncertainty or expectation, etc., in this work, this frequency variation, which is a calculated magnitude, is not defined as uncertainty, and the discussion about what defines uncertainty is made later in the description of the uncertainty risk variable (U). The word frequency was chosen because the time dimension is used to identify the number of occurrences for some event (e.g., the frequency of the valve failure is 0.2 failures/year). Then, the frequency variable is a function of the time (F(t)) and, differently of probability/likelihood values that must be between 0 and 1, may assume values higher than one (e.g., the frequency of the valve failure is 1.5 failures/year) [2].

Furthermore, as discussed by Raoni and Secchi (2018) [38], both discrete and continuous random variables must be considered in order to calculate the relative frequency of an event occurrence. The discrete random variable identifies if, given a start point of the process, the event will or will not occur, while the time as a continuous random variable identifies when the event occurred. To calculate one event occurrence probability in a given length of time, a value between 0 and 1, Equation (1) must be employed.

$$Pe\left(t_j\right)_i = Pe_i * CDF\left(t_j\right)_i \tag{1}$$

where $Pe(t_j)_i$ is the probability of the event *i* to occur in the interval t = [0, t_j], Pe_i is the discrete probability of occurrence of the event *i* given the start point of the process and $CDF(t_j)_i$ is the cumulative probability of one event occurrence *i* between the time 0 and t_j.

Thus, the frequency risk variable (F) assembles the information if and when the event (E) occurs without considering uncertainty (given a probabilistic function to represent F(t), the variability of the time to the event occurrence is not considered as uncertainty).

- **Severity of the loss of the event occurrence (S)**

The severity is the quantitative or qualitative measurement of some potential losses with human value [7, 8] or the estimation of potential damage or injury due to a specific unwanted event [41]. Thus, the severity (S) is the amount of loss (L) of one event (E). The key point here is the difference between the definitions of loss (L) and severity (S). While the first only identifies the loss to be analyzed, the latter is a measurable value of the loss, which can be represented by qualitative information or by quantitative value as a discrete number or probabilistic function. It is important to highlight the difference of employing a probabilistic function to the frequency of the event (F(t)), where time is a continuous random variable, and the severity loss (S(L)), where the magnitude of the loss is the continuous random variable. Furthermore, just as in the frequency, the variability of the severity, given its probabilistic function, is not considered as risk uncertainty.

- **Uncertainty (U)**

The topic of uncertainty is probably the most discussed in the literature and is the main source of mistrust about the concept of risk and its usefulness. Despite the discussion about risk uncertainty due to the risk result interpretation, or "risk acknowledgement" [3], the proposed approach identifies the risk uncertainty (U) as the difficulty in obtaining the precise risk value. In this perspective, the risk uncertainty (U) is not identified as the variability of the risk estimation caused by the employment of probabilistic functions for frequency (F) or severity (S), but as the intrinsic uncertainties of the whole risk estimate. This assumption partially agrees with Aven (2010) [7] who argued that, for risk estimation, uncertainties beyond the probabilities should be taken into account.

In this sense, one may agree that, for real world risk assessment, several assumptions and simplifications are made [10], mainly during the (i) abnormal events identification and during the modeling, resolution and result interpretation of problem that seeks to estimate (ii) frequency and (iii) severity of unwanted events. These assumptions and simplifications are the ones that propagate throughout the risk assessment and lead to the uncertainty (U) in the risk result. Thus, the proposed uncertainty (U) assembles all possible errors of the event identification (E) and frequency (F) and severity (S) estimations, being a function of these three variables (U=f(E, F, S)). Furthermore, the uncertainty may be described as a function of two factors: (i) some lack of quality of the risk study or the analyst's lack of SoK and (ii) a deeper unknown cause. The consideration of unknown means that the named SoK is something that, even with a continuous evolution, has a limit that will never embrace the whole knowledge needed to correctly predict a risk value, embracing then the state-of-the-art in risk assessment. In Figure 2, the relation between SoK, which varies between a minimum basic knowledge and a maximum technical quality, and the uncertainty (U) is shown.

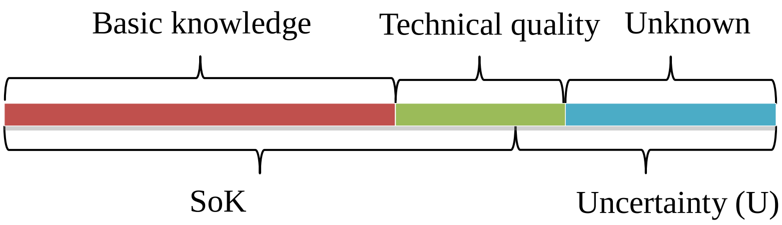


Figure IV 2: Relation of SoK and uncertainty (U).

The uncertainty measures the difference between the risk estimate and the correct risk value. But, as the correct risk will never be truly obtained, uncertainties will always be non-null and non-quantified risk dimension. Thus, the uncertainty is a variable that identifies the accuracy of the risk estimate, which must consider the limitation of the events, frequency and severity estimations according to the sensibility of the analyst. Some authors, in a perspective of frequency uncertainties, argue that, given some worries [37], uncertainty may be represented by introducing a new subjective probability [31], a second order distribution probability [7, 44] or by other manners [3, 14, 35]. In the proposed risk uncertainty perspective, the advantages of using procedures or tools to represent and treat uncertainties in order to understand how they influence the risk estimate are noted, but this discussion is not the purpose of the current work.

Finally, the introduced uncertainty is a risk dimension that tries to highlight the possible errors in the risk estimates, making the QRA and the widely employed quantitative risk acceptance criteria seems limited. Despite that fact, it is understood that risk quantification is still the most accurate approach for understanding and managing undesirable futures and should be estimated according to the discussion in the next section.

2.2. Risk characterization

Given the discussion of the four risk variables (L, E, F and S), the risk may be estimated in order to be analyzed considering the variable uncertainty (U). However, managing different simplifications of F and S in the risk estimate lead to different risk representations as the (i) expected value, (ii) probabilistic risk curve and (iii) risk surface. In this sense, this subsection aims to highlight the difference and advantages of these risk representation in order to facilitate the understanding of their results.

(i) Expected value

The expected value is a known, widely applied in engineering [7] and controversial risk estimate. The simplification considers a static picture of time, with frequency and severity as fixed values. The expected value of one or a group of events is the arithmetic mean of the loss generated by the occurrence of a group of infinite similar events [9]. Such risk representation is in widespread use, mainly due to its easy calculation and comparison with regulatory acceptance criteria, and may be calculated employing Equation (2).

$$R_L = \sum_{E=1}^{n} \left(F_E * S_E \right) \tag{2}$$

where R_L is the risk of the analyzed loss and n is number of identified events (E).

Given the law of large numbers, the expected value may represent the risk of events that can occur several times in a process history, just as in the expectation of a loss of $50 given a gamble on a flip of an unbiased coin repeated 100 times that when it is heads leads to a loss of $1 ($R_L$ = F×S = 0.5×1 = 0.5 → Total loss = 100×R_L = 50). Such risk representation is equivalent to considering that the total amount of loss occurs proportionally and gradually. This means that, given the situation that leads to the event occurrence repeats until the sum of the event frequency of occurrence reaches one, the total loss of the event can be fully computed. Using the unbiased coin gamble as an example: for one coin flip, R=0.5*1=0.5; for two coin flips: R=2*0.5*1=1. This means that only with two coin flips, which makes the sum of the frequency of each flip reach 1, the full computation of the severity of the risk is enabled. Then, for a frequency value lower than one, the expected value considers the partial occurrence of the event, even that it is not truly possible (just as in the partial death of Schrödinger's cat).

Because of that, the expected value is inappropriate to represent the risk of events that cannot occur several times in the process history, just as for events with high severity and low frequency that receive great attention in industry safety risk analysis, and to represent the risk of events that require considering variability in their frequency and/or severity estimates. The expected value also makes no distinction between the risk of events that have high severity and low frequency and risk of events that have low severity and high frequency, as long the product of their frequency and severity are equal [2, 7]. Because of these points and despite the useful information for decision-making, the expected value cannot be used as a general risk definition [7].

(ii) Probabilistic risk curve

The expected value assumes that both severity and frequency are discrete values. However, one may agree that to represent both risk variables in this way may seem limited because the frequency may vary over time and the severity may be better represented as a continuous random variable. Thus, the probabilistic risk curve is obtained when one of the severity (S) or the frequency (F) of an event occurrence is represented by a probabilistic curve while the other variable is kept as a fixed value.

A risk representation with variable severity is presented, for example, in the FN (frequency F of N or more number of fatalities) curve to represent the risk acceptance criteria of fatally risky activities [30]. This kind of risk representation is classified as probability consequence diagrams (PCDS), which can be applied to analyze different kinds of loss and allow a better visualization of the risk [2]. Such representations are normally used to represent the Frequency (F) and Severity (S) pair of different Events (E) that lead to the same kind of Loss (L), enabling an ease of visualization and classification of the risk of a specific loss for a group of events.

Despite this, our proposed approach aims to obtain the probabilistic risk curve by considering the severity variability of the analyzed event loss, meaning that the severity is represented as a continuous random variable. In this sense, the risk of a unique event can be represented by a risk curve. For example, given that a process failure (E) has a fixed frequency of occurrence (F) equal to 0.5 failure/year and leads to financial loss (L) with severity (S) represented by a normal probabilistic function with mean equal to \$100,000 and standard deviation of \$30,000, the probabilistic risk curve can be represented by the probability density and cumulative distribution risk functions shown in Figure 3.

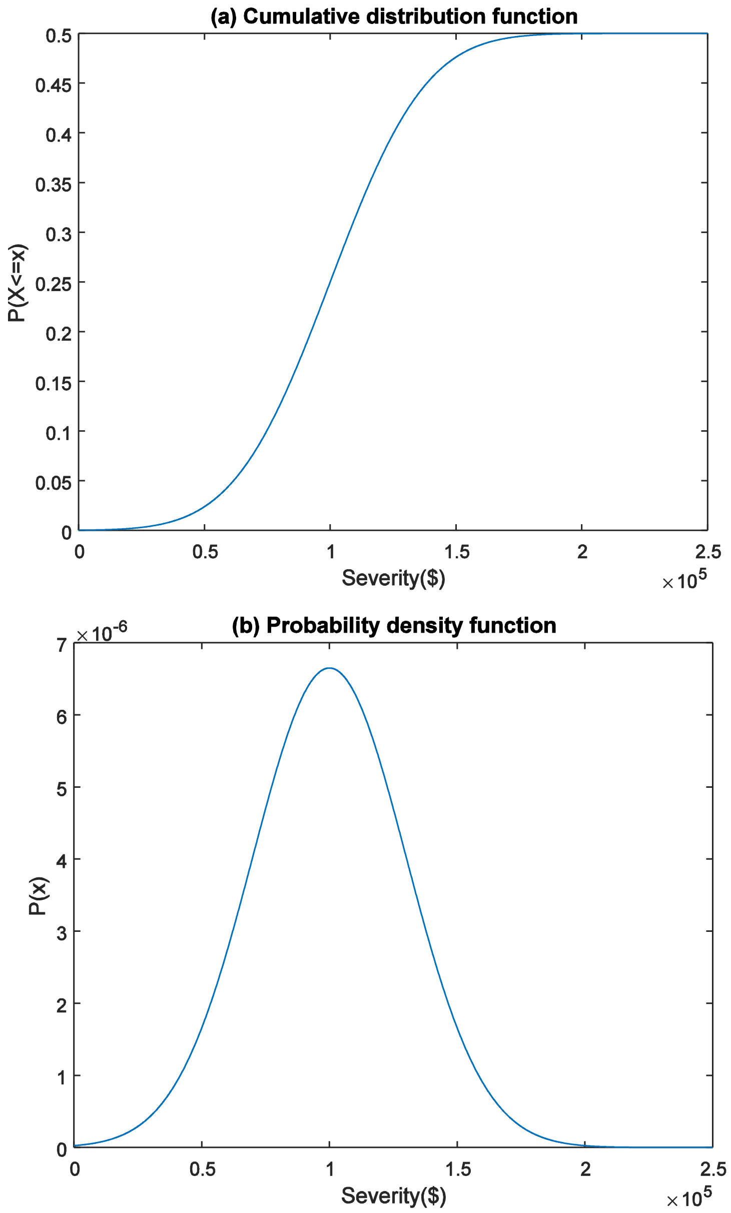


Figure IV 3: Probabilistic risk curve for the variable severity example - (a) Cumulative distribution function; (b) Probability density function.

Such risk representation enables verifying the probability of the occurrence of different severity magnitudes, which is very important to improve the understanding of risk.

Furthermore, the variability of the event occurrence frequency in time leads to other kinds of risk curves. Such frequency representation is commonly employed in reliability problems, where, for example, applying a Monte Carlo procedure in a process model with defined failure states, the statistical probability of the system failure in the defined mission time may be obtained [32, 33]. Such application normally aims to obtain the time probabilistic function of an event with known and undesirable consequences.

Despite this, the purpose of the proposed risk representation is, given the time as a continuous random variable, to obtain a time dependent risk representation, combining then the frequency and severity. Using the same introduced example but with frequency of occurrence (F) represented by an exponential probabilistic function with mean equal to 0.5 failure/year and severity (S) equal to \$100,000, the probabilistic risk curve is represented by the probability density and cumulative distribution risk functions shown in Figure 4.

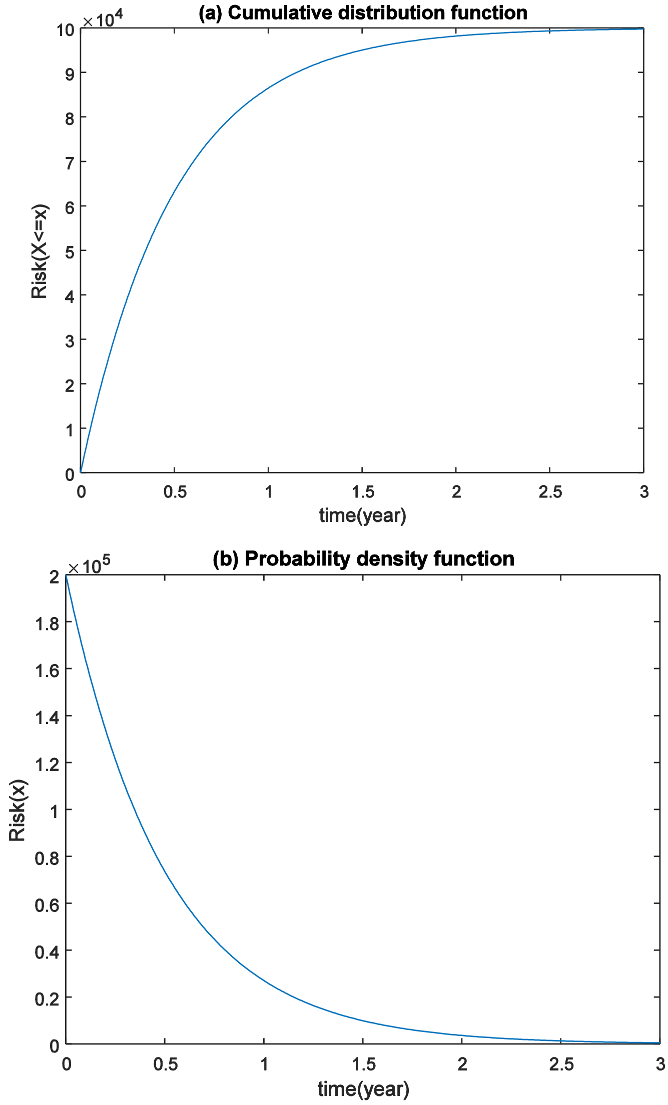


Figure IV 4: Probabilistic risk curve for the variable frequency example - (a) Cumulative distribution function; (b) Probability density function.

The *y* axis of the distribution risk functions in Figure 4 is the product of the frequency of occurrence and severity, identifying the risk (Frequency times Severity) at a given time on the *x* axis, introducing a time dependent risk representation.

(iii) Probabilistic risk surface

A risk representation where both severity (S) and frequency (F) are probabilistic functions is proposed, and employing Equation (2), a three dimensional "*time x frequency x severity*" risk estimate is obtained. Using the same example introduced above but with frequency of the event occurrence (F) represented by an exponential probabilistic function with mean equal to 0.5 failure/year and severity (S) represented by a normal probabilistic function with mean equal to $100,000 and standard deviation of $30,000, the probabilistic risk surface is represented by the probability density and cumulative distribution surfaces shown in Figure 5.

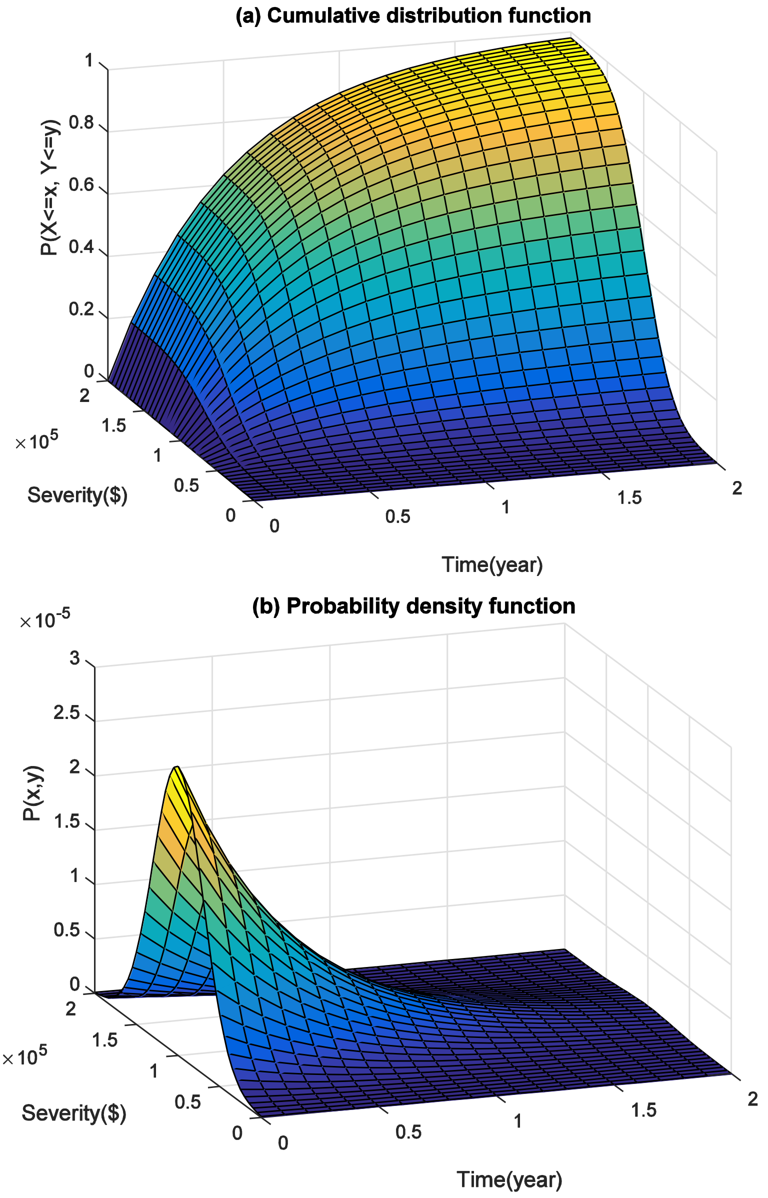


Figure IV 5: Probabilistic risk surface example - (a) Cumulative distribution surface; (b) Probability density surface.

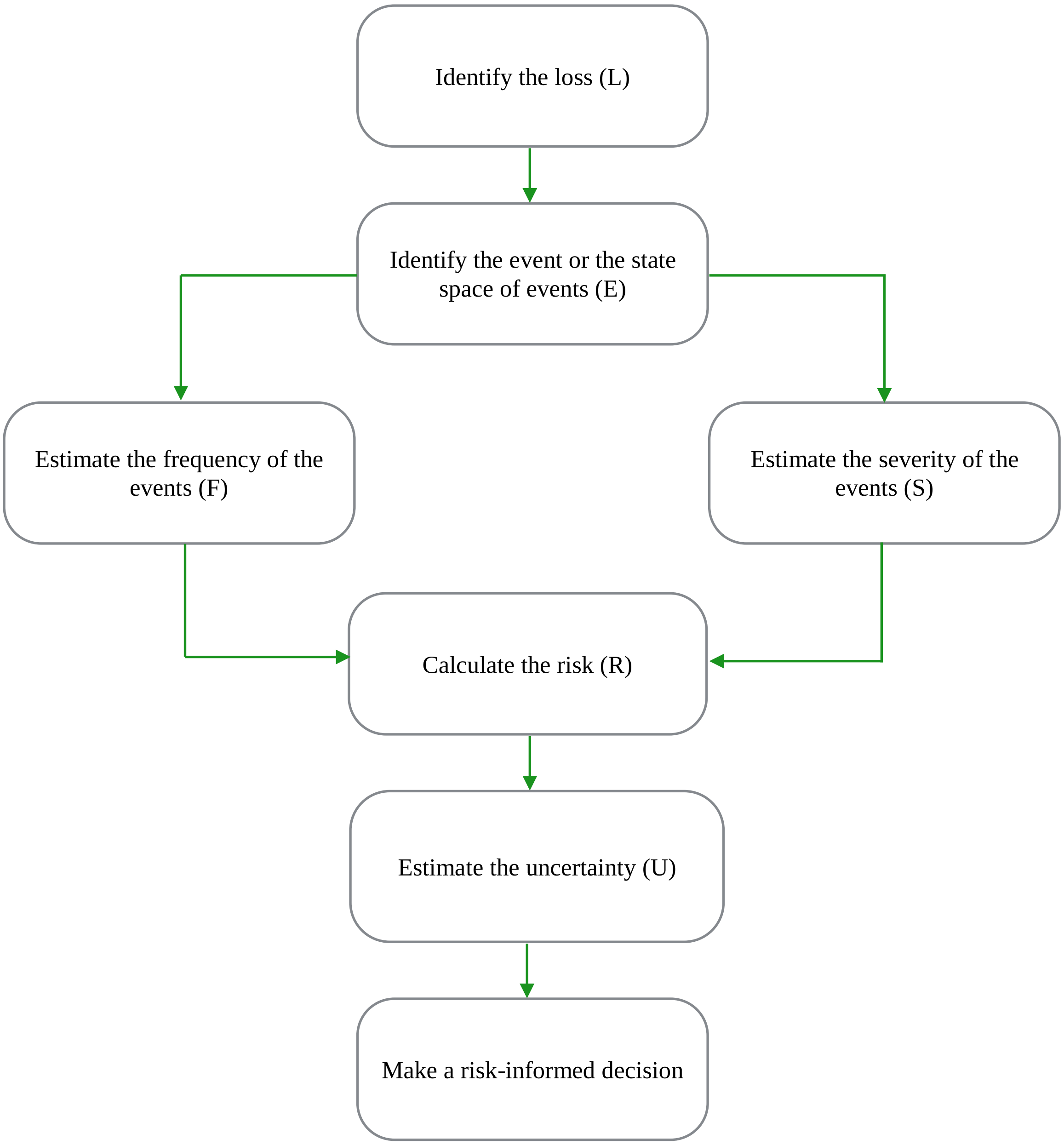
The examples show the application of the proposed approach in a unique event quantitative risk estimate. However, by employing the sum of Equation (2), a total risk picture of a group of events may be obtained. In order to obtain the best total risk surface representation, all identified events, even those with apparently neglected risk, should be considered since the sum of small risks may influence the total risk picture. Such a probabilistic risk surface leads to a risk perspective that does not focus on the avoidance of a unique undesirable event but on a wider risk for the process behavior just as the PCDS [2].

Furthermore, separating the time in the risk representation enables the analysis of the risk variation over a short period of time, as in the variation of the risk to humans during a day that has different human traffic in an industrial plant (daily variation of the severity), or over a long period of time by enabling visualization of when the process, which today presents acceptable risk, starts to be unacceptably risky (long term variation of the frequency or/and severity).

The risk surface enables us to visualize the value or the variation of the frequencies along the time and severity length, introducing a new way to understand risk. The probabilistic density risk surface representation is equivalent to a three-dimensional probability density function, and, the frequency of a specified length of severity and time is the volume under the surface. At the same time, the cumulative risk surface representation is equivalent to a three-dimensional cumulative distribution function, and given a specified severity value and time, the frequency axis is the frequency of the cumulative severity and time. Furthermore, it should be noted that, despite not identified, when a unique event can occur more than once in one time unit, or different events that lead to the same severity may occur together in one risk time unit, the severity may have a frequency higher than one. In the second case study, such a risk representation is exemplified.

2.3. Concluding the risk assessment

Different manners to estimate risk were discussed. However, none of them considered the uncertainty variable (U). After the risk obtainment, the last thing to do is understanding that the result does not represent the real risk of the process, principally in a long time perspective, to highlights the importance of a risk management program that should focus more attention on mitigating a wider risk perspective and also to update the risk results with actualized data and knowledge. Finally, in order to manage a risk assessment with the present proposed concerns, the steps shown in Figure 6 must be followed.


Identify the loss (L)
Identify the event or the state space of events (E)
Estimate the frequency of the events (F)
Estimate the severity of the events (S)
Calculate the risk (R)
Estimate the uncertainty (U)
Make a risk-informed decision

(E) Will the risk analysis be of a process or of a unique event?
(F) Will the frequency be a fixed value or a time probabilistic function?
(S) Will the severity be a fixed value or represented by a probabilistic function?
(R) Depending on the frequency and severity the risk will be represented by:

- Expected value;
- Severity probabilistic risk curve;
- Time probabilistic risk curve;
- Risk surface.

(U) If needed, change the risk representation.

Figure IV 6: Steps for risk assessment.

In the end, to make a risk assessment of different losses (L) for the already identified group of events, their Frequency (F) estimation(s) may be used.

2.4. Further comments

Follow, two important topics for concluding the aimed risk description are discussed.

- **Black swan events**

Given the discussion and some proposed definitions for black swan events [9, 21, 23], it is understood that these sorts of events are those that lie in the described risk uncertainty variable, more specifically in the event identification uncertainties, embracing the unknown and lack of technical quality. Furthermore, given the group of non-identified events, the ones that are represented by the pair of high severity and low frequency are those identified as black swan events, and once they occur and become known, they stop being one. In the frame of the proposed risk representations, the black swan events are located, but not represented, on the curve/surface tail with high severity and low frequency of a process total risk picture. Furthermore, there are also non-identified events without high severity and low frequency not named as black swan events but that obviously influence the risk representation.

- **Quantitative forecasting models**

The forecasting models are extrapolations of past observations that predict uncertain future behaviors [42]. Given that the process in which the forecast models are applied are difficult to be predicted, such models are mostly based on best judgment and presents a lot of uncertainties. In this sense, financial time series based in Geometric Brownian Motion (GBM) or autoregressive models (e.g.: AR, ARMA, ARIMA, etc.), for example, can be related with the proposed risk surface. In essence, the results of these models can be understood as one of many histories of process behaviors that together can form the proposed risk surface. For example, if a forecasting model is simulated several times, the proposed probabilistic risk surface of the process may be obtained. In Figure 7 an example of a related probabilistic risk surface and forecasting model is shown, where a GBM, presented in Equation (3), with mean (μ) equal to 0.1 and standard deviation (σ) equal to 5, in a period of 100 time units was used. In this example the increase of the severity variability along the time dimension, which represents the increase of the uncertainties over the time, may be observed.

$$x_{t+1} = x_t + Normal\left(\mu,\sigma\right) \tag{3}$$

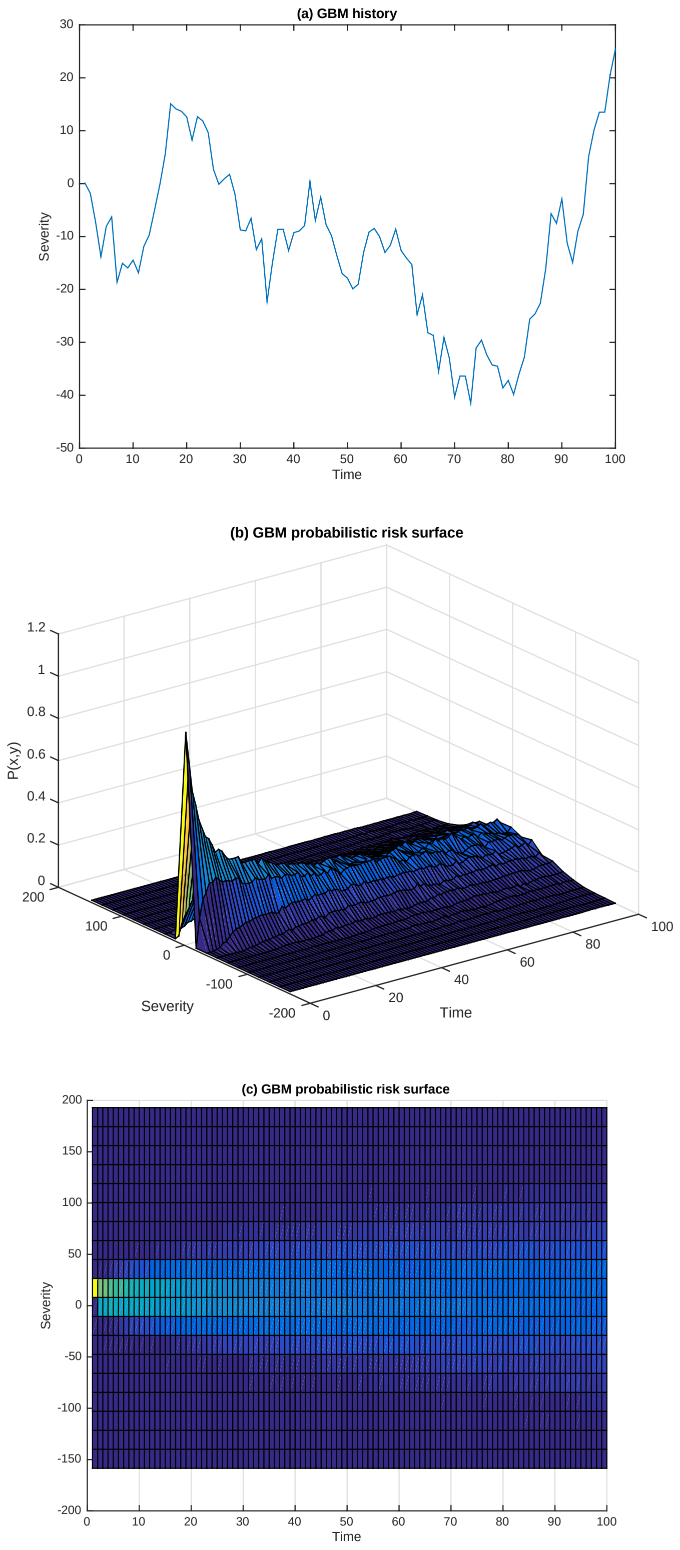


Figure IV 7: Relation between probabilistic risk surface and forecasting models - (a) One history of GBM; (b) GBM probabilistic density risk surface; (c) GBM probabilistic density risk surface upper view.

3. CASE STUDIES

The two case studies presented are reliability benchmark problems. The first case study investigates the risk of the failure of two valves that contribute to the vessel pressure change [38], and the second investigates the risk of the dynamic behavior of the level of a holdup tank, considering the failures of its two pumps and one valve [16, 25].

3.1. Pressurized vessel

3.1.1. Process description

The process is characterized by a vessel that is continuously pressurized from its initial condition (P_0), until it reaches the high-pressure (P_h) at which the valve (V1) is required to open to release the pressure. During this process, a second valve (V2) can eventually fail open, contributing even more to the rise in vessel pressure. In the case where V1 fails to open and/or V2 fails open, the vessel can reach the critical pressure (P_c) where the occurrence of losses is considered. The described process is presented in Figure 8.

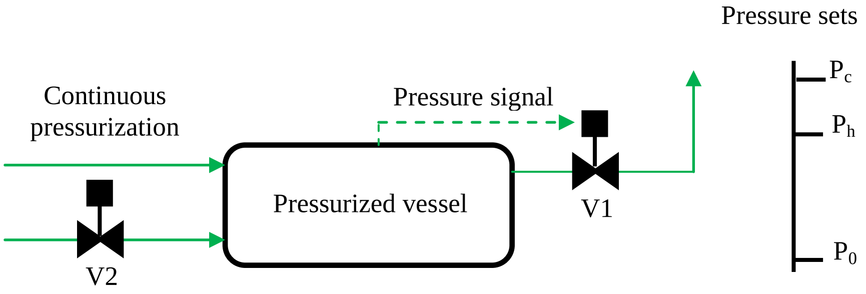


Figure IV 8: Pressurized vessel process.

3.1.2. Risk variables identification

In this example, the financial loss (L) of the undesirable vessel overpressure behavior was analyzed. Given the state space of the process, presented in Figure 9, only event 5 (E5) leads to a financial loss and needs to have its frequency and severity estimated. Both event identification and frequency estimation of the event E5 were obtained from Raoni and Secchi (2018) [38]. The frequency (F) of the E5 occurrence is characterized by a discrete probability equal to one and time cumulative probabilistic function shown in Figure 10. For the severity (S), a normal distribution with mean equal to \$10,000 and standard deviation equal to \$2,000 was considered.

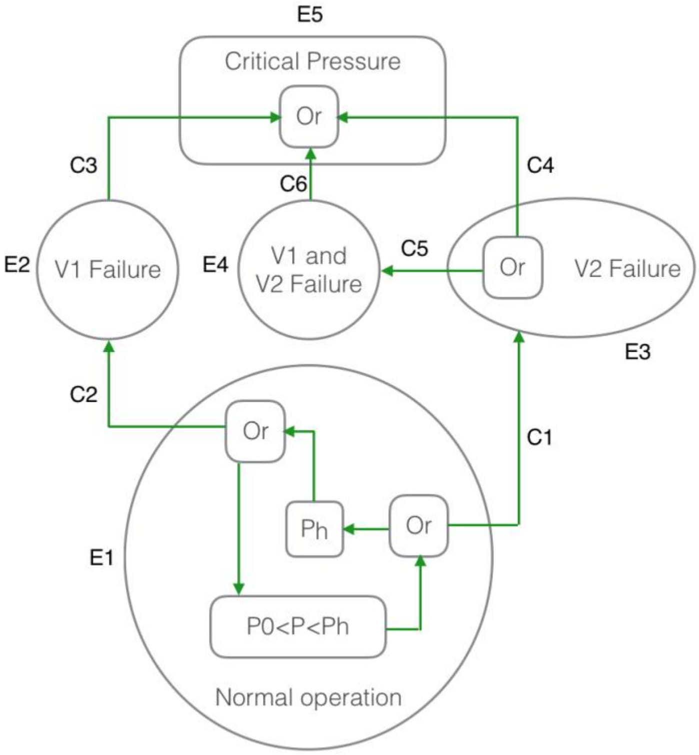


Figure IV 9: Graphical representation of the pressurized vessel problem.

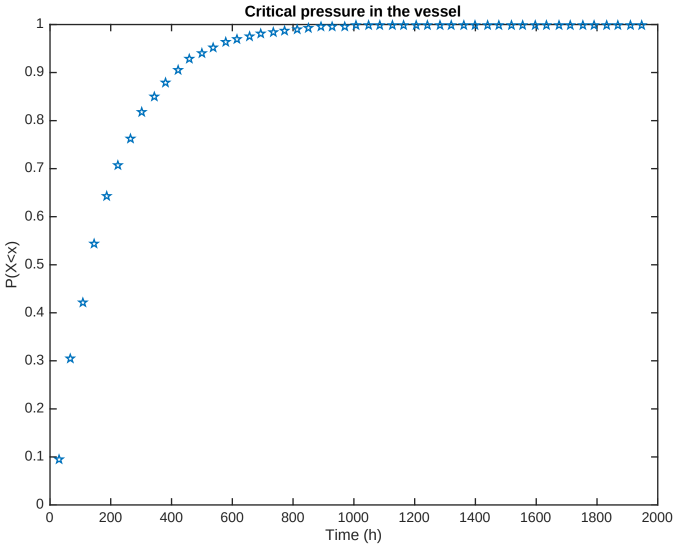
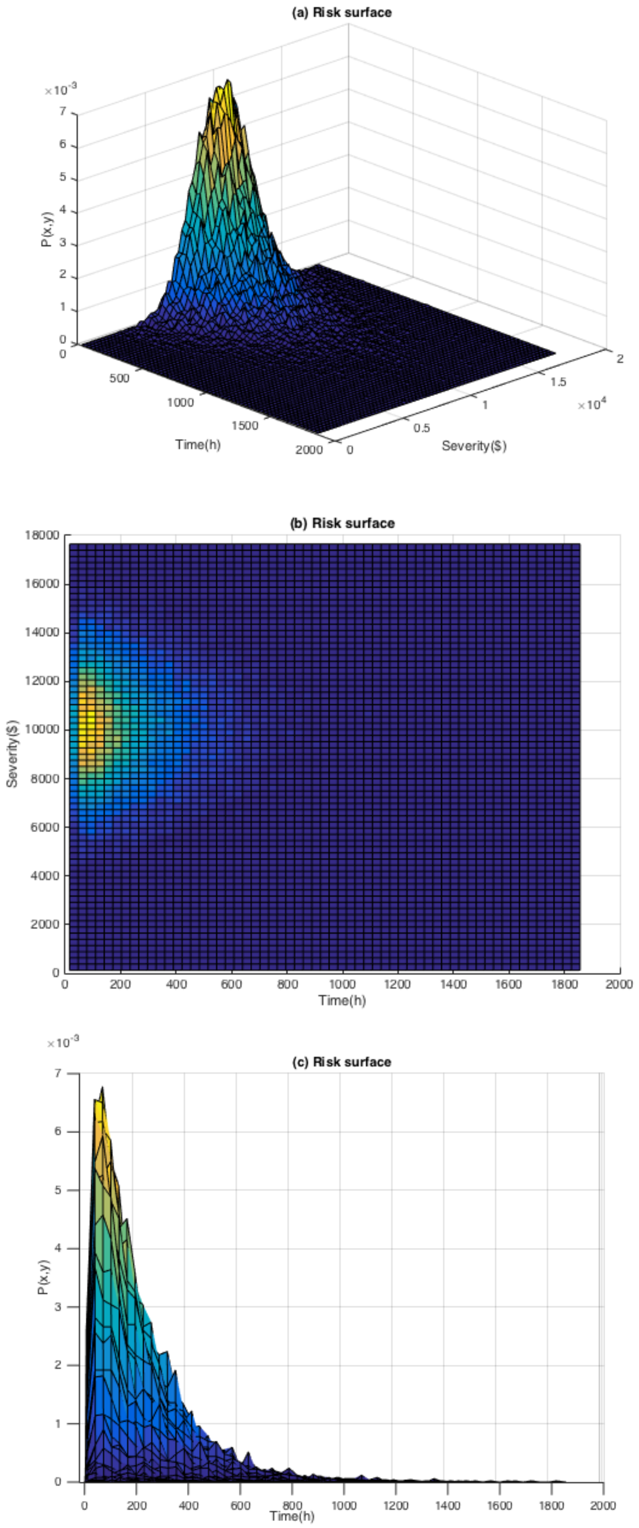


Figure IV 10: Time cumulative probabilistic function of the occurrence of event 5 (E5).

3.1.3. Risk calculation

The problem was modeled and solved in MATLAB® software using a Monte Carlo procedure with 2,000 histories; the obtained probabilistic density risk surface is shown in Figure 11 and the obtained cumulative risk surface is shown in Figure 12.


(a) Risk surface
×10^-3
7
6
5
4
3
2
1
0
P(x,y)
0
500
1000
1500
2000
Time(h)
0
0.5
1
1.5
2
×10^4
Severity($)
(b) Risk surface
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
Severity($)
0
200
400
600
800
1000
1200
1400
1600
1800
2000
Time(h)
×10^-3
(c) Risk surface
7
6
5
4
3
2
1
0
P(x,y)
0
200
400
600
800
1000
1200
1400
1600
1800
2000
Time(h)

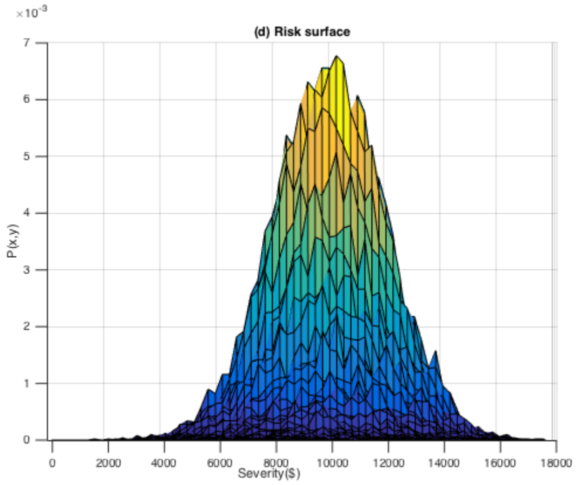
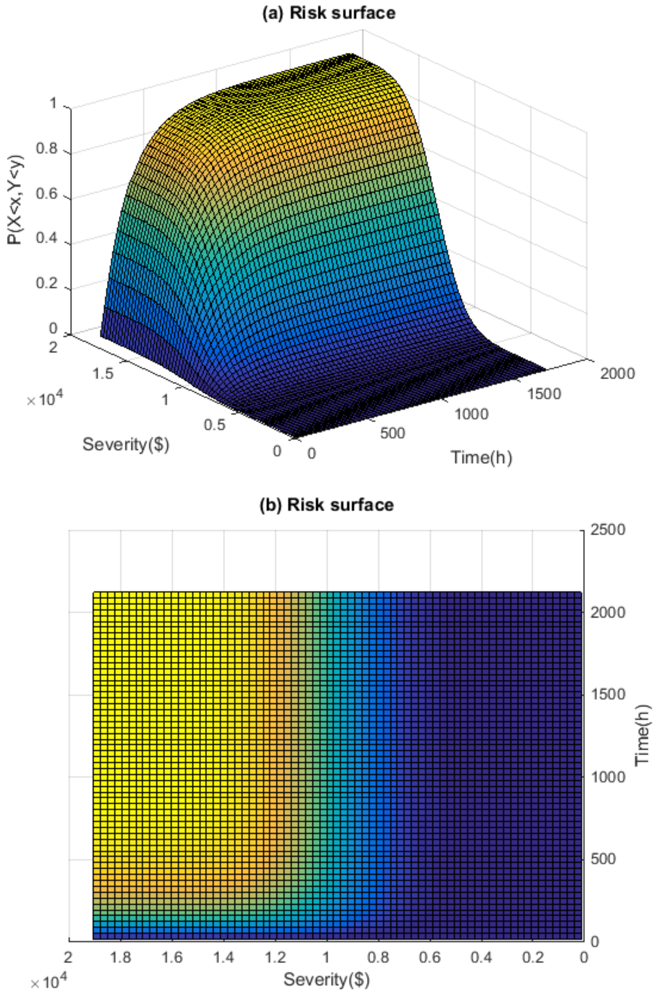


Figure IV 11: Pressurized vessel - (a) Probabilistic density risk surface; (b) Probabilistic density risk surface upper view; (c) Probabilistic density risk surface in time axis; (d) Probabilistic density risk surface in severity axis.



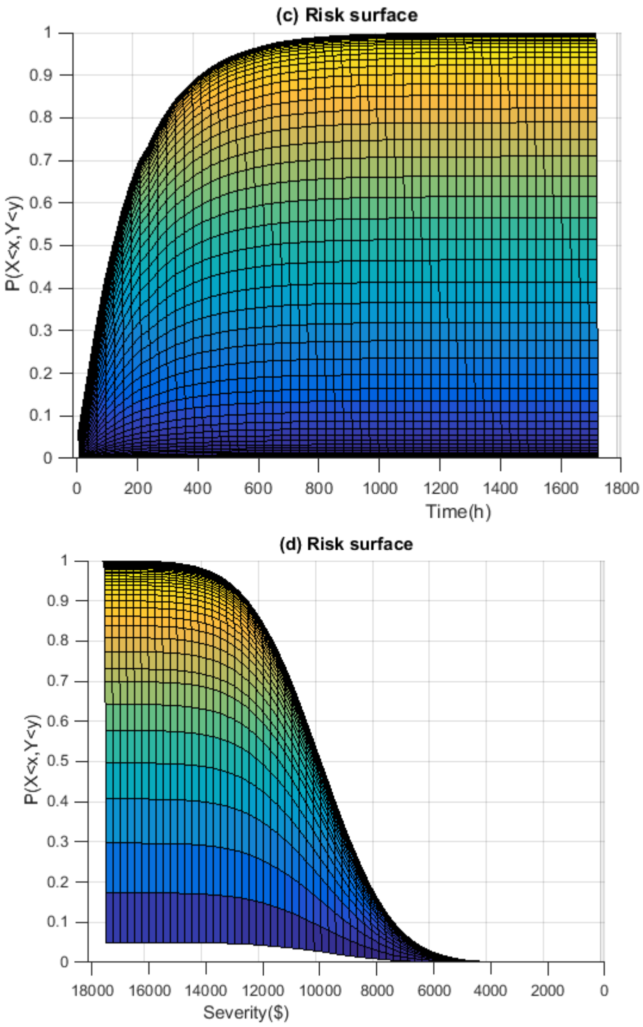


Figure IV 12: Pressurized vessel - (a) Cumulative risk surface; (b) Cumulative risk surface upper view; (c) Cumulative risk surface in time axis; (d) Cumulative risk surface in severity axis.

3.1.4. Problem observations

In the risk surfaces shown in Figure 11 and Figure 12, the term probability was employed due to the analysis of one event occurrence over the time duration. Furthermore, the calculated risk surface presented in Figure 11 highlights the higher probability of the event occurring within the first 200 hours and the higher probability of the severity around $10,000, in accordance with the frequency and severity data. In order to conclude the risk assessment, the consideration of the risk uncertainty dimension is necessary. For that, some corrections in the obtained risk surface should be made using, for example, a second order probability distribution [7, 44] in the frequency or severity value.

The presented risk surface was calculated for a unique event (E5) and considered a unique possibility of occurrence in the process history (once the event occurs, the process does not return to operation, and risk no longer exists). Despite the usefulness of these considerations, the risk analysis of multiple events that could occur several times in a process history is very important to understand a wider risk framework and is exemplified in the next study case.

3.2. Holdup tank

3.2.1. Process description

The holdup tank problem was built to understand the dynamic level behavior of the tank due to the operation of its two inlet pumps (Unit 1 and Unit 2) and one outlet valve (Unit 3). In order to investigate the risk of the tank operation, the possibility of overflow, dry-out or stopping of the operation with a stable level due to failures of its Units was studied. The holdup tank process is shown in Figure 13.

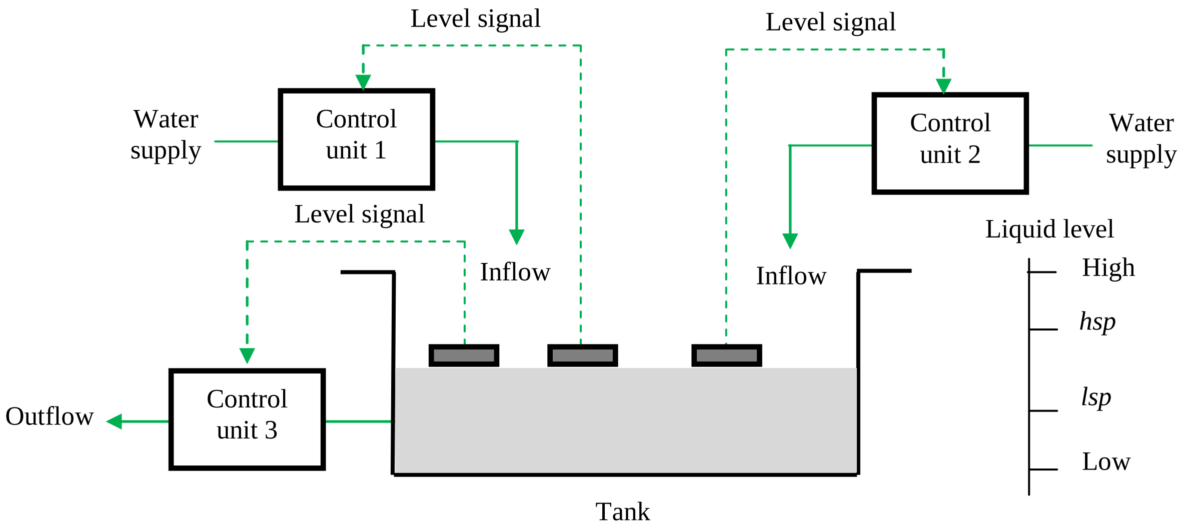


Figure IV 13: Holdup tank process [16].

According to the correct operation of the Units, the normal level varies between *hsp* (high level set point) and *lsp* (low level set point). When level > *lsp* changes to level < *lsp*, the pumps 1 and 2 turn on and the valve closes, and when level < *hsp* changes to level > *hsp*, the pumps 1 and 2 turn off and the valve opens. Finally, when the tank level reaches Low or High level, the tank is in dried-out or overflow condition, respectively.

3.2.2. Risk variables identification

In this example, the financial loss (L) of the undesirable process behavior was analyzed. Given the state space identification of the process, presented in Figure 14, the events E2, E3 and E4 were assumed to lead to financial loss and thus needed to have their frequency and severity estimated. In order to obtain a risk surface of a continuous process operation, the process needs some time, represented by probabilistic functions (repair connections C4, C5 and C6), to return to its normal operation (E1) due to the fixing of the damaged unit(s). In this probabilistic dynamic system problem (PDSP) [38], the normal operation (event E1) groups the oscillation of the level between *hsp* and *lsp*, which is the consequence of correct operation of the units. The failures of the units could be a discrete random failures, which occurs when their operational logics are not followed, or follow a failure rate described by an exponential probability distribution function, which makes the valve remain in its last position (open or close) and turn off the pumps. The state space of the problem is shown in Figure 14, the inlet parameters of the problem are presented in Table 1 and, as an intermediary result of the PDSP, the obtained cumulative probabilistic functions of the time of occurrence of E2, E3 or E4 are shown in Figure 15 and their discrete probability of occurrence are presented in Table 2.

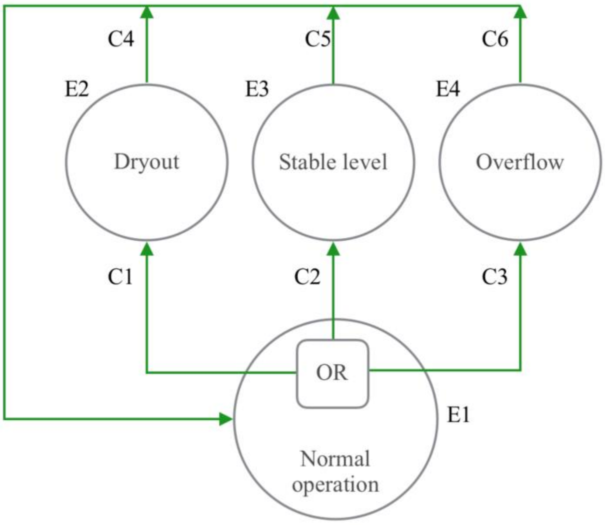


Figure IV 14: Graphic representation of the holdup tank problem.

Table IV 1: Parameters of the holdup tank problem.

Parameters	**Value**	**Parameters**	**Value**
Initial level (m)	5.5 (filling)	λ (Pump 1 failure rate –f/h)	1.67×10^{-3}
H (m)	10	ρ (Pump 1 discrete failure - %)	0.03
hsp (m)	8	λ (Pump 2 failure rate –f/h)	1.67×10^{-3}
lsp (m)	3	ρ (Pump 2 discrete failure - %)	0.03
L (m)	1	λ (Valve failure rate –f/h)	3.33×10^{-3}
-	-	ρ (Valve discrete failure - %)	0.1
Change of the tank level due to unit 1 operation - Pump 1 (m/h)			0.40
Change of the tank level due to unit 2 operation - Pump 2 (m/h)			0.20
Change of the tank level due to unit 3 operation - Valve (m/h)			-0.40
Connections		**Probabilistic function**	**Mean**
C4 connection		Exponential	48 h/repair
C5 connection		Exponential	100 h/repair
C6 connection		Exponential	240 h/repair
Time of simulation		10000 h	
Number of Monte Carlo histories		50000	

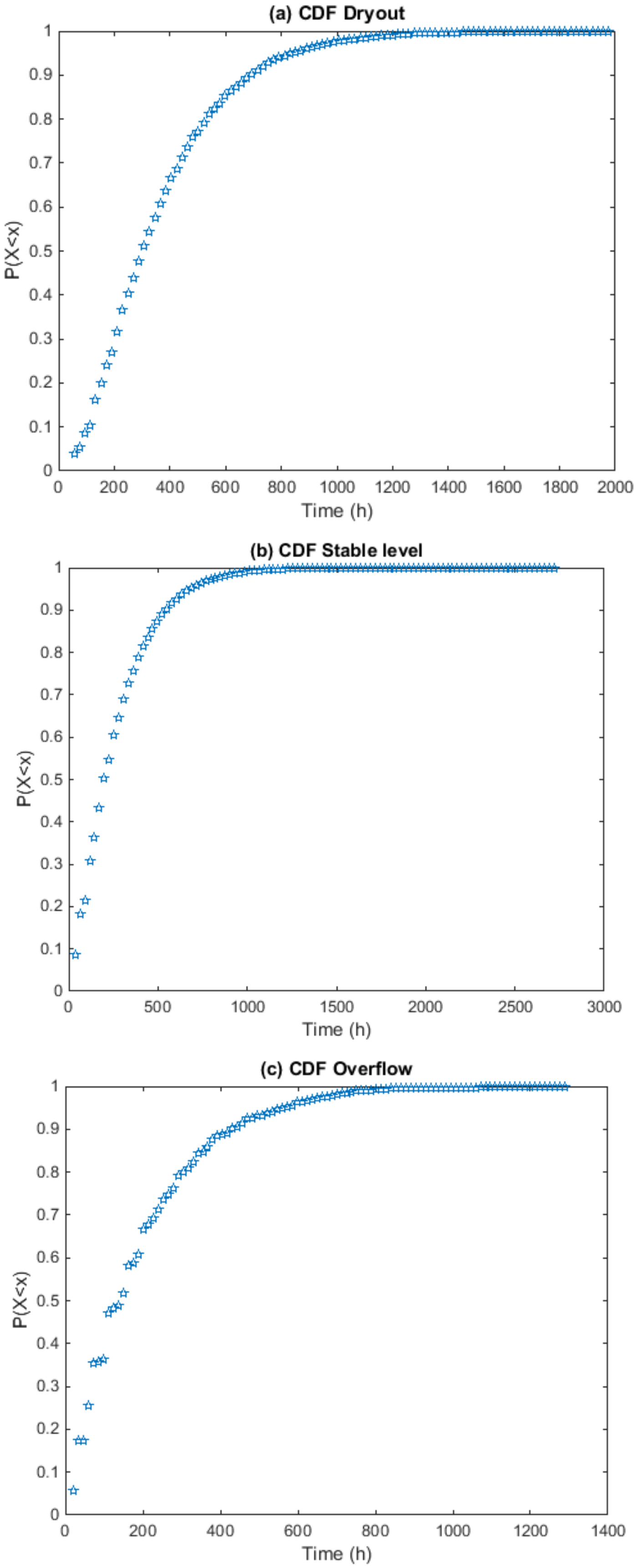


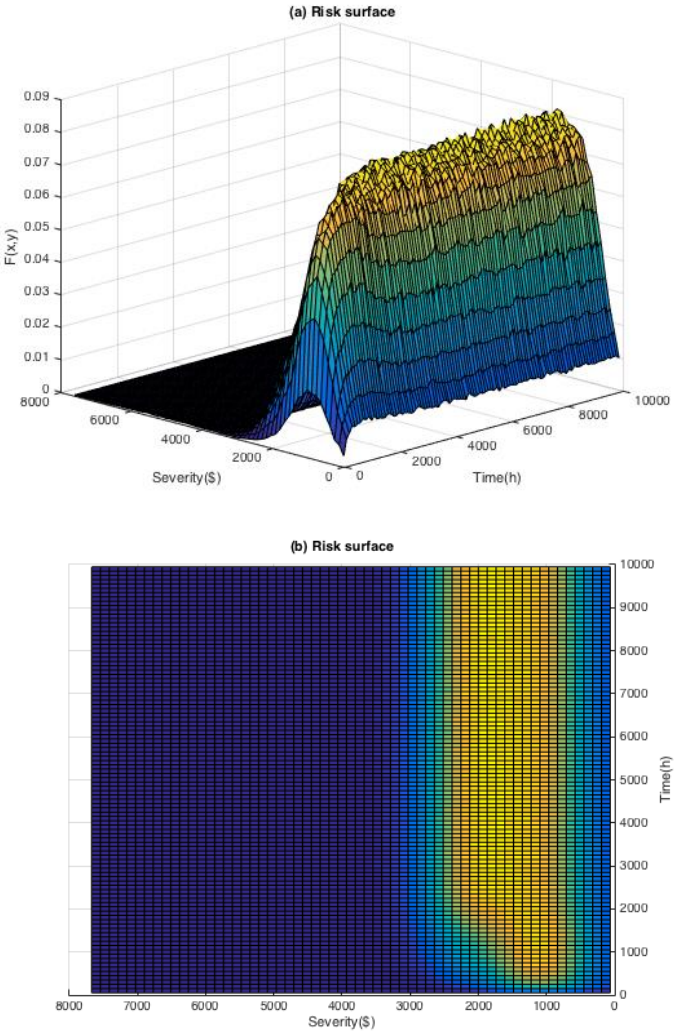
Figure IV 15: Cumulative distribution functions of the holdup tank problem: (a) E2 - Dryout; (b) E3 - Stable level; (c) E4 – Overflow.

Table IV 2: Simulation data of the holdup tank problem.

	Frequency		Severity		
	Probabilistic function	**Discrete probability**	**Probabilistic function**	**Mean**	**Standard deviation**
(E2) Dryout	Figure 16 (a)	17.70%	Normal	$2.000	$500
(E3) Stable level	Figure 16 (b)	80.36%	Normal	$1.000	$500
(E4) Overflow	Figure 16 (c)	1.94%	Normal	$5.000	$1.000

3.2.3. Risk surfaces presentation

The problem was modeled and solved in MATLAB® software using a Monte Carlo procedure with 50,000 histories. The obtained probabilistic density risk surface is shown in Figure 16 and the obtained cumulative risk surface is shown in Figure 17.



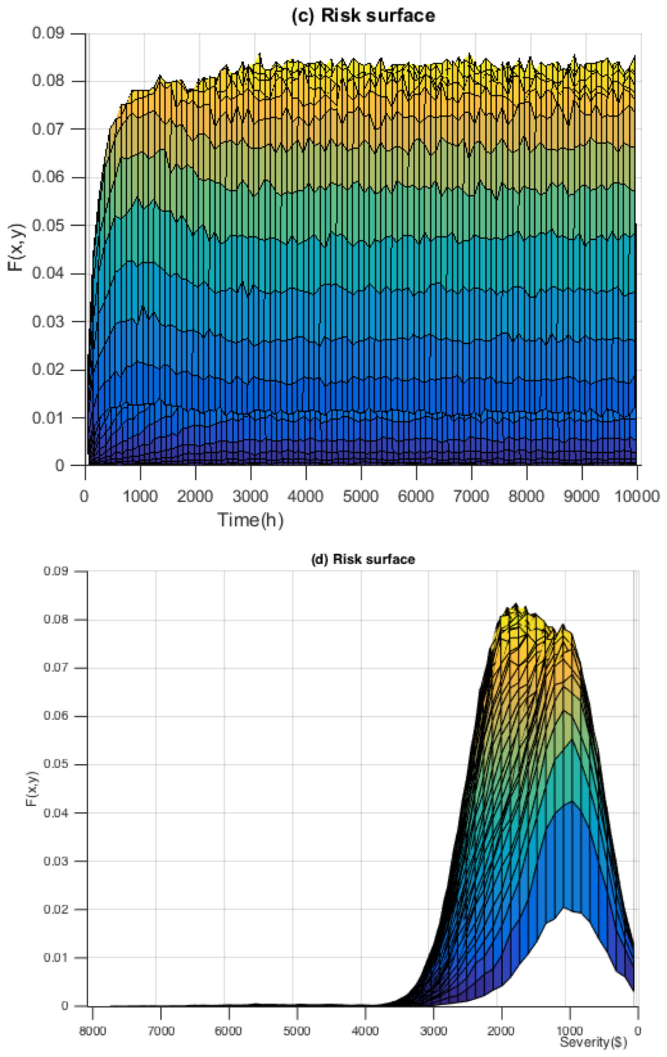
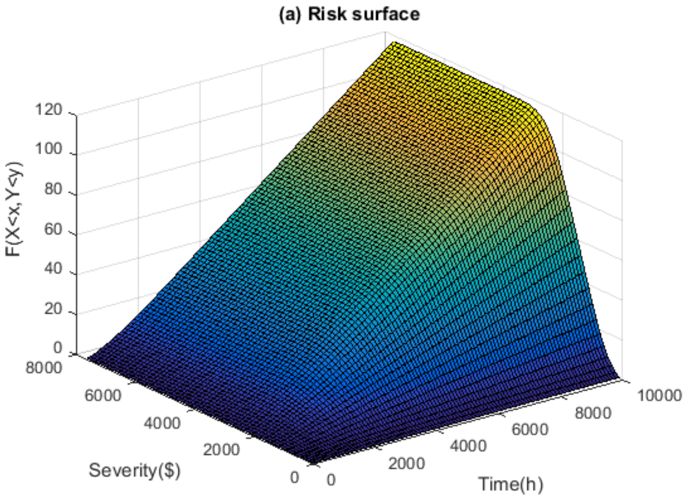


Figure IV 16: Holdup tank - (a) Probabilistic density risk surface; (b) Probabilistic density risk surface upper view; (c) Probabilistic density risk surface in time axis; (d) Probabilistic density risk surface in severity axis.



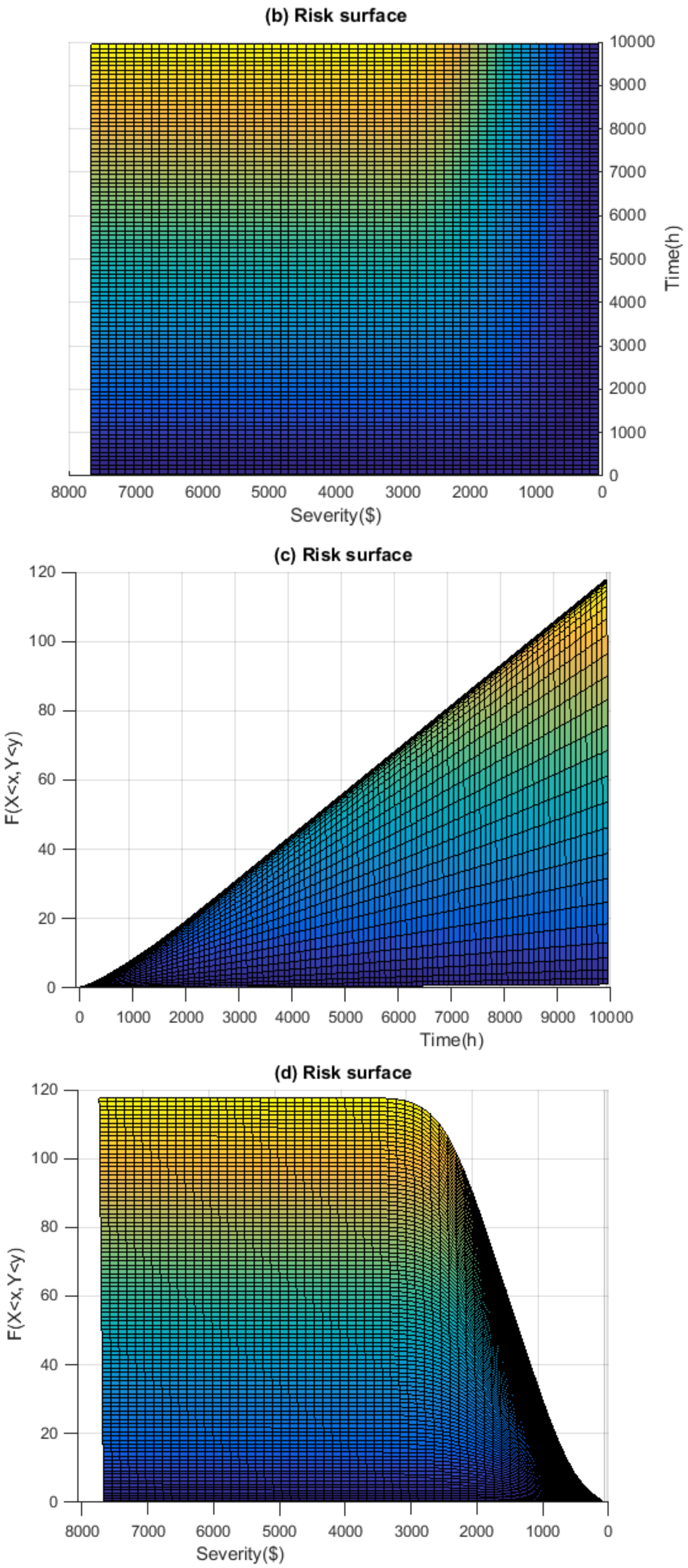


Figure IV 17: Holdup tank - (a) Cumulative risk surface; (b) Cumulative risk surface upper view; (c) Cumulative risk surface in time axis; (d) Cumulative risk surface in severity axis.

3.2.4. Problem observations

Given the connections C4, C5 and C6, a unique process history with 1000 hours may have more than one occurrence of the events E2, E3 or E4. This continuous process evaluation, different from the previous case study, enables a risk surface with frequency axis that exemplifies, as noted in Figure 17, frequency of severities occurrence higher than one.

The obtained risk surface presents variability until the process time reaches 2500 hours, which is represented by the major occurrence of E3 (stable level) due to its higher discrete probability of occurrence (80.36% - Table 2). After that process time, the risk surface remains roughly with the same shape, which is interpreted as a stabilization of the time to occurrence and repair of events E2 and E3. Furthermore, given its small number of occurrences in the process history (discrete probability of occurrence equal to 1.94 – Table 2), E4 occurrence does not change the obtained risk surface much. However, analyzing Figure 16(d), the small contribution of the E4 occurrence given by a very thin line around the severity of $5,000 may be observed.

To deal with the uncertainties, just as discussed in the case study of the pressurized vessel, the representativeness of the state space presented in Figure 14 needs to be checked, the frequency and severity data have to be verified with the expected values of the specialists and, to consider uncertainties, some corrections should be made in the obtained risk surface. Finally, it is important to note that, in a perspective of dynamic update of the risk, one may agree that as the time value of the presented risk surface get higher, higher should be the uncertainty of the estimate risk. In this sense, given an adequate risk management program, the importance of the dynamic update of the risk value over the time is highlighted and can be manageable for a small or a long time period.

4. CONCLUSION

In this work, a new risk interpretation was proposed that considers five variables: the loss to be analyzed (L), the identified event(s) (E), the frequency of the event occurrence (F), the severity of the event (S) and the uncertainties (U). The main contribution that enabled this definition was the organization of the ideas and definitions normally used to describe risk, avoiding the word “consequence” and marking the difference between frequency and uncertainty in order to separate the variabilities that may be calculated from the uncertainties that may not be identified or quantified. Moreover, considering or not considering frequency and severity variability leads to different risk representations: (i) Expected value, (ii) Probabilistic risk curve with variable severity, (iii) Probabilistic risk curve with variable frequency and (iv) Probabilistic risk surface, which is understood as the more complete risk representation. Such achievements led to a wider risk characterization that improves our understanding of uncertainties, black swan events and the relation between the quantitative forecasting risk models and the prosed risk description. The proposed approach was applied in two case studies; in the first the risk of occurrence of a unique event was investigated, while in the second a continuous risky process, including the consideration of process repair connections, was investigated.

The proposed structured risk characterization enables us to choose the visualization of a quantified risk picture that may be in accordance with the data and the sort of decisions to be made. In this sense, the proposed approach deals with some risk drawbacks, providing new technical evidence for better guidance in decision making. The time dimension present in the “Probabilistic risk curve with variable frequency” and in the “Probabilistic risk surface” facilitates the understanding about how the risk varies in time, making it possible to visualize when the process starts to be riskier thereby helping us to anticipate future decisions and to understand how the actions of today influence the long-range risk estimate. In the end, it was possible to combine a dynamic risk assessment, which obtain risk as a function of time, with a dynamic risk update, which aims to update the obtained risk given the dynamic obtainment of new knowledge or data.

5. ACKNOWLEDGMENTS

The present work was accomplished with the CNPq support, Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brasil and CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil.

6. REFERENCES

[1] AIChE, Guidelines for chemical process quantitative risk analysis (2th ed.). New York, 2000. Center for Chemical Process Safety of the American Institute of Chemical Engineers.

[2] Ale, B., Burnap, P., Slater, D., 2015, On the origin of PCDS – (Probability consequence diagrams), Safety Science 72 (2015) 229–239

[3] Amundrud, Ø., Aven, T., 2015, On how to understand and acknowledge risk, Reliability Engineering and System Safety 142 (2015) 42–47

[4] AS/NZS. Risk Management Standard, AS/NZS 4360: 2004. Jointly published by Standards Austra

[5] Apostolakis, G. E., 2004, How Useful Is Quantitative Risk Assessment?, Risk Analysis, Vol. 24, No. 3, 2004.

[6] Aqlan, F., Ali, E. M., 2014, Integrating lean principles and fuzzy bow-tie analysis for risk assessment in chemical industry, Journal of Loss Prevention in the Process Industries 29 (2014) 39e48

[7] Aven, T., 2010, On how to define, understand and describe risk, Reliability Engineering and System Safety 95 (2010) 623–631

[8] Aven, T., 2011, On the new ISO guide on risk management terminology, Reliability Engineering and System Safety 96 (2011) 719–726

[9] Aven, T., 2012, The risk concept - historical and recent development trends, Reliability Engineering and System Safety 99 33–44.

[10] Aven, T., 2013, On the meaning of a black swan in a risk context, Safety Science 57 (2013) 44–51

[11] Aven, T., Krohn, B. S., 2014, A new perspective on how to understand, assess and manage risk and the unforeseen, Reliability Engineering and System Safety 121 (2014) 1–10

[12] Aven, T., 2016, Supplementing quantitative risk assessments with a stage addressing the risk understanding of the decision maker, Reliability Engineering and System Safety 152 51–57.

[13] Aven, T., Ylönen, M., 2016, Safety regulations: Implications of the new risk perspectives, Reliability Engineering and System Safety 149 (2016) 164–171

[14] Berner, C., Flage, R., 2016, Strengthening quantitative risk assessments by systematic treatment of uncertain assumptions, Reliability Engineering and System Safety 151 (2016) 46–59

[15] Borst, M., Schoonakker, H., 2001, An overview of PSA importance measures, Reliability Engineering and System Safety 72 (2001) 241-245.

[16] Bucci, P.; Kirschenbaum, J.; Mangan, A.; Aldemir, T.; Smith, C.; Wood, T., 2008, *Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability*, Reliability and System Safety, 93, 1616-1627.

[17] Campbell, S., 2005, Determining overall risk, Journal of Risk Research 8 (7–8), 569–581

[18] Creed, G. D., 2011, Quantitative risk assessment: How realistic are those frequency assumptions?, Journal of Loss Prevention in the Process Industries 24 (2011) 203e207

[19] Demichela, M., Piccinini, N., 2004. Risk-based design of a regenerative thermal oxidizer. Ind. Eng. Chem. Res. 43, 5838–5845. http://dx.doi.org/10.1021/ie0342208.

[20] Duijm, N. J., Fiévez, C., Gerbec, M., Hauptmanns, U., Konstandinidou, M., 2008, Management of health, safety and environment in process industry, Safety Science 46 (2008) 908–920

[21] Flage, R., Aven, T., 2015, Emerging risk – Conceptual definition and a relation to black swan type of events, Reliability Engineering and System Safety 144 (2015) 61–67

[22] Hauge, S., Okstad, E., Paltrinieri, N., Edwin, N., Vatn, J., Bodsberg, L., 2015. Handbook for Monitoring of Barrier Status and Associated Risk in the operational Phase, the Risk Barometer Approach. SINTEF F27045. Trondheim, Norway.

[23] Haugen, S., Vinnem, J. E., 2015, Perspectives on risk and the unforeseen, Reliability Engineering and System Safety 137 (2015) 1–5

[24] Hopkins, A., 2011, Risk-management and rule-compliance: Decision-making in hazardous industries, Safety Science 49 (2011) 110–120.

[25] Karanki, D.R.; Rahman, S.; Dang, V.N.; Zerkak, O., 2017, *Epistemic and aleatory uncertainties in integrated deterministic and probabilistic safety assessment: Tradeoff between accuracy and accident simulations*, Reliability

[26] ISO, 2009. Risk Management – Vocabulary. Guide 2009.

[27] ISO 31000:2009, 2009. Risk management – Principles and Guidelines. Geneva, Switzerland.

[28] Jocelyn, S., Chinniah, Y., Oualim M. S., 2016, Contribution of dynamic experience feedback to the quantitative estimation of risks for preventing accidents: A proposed methodology for machinery safety, Safety Science 88 (2016) 64–75

[29] Johansen, I. L., Rausand, M., 2015, Ambiguity in risk assessment, Safety Science 80 (2015) 243–251

[30] Jonkman, S. N., van Gelder, P.H.A.J.M., Vrijling, J.K., 2003, An overview of quantitative risk measures for loss of life and economic damage, Journal of Hazardous Materials A99 (2003) 1–30

[31] Kaplan, S., Garrick, B. J., 1981, On the quantitative definition of risk, Risk Analysis, Vol. I, No. I, 1981.

[32] Manno, G; Chiacchio, F.; Compagno, L.; D'Urso, D.; Trapani, N., 2012, MatCarloRe: An integrated FT and Monte Carlo Simulink tool for the reliability assessment of dynamic fault tree, Expert System with Applications, 39, 10334-10342.

[33] Marseguerra, M.; Zio, E., 1996, Monte Carlo approach to PSA for dynamics process systems, Reliability Engineering and system safety, 52, 227-241.

[34] Paltrinieri, N., Scarponi, G.E., Khan, F., Hauge, S., 2014. Addressing dynamic risk in the petroleum industry by means of innovative analysis solutions. Chem. Eng. Trans. 36, 451–456.

[35] Paté-Cornell, M. E., 1996, Uncertainties in risk analysis: Six levels of treatment, Reliability Engineering and System Safety 54 (1996) 95-111

[36] Pidgeon, N., O'Leary, M., 2000, Man-made disasters: why technology and organizations (sometimes) fail, Safety Science 34 (2000) 15-30.

[37] Rae, A., Alexander R., McDermid, J., 2014, Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment, Reliability Engineering and System Safety 125 (2014) 67–81

[38] Raoni, R, Secchi, A., 2018, Procedures to Model and Solve Probabilistic Dynamic System Problems. Article in submission process at Reliab. Eng. Syst. Safe..

[39] Rathnayaka, S., Khan, F., Amyotte, P., 2014, Risk-based process plant design considering inherent safety, Safety Science 70 (2014) 438–464

[40] Sampera, J. B., Guillen, M., Santolino, M., 2016, What attitudes to risk underlie distortion risk measure choices?, Insurance: Mathematics and Economics 68 (2016) 101–109

[41] Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016, Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry, Safety Science 89 77–93.

[42] Vose, D., 2008, Risk analysis – A quantitative guide. John Wiley & Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, Ltd, 3rd ed. ISBN 978-0-470-51284-5.

[43] Yang, X., Haugen, S., 2015, Classification of risk to support decision-making in hazardous processes, Safety Science 80 115–126.

[44] Yang, X., Haugen, S., 2016, Risk information for operational decision-making in the offshore oil and gas industry, Safety Science 86 (2016) 98–109

CHAPTER V - COMPLETE QUANTITATIVE RISK ASSESSMENT USING THE PROPOSED COMPLEMENTARY METHODS

Article submitted to Reliability Engineering and System Safety at 19/01/2018.

THE COMBINATION OF RISK ANALYSIS PROCEDURES BASED ON MONTE CARLO AND DYNAMIC PROCESS SIMULATION FOR QUANTITATIVE RISK SURFACE ASSESSMENT

Rafael Raoni[a], Argimiro R. Secchi[a], Micaela Demichela[b], Serena Bosca[b]

[a] Chemical Engineering Program-COPPE, Universidade Federal do Rio de Janeiro, Cidade Universitária, Centro de Tecnologia, 21941-914 Rio de Janeiro-RJ, Brasil
[b] Department of Applied Science and Technology, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italia
E-mail addresses: rbritto@peq.coppe.ufrj.br (R. Raoni), arge@peq.coppe.ufrj.br (A. R. Secchi), micaela.demichela@polito.it (M. Demichela), d027311@polito.it (S. Bosca).
Corresponding author e-mail address: rbritto@peq.coppe.ufrj.br (R. Raoni)

Abstract: In this work, the procedures to turn three risk analysis methods, described as (i) hazard identification based on device failures and process simulation, (ii) probabilistic investigation of event occurrence of batch and dynamic systems using Monte Carlo simulation, and (iii) three dimension risk representation "time x frequency x severity", complementary among each other is proposed. Given that the three methods were developed in order improve different steps of risk assessment, the main contribution of the work is propose their complementarity, explaining the advantages on using these methods together to manage a quantitative risk assessment. The procedure is applied to investigate the risk of economic loss during the operation of the freeze-drying process. In this freeze-drying case study, four different consequences of device failures were identified and the state space representing the abnormal process behaviors was built and used to obtain the three-dimensional risk surface. In the end, the proposed method is compared with other approaches for integrate risk analysis techniques.

Keywords: Process simulation; Quantitative Risk Assessment (QRA); Risk surface; Freeze Drying; Dynamic batch process.

1. INTRODUCTION

Despite the importance of risk analysis in different areas [33] and to help different kind of decision [40], risk concept is not a consensus in the scientific community [5]. Different risk concepts have been applied to manage risk, being the events probability-of-loss the most dominant one [6, 20, 39]. In order to manage a risk assessment, the identification of (i) the possible accident scenarios, (ii) the consequences, and (iii) the scenarios likelihood are needed [34], and for a complete quantitative risk assessment, the use of complementary methods is necessary.

For hazard identification, multidisciplinary team of experts commonly employs techniques with rigorous procedures to identify the desired kind of hazard [43, 44]. In process industries, HAZOP (*Hazard Operability*) [21, 25, 37] is one of the most recognized and used [45], being suitable to analyze continuous processes. The method aims to identify hazardous consequences of process variable deviations to enable system improvements that eliminate sources of big accidents [18]. Given the importance of the method, improvements such as the use of expert systems to automate the analysis of deviation propagation throughout an empirical model [7, 9, 14, 15, 26, 41], or the use of process simulation to quantify deviations and to understand the process dynamics and non-linearities [24, 27, 29, 36] were proposed. Raoni et al. (2018) [30] proposed a procedure based on devices failures simulation that allows understanding the dependencies among the process variable deviations that feed a heuristic analysis to identify further undesirable consequences.

For likelihood scenarios estimation, the study of dynamic and stochastic system behaviors is normally required. For that, two of the most employed techniques, classified as static models [23], are the Fault Tree (FT) and Event Tree (ET) analyses. Despite the static model application, several other methods are widely employed for probabilistic dynamic system investigation aiming to obtain the time of event occurrence, identified as a continuous random variable. To model and solve the problem, the state-space system representation [34] and the Markov basis are the most employed. The Markov basis has been employed for decades [23], being applied, for example, in the *State Transition Diagram/Graphs* [13] and in the Champman-Kolmogorov equation, which mix probabilistic and deterministic dynamic system analyses [17]. Despite the hard-work task [22], the state-space representation and Markov basis enable the analytic problem resolution. To overcome the difficulties for the analytic resolution, a probabilistic problem resolution based on Monte Carlo (MC) procedure [22, 46] may be used. However, the MC has also its drawbacks, since it requires high computational effort to solve very reliable systems [2, 42]. Despite the most applied methods for probabilistic investigation of events occurrence be separated by static and dynamic methods, Raoni and Secchi (2018a) [31] highlighted procedures that can be followed to analyze system considering the occurrence of discrete events with a dynamic system investigation. In this sense, the event occurrence can be represented by both discrete and continuous random variables.

Finally, the ways to identify the risk have great importance for its understanding. The expected risk value is obtained multiplying frequency and severity values, being one of the most recognized and widely applied in engineering risk representations [3]. Furthermore, the probability-of-loss risk representation may follow a curve, just as the FN (frequency F of N or more number of fatalities) curve [19], or by probability consequence diagrams, in which different events may be represented together in a unique colored diagram that helps to classify the risk [1]. Despite that, Raoni and Secchi, 2018b [32] have shown other risk representation given the specification of the frequency and/or the severity as discrete value or as a probabilistic function of the time or magnitude of the severity, respectively. Considering one of them as a discrete value while the other is a probabilistic function of a continuous random variable, a risk curve may be obtained given their product. Furthermore, risk may also be estimated when both frequency and severity are represented by probabilistic function of continuous random variables, being possible to obtain a risk surface with *"time x frequency x severity"* axes. In this sense, risk may have three different representations: (i) expected value: when frequency and severity are fixed values; (ii) probabilistic risk curve: when one of frequency or severity is a fixed value while the other is represented by a continuous probabilistic function; or (iii) risk surface: when both frequency and severity are represented by continuous probabilistic functions.

As highlighted, different risk analyses may be employed to understand risky process and to manage risk estimation. The main point of this work is that different risk analyses should be applied together to manage a quantitative risk assessment, and the integration of the procedures must be in a way that is possible to manage and reduce uncertainties and errors of interpretation of the final risk result. Some authors have already implemented different combination of risk analyses and, according to Bendixen and O'Neill (1984) [8], the HAZOP and FT is the best combination to identify hazards and evaluate their impacts. Demichela et al. (2002) [16] have also improve the quality of hazard assessment mixing concepts of different risk analysis techniques, developing the Recursive Operability Analysis (ROA) that enables to directly obtain the FT from the HAZOP table results.

In this work, a procedure that integrates the following three complementary methods is introduced and applied in a case study of an economic loss risk investigation of the freeze-drying process:

(i) Hazard identification based on device failures and dynamic process simulation;

(ii) Investigation of the probability of the events occurrence using state-spaces and MC simulation; and

(iii) Three-dimensional *"time x frequency x severity"* risk representation, obtained by MC simulation.

In Section 2, the employed risk characterization is introduced, the method employed to identify hazard scenarios is described, and the procedure that combines the results of the hazard identification, the events frequency of occurrence calculation and the estimated severity to build the risk surface are presented. In Section 3, the freeze-drying process is described, the complementary methods are applied to obtain the risk surface of the economic loss of the process, and a comparison of the proposed method with the literature is discussed. In Section 4, the conclusions of the work are summarized.

2. INTEGRATED PROCEDURE FOR QUANTITATIVE RISK ANALYSIS

2.1. Risk definition

The employed risk characterization, described by Raoni and Secchi (2018b) [32], is dependent on five variables: (L) loss to be analyzed; (E) event; (F) frequency of the event occurrence; (S) severity of the event; and (U) uncertainties. The relation between these five risk variables is shown in Figure 1.

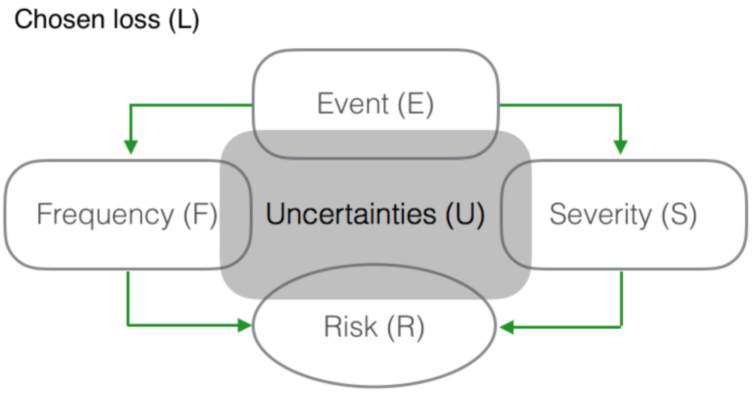


Figure V 1: Relation between the five risk variables.

In such risk representation, the loss (L) identifies the risk analysis focus, or the undesirable consequence with human value [4, 40]; the event (E) represents each scenario that may occur during the process operation that leads to the undesirable loss; the frequency (F) is the estimation of the event frequency of occurrence, which considers both discrete probability and the random time to the event occurrence [31]; the severity (S) is the magnitude of the loss, represented by a probabilistic function; and the (U) represents all uncertainties in the event identification, and in the frequency and severity estimate [32].

2.2. Hazard identification

The hazard identification proposed by Raoni et al. (2018) [30] is employed to identify and analyze process hazardous events (E). Given that process deviations are caused by devices malfunctions, the procedure starts identifying the devices malfunctions to be computationally simulated. The procedure is based on a better interpretation between cause and consequence of the process deviations, enabling an improved hazard empirical analysis. The process interpretation of the employed hazard identification is depicted in Figure 2.

The main characteristics of this method are:

- The process hazard analysis starts from process devices malfunctions;
- Phenomenological process simulation is employed to identify and quantify dependent process variables deviations;
- Simulation results are used as input to hazard heuristic analysis that identifies and analyzes further deviations consequences;
- Hazard identification results are organized as shown in Table 1.

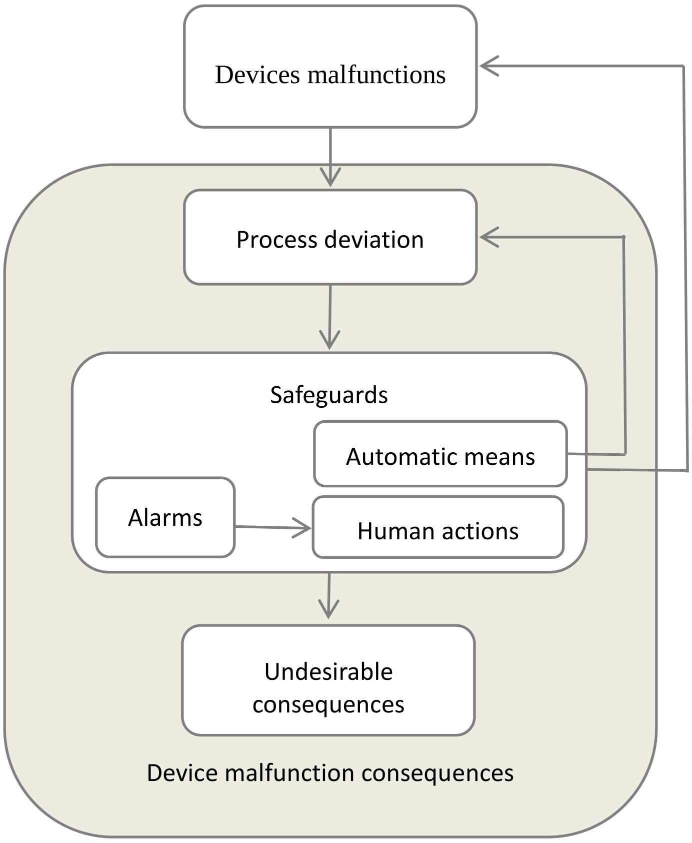


Figure V 2: Process interpretation of the used hazard identification.

Table V 1: Hazard identification table

System under study:						
Device:						
Scenario number:						
Device malfunction	***Simulation results analysis***					
	Variable deviation information		**Deviation safeguards**			
	Variable identification and normal value	**Value under deviation**	**Displayed variable**	**Alarms**	**Automatic means**	**Possibility of human actions?**
	Hazard heuristic analysis					
	Further consequences	**Consequences safeguards**	**Risk assessment:**			**Notes, observations, recommendations**
			Frequency	**Severity**	**Risk**	

To continue the risk assessment of the process, further risk analyses must be employed to quantify the risk. As mentioned, despite the poor dynamic process behavior evaluation, the FT is one of the most employed techniques for complement hazard identification analysis. To improve this step for quantitative risk assessment, the state space representation of the process behavior is the best choice to join the dynamic process behavior with methods for probabilistic dynamic problem resolution. In this sense, the next step of the proposed methods integration for quantitative risk assessment is obtaining the problem state space.

2.3. Obtaining the state space of the process

Following the procedures presented in Raoni and Secch (2018a) [31], the state space of the process may be built. However, given the identified scenarios using the presented hazard identification method, the construction of the state space of the process is facilitated. Given the scenarios of the hazard identification, all device malfunctions of the process are listed together with their dependent process variable deviations and further consequences. In this sense, the abnormal process behaviors are already mapped in a sequenced cause and consequence assumption that follows the natural order of events in an abnormal process condition, being possible to directly obtain the desired state space of the process to be analyzed. To link the hazard identification with the state space building, it is needed to consider the initial state space of the process as its normal operation. Such condition may change to one of each identified scenario of device malfunction, which lead to their dependent process variable deviations and to the identified further undesirable consequences

2.4. Quantitative risk calculation and representation

To conclude the quantitative risk assessment, the frequency of occurrence and the magnitude of the severity of the identified state spaces are required. According to Raoni and Secch (2018a) [31], to calculate the frequency (F) of all the events of the state space, the time to occurrence and the discrete probability of occurrence of the connections between the events are needed, and to calculate the risk as a function of the frequency and severity, the severity magnitude of the connections should be also incorporated in the problem. Finally, the MC procedure should be used to solve the state space problem to obtain the time dependent risk. The state space problem to be solved aims to calculate the probability of occurrence of different severity magnitude over the time, enabling the obtainment of the process three-dimensional "*time x frequency x severity*" risk surface. In Figure 3, the steps to build the risk surface using the proposed integrated procedures are shown.

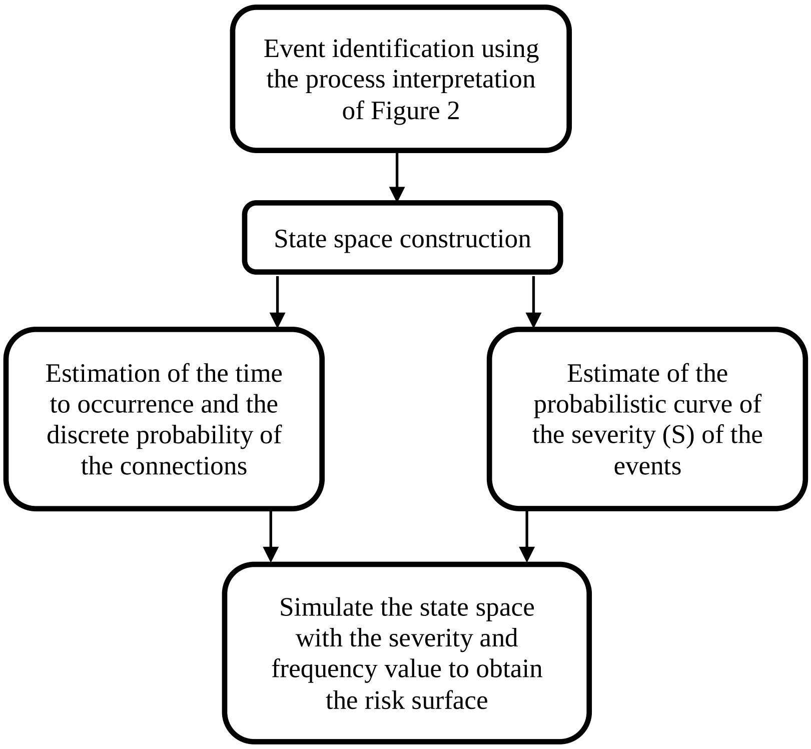

Event identification using the process interpretation of Figure 2
State space construction
Estimation of the time to occurrence and the discrete probability of the connections
Estimate of the probabilistic curve of the severity (S) of the events
Simulate the state space with the severity and frequency value to obtain the risk surface

Figure V 3: Steps to build the risk surface.

3. FREEZE-DRYING RISK ASSESSMENT

3.1. Freeze-drying process

The freeze-drying is a widely applied process, mainly in biological and pharmaceutical areas. Given an aqueous solution with a substance of interest, the process consists of dry off the free water and the water absorbed on the molecules by batch freezing, sublimation and heating processes. The freeze-drying process advantages lay on the easy reconstitution of the dried substance and on drying the solution without damage the characteristics of the substance of interest, what normally occurs when the drying is carried out by a heating process [11]. The freeze-drying process has three steps: (i) the freezing, in which the aqueous solution is cooled down to freeze the free water; (ii) the primary drying phase, in which the free water is sublimated from the solution by lowing the chamber pressure and providing heat; and (iii) the secondary drying, in which the solution is slightly heated and subject to even lower pressure condition to evaporate the adsorbed water on the product molecules [11].

The primary drying is the most important freeze-drying process step, mainly because of the characteristics of the dried product are defined in this stage. During this step, the chamber temperature and pressure are controlled to avoid the degradation or collapse of the dried product cake, which may occur given a high flux of water sublimation. Due to the extreme pressure and temperature conditions maintained during long time, the primary drying has high cost and then the adequate chamber condition is essential to the right and economical process operation [11].

In order to operate the freeze-drying process, a system composed by chamber, pumps and refrigeration cycles, just as shown in the simplified flowchart presented in Figure 4, is needed.

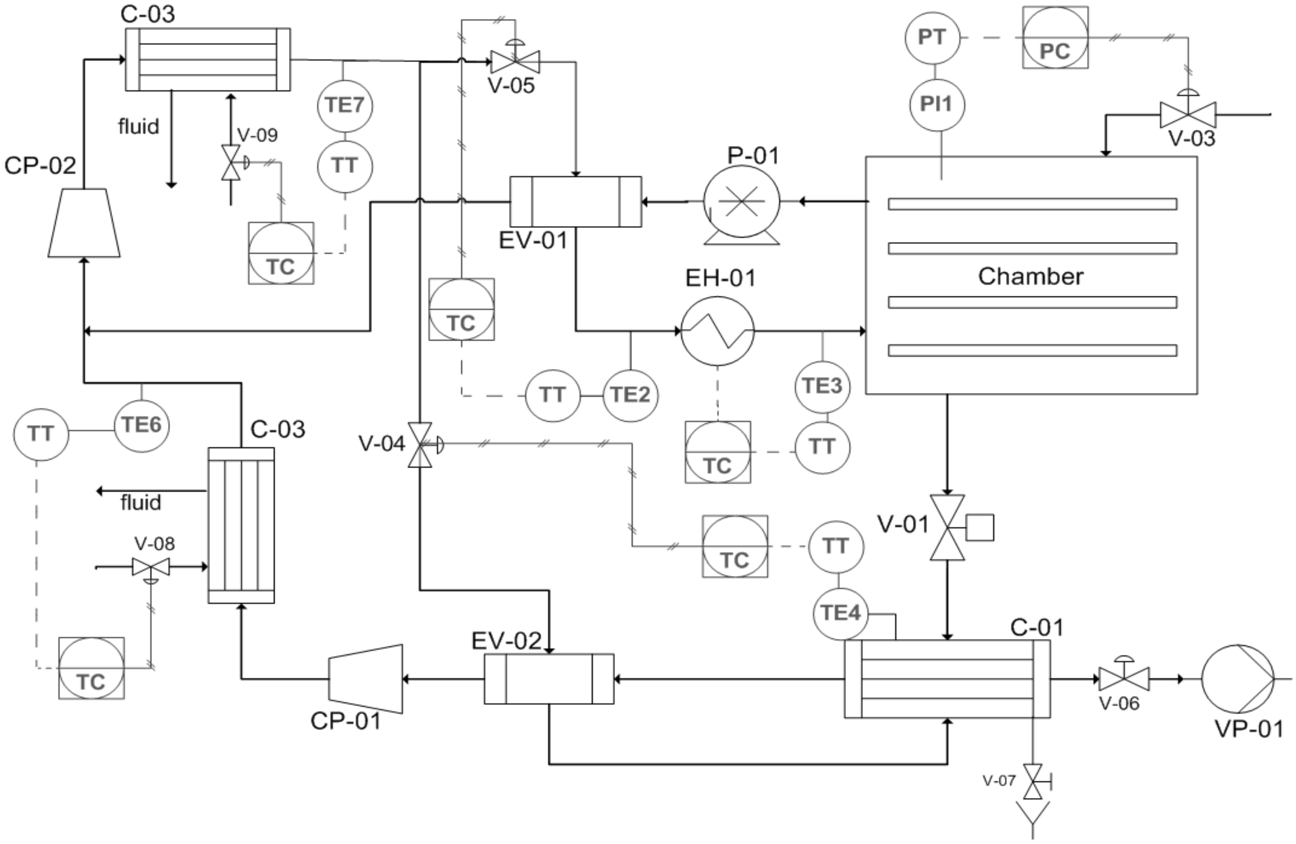


Figure V 4: Simplified flowchart of the Freeze-drying process.

3.2. Freeze-drying hazard identification

The simulated process does not lead to human or environmental damages. However, given the high-cost of the product and to maintain the operation conditions, the risk assessment of the freeze-drying process financial loss (L) was followed. Due to its major importance, the hazard identification was made on the primary drying step in order to identify and to understand the process abnormal behaviors caused by all identified devices malfunctions.

3.2.1. Phenomenological model

The model was built in the dynamic process simulator EMSO [35], considering the follow units, according to Figure 4:

- V-03 and its pressure control system, which manipulate the chamber nitrogen injection;
- Chamber, in which the vials with aqueous solutions are submitted to the three freeze-drying steps;
- The condenser C-01, in which the sublimated water is condensed, and its inlet V-01 valve;
- VP-01 pump for vacuum generation and its inlet valve V-06.

A one-dimensional sublimation model [38] was employed to represent the water sublimation phenomenon in the vials. To solve the model, parameters for the dried cake vapor flux resistance and for the heat transfer between the refrigerant fluid and the vials solution were used. Such parameters are dependent of the product to be dried and were estimated using sucrose aqueous solution experimental data [10]. Despite the process model does not contemplate the refrigeration cycles, responsible to maintain the chamber and condenser temperatures, their devices malfunctions analyses were enabled given simulations of equivalent temperature deviations in the chamber.

3.2.2. Normal operating condition and scenario identification

During the primary drying, the normal operating condition corresponds to the maximum temperature on the sublimation interface equal to 243.15 K, which is the limit temperature before product degradation or cake collapse. This condition is reached by adequate control of pressure and temperature in the chamber. However, increasing the gap between the operating condition and the limit temperature of the sublimation interface increases the drying time, and consequently the operational cost. In the simulated process, chamber pressure and temperature were considered equal to 5 Pa and 253.15 K, respectively, resulting on a primary drying time of 21 hours.

3.2.3. Hazard identification results

Starting from the process normal condition, the devices malfunctions, which identify the hazard scenarios, were simulated. For the analysis of the simulated abnormal process behavior, some variables must be monitored in order to identity their deviations and allow the identification of their further consequences [30]. In Table 2, the analyzed variables are listed and in Table 3 all hazard scenarios and their identified consequences are shown.

Table V 2: Analyzed variables

Variable	Variable description
P_c (Pa)	Chamber pressure
T_c (K)	Chamber temperature
T_i (K)	Sublimation interface temperature
T_{fluid} (K)	Chamber refrigeration fluid temperature
P_{cond} (Pa)	Condenser C-01 pressure
T_{cond} (K)	Condenser C-01 temperature
V_{pump} (m^3/s)	Pump P-01 volumetric flow
T_{dry} (hour)	Primary drying time

Table V 3: Process devices malfunction

Scenario	Malfunction	Consequences
1	**V-03 - N2 valve failure**	
1.1	Valve total closing: x = 0	Higher drying time
1.2	Valve total opening: x = 1	Product damaged (Ti > 243.15 K)
1.3	Valve partial opening: x = 0.223[1]	Lower drying time
2	**EH-01 - Cycle refrigerator heater failure**	
2.1	50 K fluid temperature reduction [2]	The primary drying does not start
2.2	10.1 K fluid temperature reduction [3.1]	Higher drying time
2.3	10.1 K fluid temperature increase [3.2]	Lower drying time
2.4	12 K fluid temperature increase [3.4]	Product damaged (Ti > 243.15 K)
3	**P-01 - Cycle refrigerator pump failure**	
3.1	Pump shut off	The primary drying does not start
4	**V-01 - Inlet condenser valve failure**	
4.1	Valve total close: x = 0	Product damaged (Ti > 243.15 K)
5	**C-01 – Condenser failure**	
5.1	10.1 K condenser temperature increase [3.2]	Lower drying time; lose the chamber pressure control
5.2	18.1 K condenser temperature increase [3.3]	Lower drying time; losing the chamber pressure control;
5.3	20 K condenser temperature increase [3.4]	Product damaged (Ti > 243.15 K)
6	**V-06 - Pump inlet valve failure**	
6.1	Valve total closing: x = 0	Product damaged (Ti > 243.15 K)
6.2	Valve total opening: x = 1	Higher drying time
7	**VP-01 – Pump failure**	
7.1	The pump does not start	Product damaged (Ti > 243.15 K)

[1] limit opening to not damage the product

[2] Equivalent to the failure on start the heater during the transition between the freeze and primary drying process steps

[3] Adequate temperature variation to set a temperature alarm (3.1 low, 3.2 high, 3.3 very high, 3.4 damage to the product)

With exception of the scenarios 2.1 and 3.1, in which the sublimation process does not start, and the scenarios 4.1, 6.1 and 7.1, in which the chamber high pressure instantaneously leads to the product degradation, all scenarios were dynamically simulated to identify process variable deviations and further consequences. In Table 4, the results of the scenarios 1.1, 1.2 and 1.3 are presented, in which their consequences risks were qualitatively estimated following traditional qualitative risk classifications tables. Since the primary drying is a batch process, the process variables normally change over the time. To register the deviations values, it was choose 11 hours after the device malfunction as the sampling time of the presented results.

The employed hazard identification enables a quantitative deviation analysis, being a great advantage in comparison to traditional hazard deviation analyses. Furthermore, analyzing the results presented in Table 4, the following conclusions can be made:

- At Scenario 1.1, the simulated device malfunction increases the primary drying time and leads to some displayed variables deviations (P_c, P_{cond} and V_{pump}), enabling the prediction of new safety alarms.
- At Scenario 1.2, the simulated device malfunction leads to an unacceptable risk. To operate the process in a safer condition, some process or device improvement must be thought, as higher V-03 valve reliability.
- At Scenario 1.3, the V-03 valve opening that would lead to the best operating point was identified. This opening leads to lower drying time without damage the product, meaning that the process can operate in better condition.

These analyses resume the results of all simulated scenarios used to formulate the further probabilistic risk surface. As can be noted, the hazard identification supported by process simulation leads to effective process improvements, such as: (i) alarms and interlocks on the right process variable and with right set point, (ii) identification of equipment/instruments with low reliability, and (iii) identification of improved process operating conditions. However, for a quantitative risk assessment, these results must be used as input in a further risk analysis and, as showed in Figure 3, the next step is to identify the state space that represents all identified abnormal process behavior.

Table V 4: Hazard identification - results of the scenarios 1.1, 1.2 and 1.3.

System under study: Freeze drying process						
Device: V-03						
Scenario number: 1.1						
Device malfunction	***Simulation results analysis***					
	Variable deviation information		**Deviation safeguards**			
	Variable identification and normal value	**Value under deviation**	**Displayed variable**	**Alarms**	**Automatic means**	**Possibility of human actions?**
Valve total closing: x = 0	P_c: 5.00 Pa	2.13	Yes	No	No	Yes, by following the P_c, P_{cond} and V_{pump}
	T_c: 245 K	244.1	No	No	No	
	T_i: 237.2 K	235	No	No	No	
	T_{fluid}: 253.15 k	253.15	No	No	No	
	P_{cond}: 4.99 Pa	2.10	Yes	No	No	
	T_{cond}: 213 K	213.00	No	No	No	
	V_{pump}: 3.5x10^{-3} m^3/s	2.6x10^{-3}	Yes	No	No	
	T_{dry}: 21.11 h	22.92	No	No	No	
	Hazard heuristic analysis					
	Further consequences	**Consequences safeguards**	**Risk assessment:**			**Notes, observations, recommendations**
			Frequency	**Severity**	**Risk**	
	Increase of the drying time	No safeguards	3	4	Marginal	Predicts alarms for P_c and P_{cond}
Scenario number: 1.2						
Device malfunction	***Simulation results analysis***					
	Variable deviation information		**Deviation safeguards**			
	Variable identification and normal value	**Value under deviation**	**Displayed variable**	**Alarms**	**Automatic means**	**Possibility of human actions?**
Valve total opening: x = 1	P_c: 5.00 Pa	47.70	Yes	No	No	Yes, by following the P_c, P_{cond} and V_{pump}
	T_c: 245 K	250.8	No	No	No	
	T_i: 237.2 K	247.5	No	No	No	
	T_{fluid}: 253.15 k	253.15	No	No	No	
	P_{cond}: 4.99 Pa	47.50	Yes	No	No	
	T_{cond}: 213 K	213	No	No	No	
	V_{pump}: 3.5x10^{-3} m^3/s	5.3x10^{-3}	Yes	No	No	
	T_{dry}: 21.11 h	-	No	No	No	
	Hazard heuristic analysis					
	Further consequences	**Consequences safeguards**	**Risk assessment:**			**Notes, observations, recommendations**
			Frequency	**Severity**	**Risk**	
	Damage of the product (Ti > 243.15 K)	No safeguards	3	5	Unacceptable	Predicts alarms for P_c and P_{cond}
Scenario number: 1.3						
Device malfunction	***Simulation results analysis***					
	Variable deviation information		**Deviation safeguards**			
	Variable identification and normal value	**Value under deviation**	**Displayed variable**	**Alarms**	**Automatic means**	**Possibility of human actions?**
Valve partial opening: x = 0.223 (opening limit to not damage the product)	P_c: 5.00 Pa	12.40	Yes	No	No	-
	T_c: 245 K	247	No	No	No	
	T_i: 237.2 K	241	No	No	No	
	T_{fluid}: 253.15 k	253.15	No	No	No	
	P_{cond}: 4.99 Pa	12.35	Yes	No	No	
	T_{cond}: 213 K	213	No	No	No	
	V_{pump}: 3.5x10^{-3} m^3/s	4.4x10^{-3}	Yes	No	No	
	T_{dry}: 21.11 h	19.03	No	No	No	
	Hazard heuristic analysis					
	Further consequences	**Consequences safeguards**	**Risk assessment:**			**Notes, observations, recommendations**
			Frequency	**Severity**	**Risk**	
	Lower drying time	No safeguards	-	-	-	Good process consequence

3.3. State space construction

Given the hazard identification analysis, four further consequences were identified: (E1) lack of primary drying start; (E2) lower drying time; (E3) higher drying time; and (E4) product damaged. Following the natural order of the cause and consequence of the process abnormal behavior obtained during the hazard identification, the relation between the failures of the devices, the process deviation and the further consequences can be directly translated into the representative process state space presented in Figure 5.

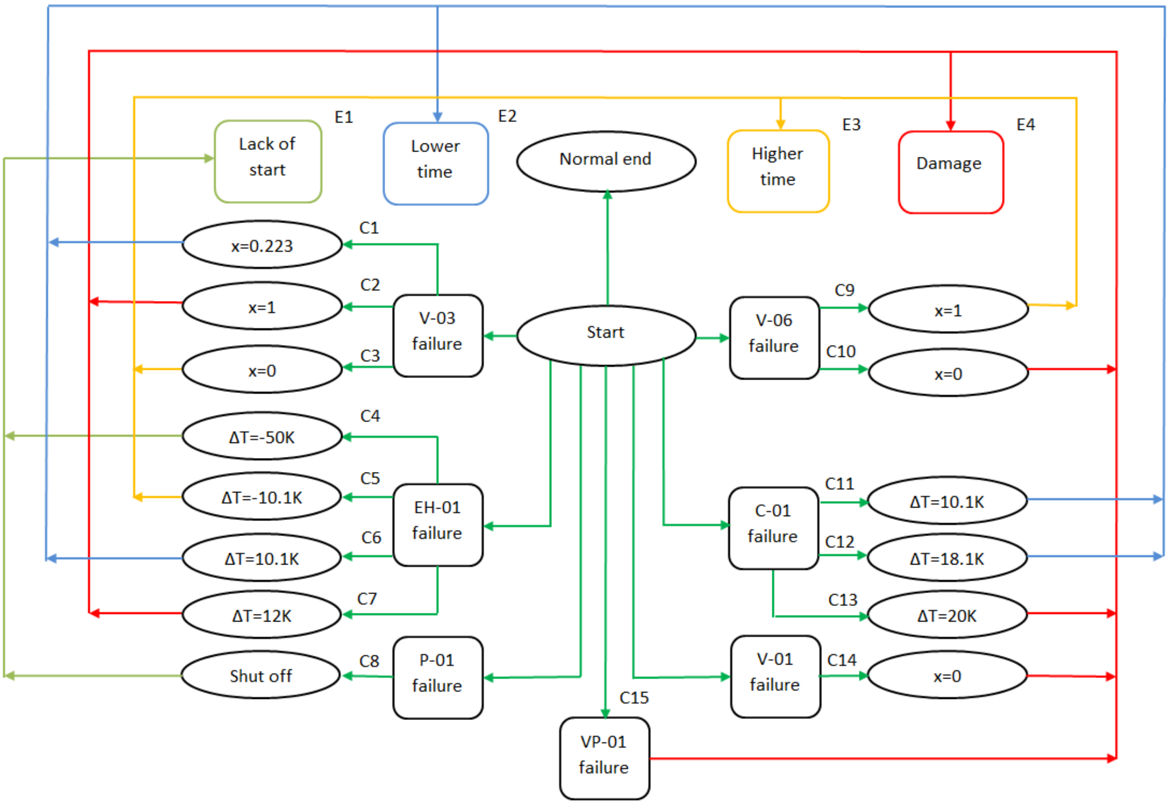


Figure V 5: State space of abnormal primary drying process behavior.

3.4. Probabilities calculation

Despite the economic risk analysis enables the investigation of events with harm and/or positive consequences, the presented work has focused only in harmful economic consequence and then the event (E2) “lower drying time”, which has a positive income, will not be considered in the risk surface. In order to estimate the frequencies (F) of the further consequences, the required time dependency and discrete probability of the connections are shown in Table 5.

Table V 5: Connections probabilistic data

Connection	**Variable dependence**		**Connection**	**Variable dependence**	
	Probabilistic time*	**Discrete****		**Continuous***	**Discrete****
C1	Not investigated		C9	Exp (10^{-2} failures/year)	3x10^{-3}
C2	Exp (10^{-2} failures/year)	2x10^{-3}	C10	Exp (10^{-2} failures/year)	3x10^{-3}
C3	Exp (10^{-2} failures/year)	9x10^{-3}	C11	Not investigated	
C4	Exp (10^{-4} failures/year)	2x10^{-2}	C12	Not investigated	
C5	Exp (10^{-3} failures/year)	-	C13	Exp (10^{-3} failures/year)	-
C6	Not investigated		C14	Exp (10^{-2} failures/year)	3x10^{-3}
C7	Exp (10^{-4} failures/year)	-	C15	Exp (10^{-3} failures/year)	4x10^{-2}
C8	Exp (10^{-4} failures/year)	4x10^{-2}			

*Time failure probability according to the first operation of the unit, with “Exp” representing the exponential distribution

**Probability of failure on the start of the primary drying process

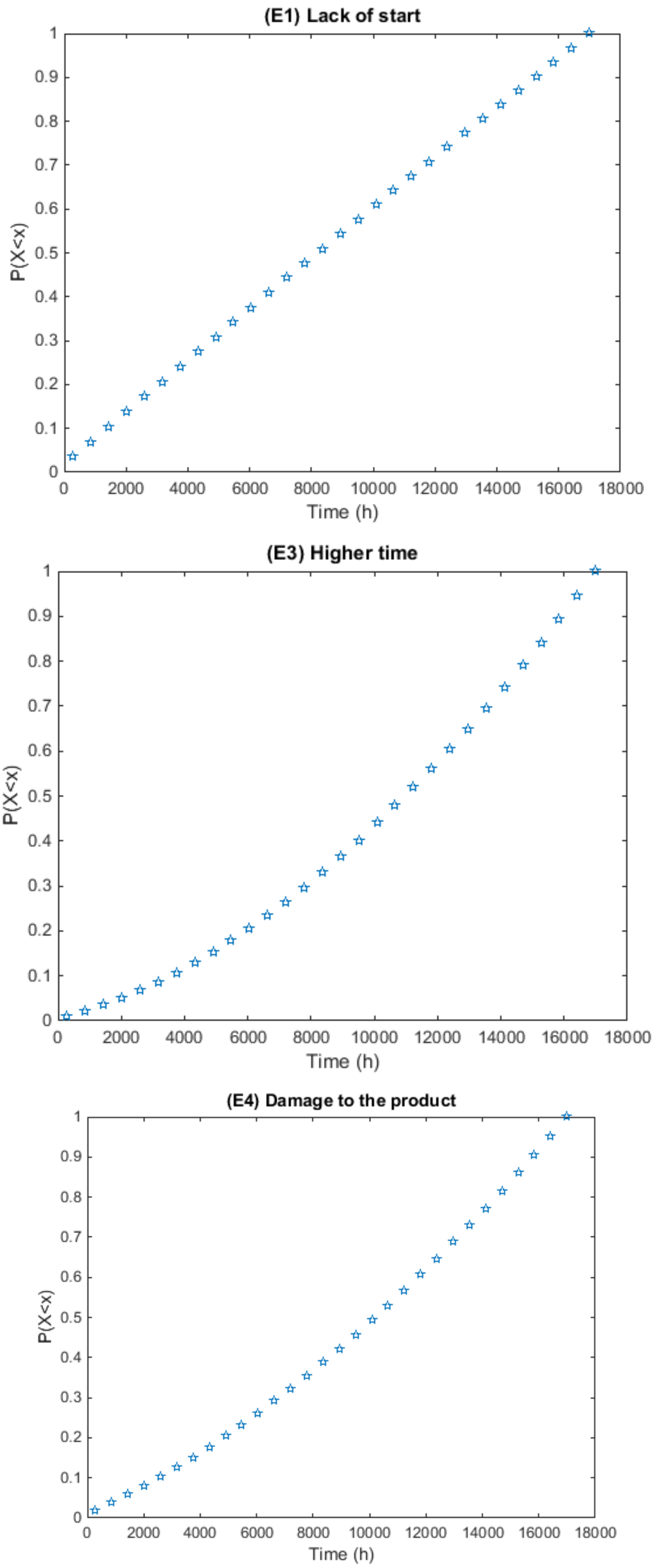
In order to simulate the batch process in a continuous time of two years, it was considered that the process returns to its initial condition after a period of time that follows a normal distribution function with parameters dependent of the occurred failure as shown in Table 6.

Table V 6: Probabilistic parameters to process restart

Connection	**Normal distribution function**		**Connection**	**Normal distribution function**	
	Mean (h)	**Standard deviation (h)**		**Mean (h)**	**Standard deviation (h)**
Normal*	24	0	C8	24	2.4
C1	Not investigated		C9	12	1.2
C2	72	7.2	C10	12	1.2
C3	72	7.2	C11	Not investigated	
C4	24	2.4	C12	Not investigated	
C5	12	1.2	C13	24	2.4
C6	Not investigated		C14	12	1.2
C7	12	12	C15	24	2.4

*After a normal operation, a period of 24 hour is required to start the next operation

Following the simulation steps proposed by Raoni and Secchi, 2018a [31], a Monte Carlo simulation with 10,000 histories (each history simulating two years period) was employed to obtain the probability of occurrence of each event in one batch process, and also their frequency of occurrence over the period of two years. In each Monte Carlo simulation, several batch processes may occur, including normal and abnormal operations. The occurrence time dependency of the three consequences is shown in Figure 6, and their discrete probability of occurrence is shown in Table 7.



(E1) Lack of start

(E3) Higher time

(E4) Damage to the product

Figure V 6: Time cumulative distribution functions (CDF): (E1) Lack of start; (E3) Higher primary drying time; (E4) product damage.

Table V 7: Discrete probability of consequences

MC trials = 10000 / Number of batches = 6803166			
Consequence	**Nº occurrences**	**Probability (%)***	**Frequency****
(E1) Lack of start	385,621	5.67	38.56
(E3) Higher primary drying time	285,210	4.19	28.52
(E4) Product damaged	603,938	8.88	60.39

*Probability of occurrence during one batch operation (Nº occurrences/Number of batches).

**Frequency of occurrence during the two years horizon (Nº occurrences/MC trials)

The cumulative distribution functions present in Figure 6 show the event occurrence probability over the time already considering that the events have occurred. To calculate the event occurrence probability in a batch process in a specified time, or even the frequency of the event occurrence in a specified time, the product of the discrete probability or frequency of the event occurrence (obtained from Table 7) and the probability of the event occurrence in the specified time (obtained from Figure 6) is required. The equation of this product is shown in Equation (1).

$$Pe(t_j)_i = Pe_i \times CDF(t_j)_i \tag{1}$$

where $Pe(t_j)_i$ is the probability of the event i to occur in the interval t = [0, t_j]; Pe_i is the probability (or frequency) of the event i occurrence; and $CDF(t_j)_i$ is the event i cumulative distribution value, which defines the occurrence probability of the event i between time 0 and t_j.

3.5. Primary drying risk surface

To build the risk surface, the estimates of the probabilistic function of the events severities are shown in Table 8. Furthermore, the (E5) “Product damaged” event occurrence, leads to an extra severity amount of $300,000.00, which represents the product loss in the chamber.

Table V 8: Failures severities

Connection	Normal distribution		Connection	Normal distribution	
	Mean ($)	**Standard deviation ($)**		**Mean ($)**	**Standard deviation ($)**
C1	Not investigated		C9	$2,000	$1,000
C2*	$5,000	$1,000	C10*	$2,000	$1,000
C3	$5,000	$1,000	C11	Not investigated	
C4	$5,000	$3,000	C12	Not investigated	
C5	$3,000	$1,000	C13*	$5,000	$2,000
C6	Not investigated		C14*	$2,000	$1,000
C7*	$3,000	$1,000	C15*	$7,000	$4,000
C8	$5,000	$3,000	-		

*Connections that lead to the (E5) “Product damaged” event.

Given the identified events and the estimates of frequencies and severities, the primary drying risk surface can be obtained. To obtain the risk surface, the same state space solved to obtain the frequencies of the final event was used, but now also computing the relative severities of the connections. In the end of state space resolution, a bunch of severity values over the time for each Monte Carlo simulation was obtained, enabling to build the “*time x frequency x severity*” risk surface [32].

Because of the severity magnitude caused by the “Product damaged” consequence, the risk surface presents two separated peaks, one in which the product loss occurs and other in which it does not occur. Figure 7 shows the probabilistic density risk surface peak in which the “Product loss” does not occur and Figure 8 shows probabilistic density risk surface peak in which the “Product loss” does occur. The risk surface representations are equivalent to a three-dimensional probability density function.

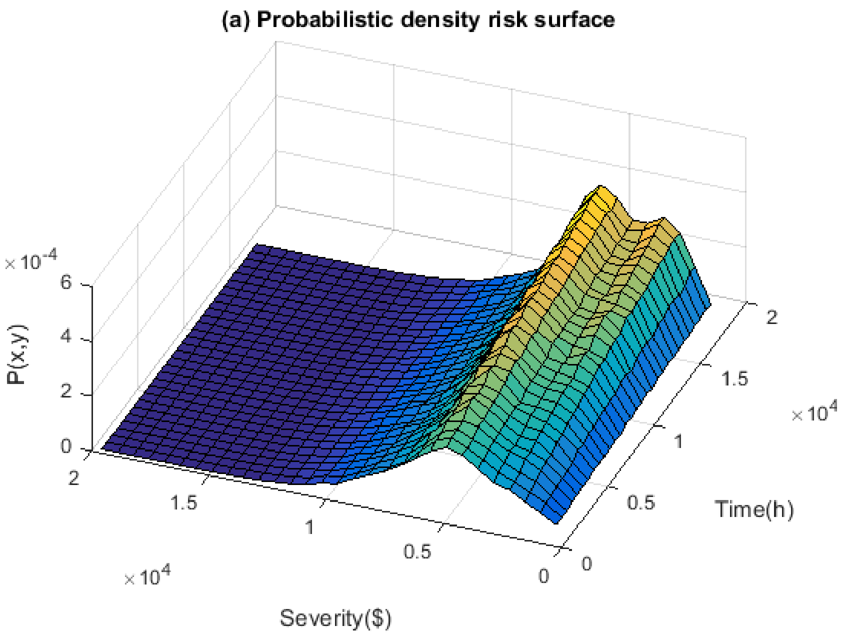


Figure V 7: Primary drying probabilistic density risk surface without product loss

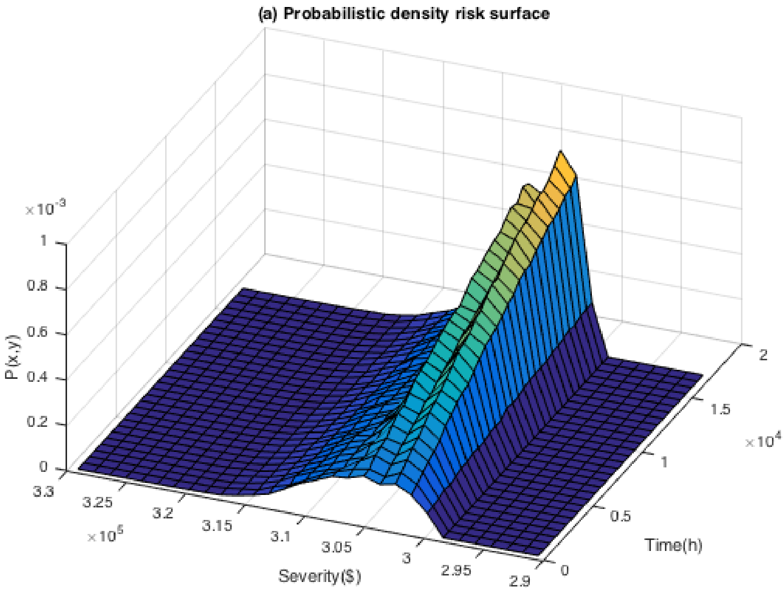


Figure V 8: Primary drying probabilistic density risk surface with product loss

The primary drying cumulative risk surfaces peaks in which the “Product loss” does not occur and does occur are shown in Figure 9 and Figure 10, respectively. Such risk surface representation is equivalent to a three-dimensional cumulative distribution function.

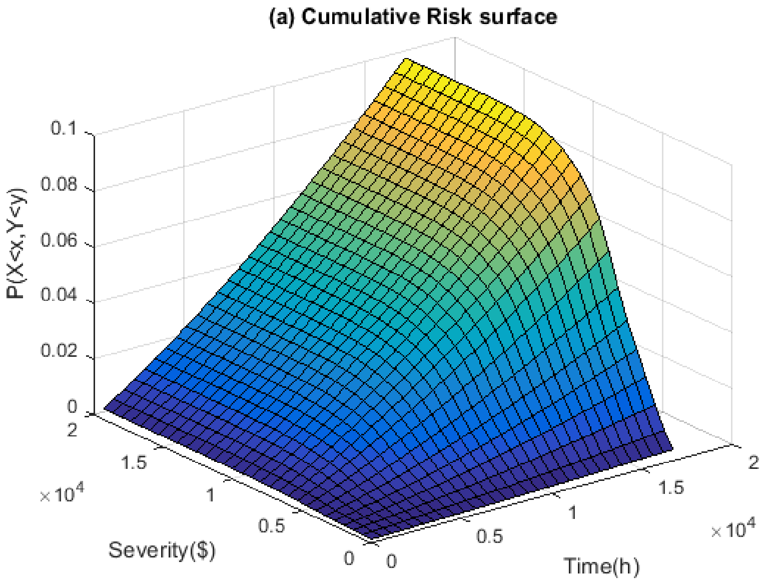


Figure V 9: Primary drying cumulative risk surface without loss of product

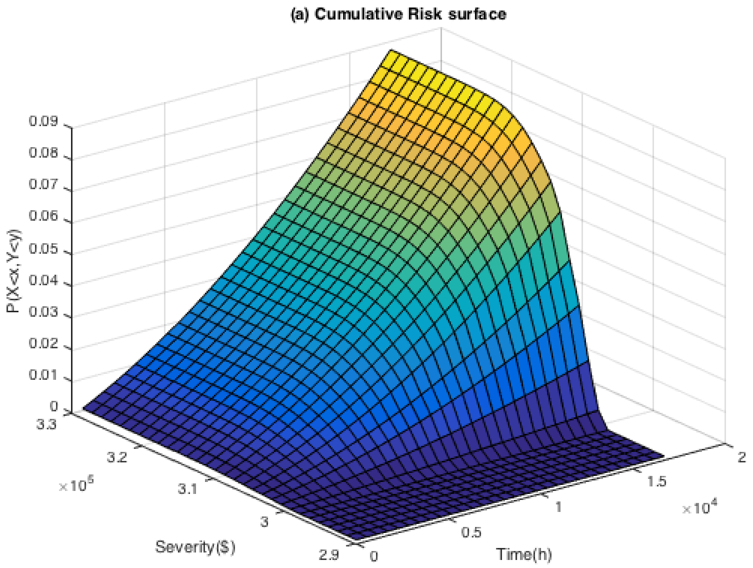


Figure V 10: Primary drying cumulative risk surface with loss of product

All presented risk surfaces were plotted considering the probability of the events occurrences during a unique primary drying batch process, using the probability of the event occurrence showed in Table 7. The risk surfaces show, in one axis, the probability to occur the severity magnitude in the time given one batch process. However, the risk surface may be also plotted considering the frequency of the severity occurrence in all time history, leading to a frequency axis, instead of a probability axis, in the risk surface. For that, the analysis of an uninterrupted process is considered, leading to more than one occurrence of the severity magnitude in some desired time. In this sense, what defines the frequency is the number of occurrence of the identified severity value in a specified time, given the total number of MC simulation, instead of given the number of batch process (see Table 7). Figure 10 shows the cumulative risk surfaces with frequency axis of the primary drying batch process.

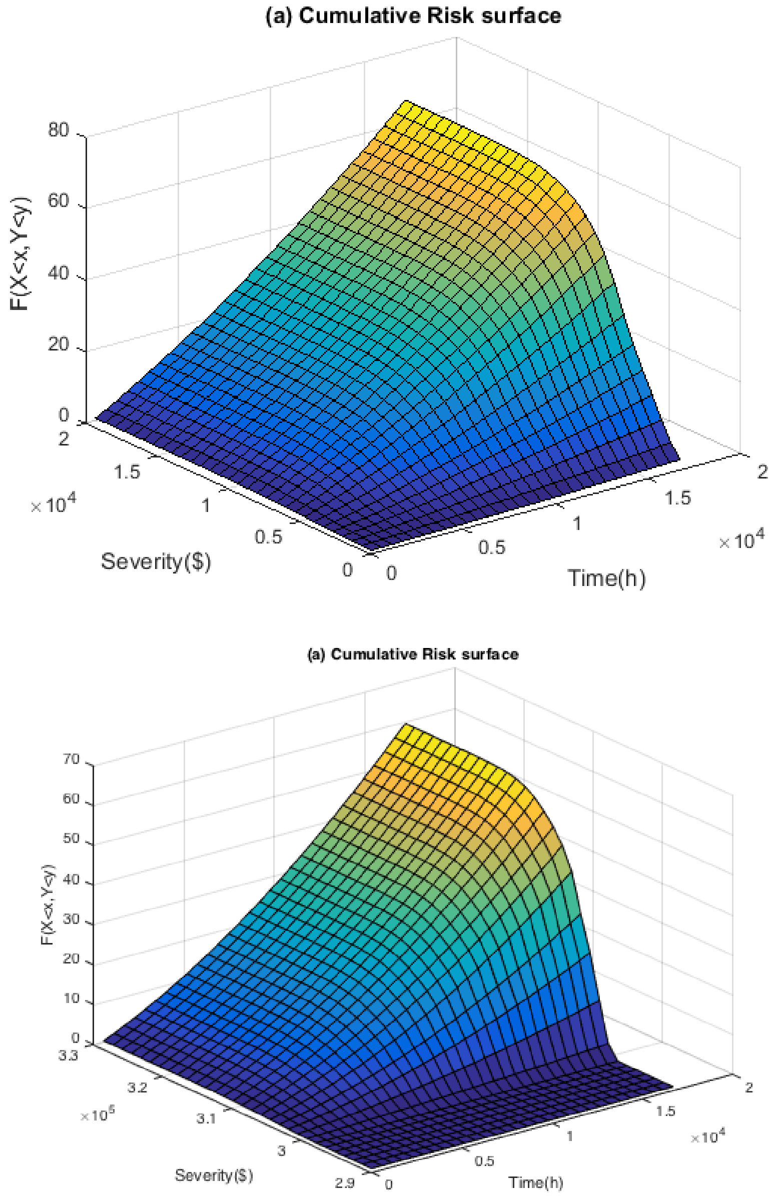


Figure V 11: Frequency primary drying cumulative risk surface normal view (a) without loss of product; (c) with loss of product.

3.6. Primary drying risk interpretation

Analyzing the cumulative risk surfaces, the maximum probability value of the primary drying cumulative risk surface without loss of product (Figure 9) is the sum of the probabilities of the (E1) “Lack of start” and (E3) “Higher primary drying time” presented in Table 7; and the maximum probability value of the primary drying cumulative risk surface with loss of product (Figure 10) is the probability of (E4) “Product damaged”. Analogously, the frequencies presented in Table 7 can be observed in the surfaces presented in Figure 10. Furthermore, analyzing Figures 7 and 8, different events, with different severities and probabilities, are contributing to form the two peaks of the probabilistic density risk surface.

The surfaces enable to visualize the probability and frequency variation over the time and severity, introducing a new way to understand risk. Considering the use of the risk surface to mitigate risky operations, risk acceptance criteria must be employed. Knowing that risk acceptance criteria must not vary over the time, the maximum frequency/probability of some defined severity must be set. For example, if the acceptance criteria do not allows probability higher than 8% for severity higher than \$3.2x10^5, by analyzing Figure 9, the process starts to be unsafe approximately after 15,576 hours requiring some actions to risk mitigation.

According to the used risk definition, uncertainty must be considered. Due to analysts’ lack of the knowledge and unknowns, the analyses present errors, during the event identification and frequency and severity estimations, which affect the obtained risk results [32]. Therefore, despite employing the best available knowledge and this sequential procedure that minimize the errors between the connection of the three risk analyses, the risk surface cannot be taken as exact information, needing to be used to make risk informed decisions.

3.7. Comparing integrated procedures for risk quantification

The presented example has used the integration of complementary methods for risk quantification. As an example, the Recursive Operability Analysis (ROA) [16, 28] improves the quality of risk assessment integrating concepts of the HAZOP for hazard identification and Fault Tree analysis for risk quantification. Despite that, the employment of the hazard identification based on device failures and process simulation enables a quantified deviation analysis that is in accordance with the temporal cause and consequence events of the abnormal process behaviors, presenting some advantages when compared with the HAZOP [30]. Such characteristics enable the direct construction of the state space that groups all dependent process variables deviations that lead to further unwanted consequences. In this sense, differently of FT that requires one tree for each identified top event, a unique state space may be built to represent all the abnormal process behaviors.

As shown, the risk surface is obtained by a procedure that starts from an advanced hazard identification that facilitate the construction of the process state space that needs the input of the frequency and severity values of the connections to be solved by the MC procedure. Solving the state space of the process, the calculation of the frequencies of final events that considers both discrete and time dependency probability, and also the magnitude of the severity represented by probabilistic function is enabled. Such calculation embraces the static result of the FT, the dynamic result of time dependency reliability problems, and also the variability of the severity magnitude. Furthermore, the obtained risk surface representation assembles more information when compared with, for example, (i) the risk as an expected value, (ii) the probability result of the top-event of the FT analysis, or (iii) the time dependency probabilistic curve of reliability problems.

Bosca et al. (2017) [12] have used the ROA to build three FTs and to obtain the probability of the top events, the minimal cut-sets and the contribution of each primary cause to the unavailability of the freeze drying process. Despite the importance of each result, the obtained risk surface has enabled a risk visualization that considers together all the process abnormal behaviors, taking also into account the magnitude of the severity of each event, instead of only the unavailability, over the time. However, the analysis of each primary cause contribution in the risk surface, done by Bosca et al. (2017) [12] is an important issue not embraced in the presented work and should be done in order to allow better actions to reduce the obtained process risk.

4. CONCLUSION

The presented work has proposed the integration of new and complementary methods to manage a quantified risk assessment. Given the batch operation condition, what requires more attention during all employed the risk analyses, the freeze-drying process was chosen to exemplify the proposed integration. The application of the (i) hazard identification based on device failures and process simulation, (ii) probabilistic investigation of event occurrence of batch and dynamic systems, (iii) three-dimensional risk representation *“time x frequency x severity”* leaded to improved results for risk quantification.

The employed hazard identification method enabled the quantification of all process variables deviations that are dependent of the analyzed device failure, enabling to obtain important information about abnormal process conditions. Comparing the method with traditional hazard analysis (HAZOP), the method presents advantage on adequate its procedure to incorporate process simulation to improve the deviation analysis without disregarding the expert opinion importance. In freeze-drying economic loss risk, the identification of several devices failures and their dependent process variables deviations leaded to four consequences: three with harmful impacts and one that indicates possibility of operational improvements.

Since the applied hazard identification analysis follows the natural order of cause and consequence of events occurrence during a real process operation, the building of the state space to investigate the probability of the events occurrence was facilitated. In the freeze-drying process, the procedure based on state space model solved by Monte Carlo, with event connections that consider discrete probability and time as continuous random variable, were employed to calculate the three identified harmful events discrete probability and random time dependence. Combining this probabilistic information about the events occurrence with their severity magnitudes, represented by probabilistic functions, the risk surfaces that represent the probability of specified severity and length of time were obtained solving a unique state space problem. This risk representation enables to visualize the most important information about risk (severity magnitude, frequency of occurrence and time) through a probabilistic density or cumulative risk surface. This visualization enables to identify the time when the process starts to have an unacceptable frequency and severity pair. In the freeze-drying case, the process is unsafe after approximately 15,576 hours given the unacceptable criteria of probability higher than 8% for severity higher than $\$3.2\text{x}10^5$.

The connection between the hazard identification with the state space building enabled the direct obtainment of the model that enables the frequency of occurrence of the identified events calculation. Furthermore, before solving the state space to obtain the frequency result, the specification, at the same problem, of the severity magnitude of the events, which may also be represented by probabilistic function, enabled the resolution of a unique problem that leads to the risk surface that represented together the frequency, the time and the severity of the process. In this sense, after the hazard identification, a unique problem that only needs the specification of the frequency and severity values must be solved to obtain an improved risk representation. These steps reduce the errors on linking risk analyses, reducing the uncertainties of the risk estimation, which is an intangible risk dimension with huge impact in the main risk objective that is correctly predicting unwanted futures behaviors.

5. ACKNOWLEDGMENTS

The present work was accomplished with the support of CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brasil and CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil.

6. REFERENCES

[1] Ale, B., Burnap, P., Slater, D., 2015, On the origin of PCDS – (Probability consequence diagrams), Safety Science 72 (2015) 229–239

[2] Alejandro, D., D., G.; John, G., K.; Joel, E., S.; Jefferey, J., Z., 2008, An integrated methodology for the dynamic performance and reliability evaluation of fault-tolerant systems, Reliability and System Safety, 93, 1628-1649.

[3] Aven, T., 2010, On how to define, understand and describe risk, Reliability Engineering and System Safety 95 (2010) 623–631

[4] Aven, T., 2011, On the new ISO guide on risk management terminology, Reliability Engineering and System Safety 96 (2011) 719–726

[5] Aven, T., 2012, The risk concept - historical and recent development trends, Reliability Engineering and System Safety 99 33–44.

[6] Aven, T., Ylönen, M., 2016, Safety regulations: Implications of the new risk perspectives, Reliability Engineering and System Safety 149 (2016) 164–171

[7] Bartolozzi V., Castiglione L., Picciotto A., Galluzzo M., Qualitative models of equipment units & their use in automatic HAZOP analysis. Reliability Engineering & System Safety 70 (2000) 49–87.

[8] Bendixen, L., O'Neill, J.K., Chemical plant risk assessment using HAZOP and fault tree methods, Plant/Operations Progress 3 (3) (1984) 179–184.

[9] Boonthum N., Mulalee U., Srinophakun, T., A systematic formulation for HAZOP analysis based on structural model. Reliab. Eng. Syst. Saf. 121 (2014) 152-163.

[10] Bosca, S; 2013, Product quality monitoring and cycle design in a freeze-drying process, Ph.D Thesis, Dottorato di Ricerca in Ingegneria Chimica XXVI Ciclo – Politecnido di Torino.

[11] Bosca, S.; Barresi, A.; Fissore, D.; Demichela, M., 2015, Risk assessment for the freeze-drying process of pharmaceuticals in vials, 7th European Meeting on Chemical Industry and Environment (EMChIE 2015).

[12] Bosca, S.; Fissore, D.; Demichela, M., 2017, Reliability Assessment in a Freeze-Drying Process, Ind. Eng. Chem. Res. 2017, 56, 6685−6694.

[13] Chiacchio, F.; Compagno, L.; D'Urso, D.; Manno, G.; Trapani, N., 2011, *Dynamic fault tree resolution: A conscious trade-off between analytical and simulative approach*, Reliability Engineering and System Safety, 96, 1515-1526.

[14] Cocchiara M., Bartolozzi V, Picciotto A, Galluzzo M., Integration of interlocks system analysis with automated HAZOP analysis. Reliability Engineering & System Safety 74 (2001) 99-105.

[15] Cui L., Zhao J., Zhang R., The integration of HAZOP expert system and piping and instrumentation diagrams. Process Saf. Environ. Prot. 88 (2010) 327–334.

[16] Demichela M., Marmo L., Piccinini N.,Recursive operability analysis of a complex plant with multiple protection devices, Reliab. Eng. Syst. Saf. 77 (2002) 301–308.

[17] Devooght, J.; Smidts, C.; 1996, Probabilistic dynamics as a tool for dynamic PSA, Reliability and System Safety, 52, 185-196.Franks, F., 2007. Freeze-Drying of Pharmaceuticals and Biopharmaceuticals. Cambridge: Royal Society of Chemistry.

[18] Dunjó J., Fthenakis V., Vílchez J. A., Arnaldos J., Hazard and operability (HAZOP) analysis. A literature review. J. of Hazard. Mater. 173 (2010) 19-32.

[19] Jonkman, S. N., van Gelder, P.H.A.J.M., Vrijling, J.K., 2003, An overview of quantitative risk measures for loss of life and economic damage, Journal of Hazardous Materials A99 (2003) 1–30

[20] Kaplan, S., Garrick, B. J., 1981, On the quantitative definition of risk, Risk Analysis, Vol. I, No. I, 1981.

[21] Kletz T. A., Hazop-past and future. Reliab. Eng. Syst. Saf. 55 (1997) 263-266.

[22] Labeau, P. E., 1996, *A Monte Carlo estimation of the marginal distributions in a problem of probabilistic dynamics,* Reliability Engineering and System Safety, 53, 65-75.

[23]Labeau, P. E.; Smidts, C.; Swamaiathan, S., 2000, Dynamic reliability: Towards an integrated platform for probabilistic risk assessment. Reliability Engineering and System Safety, 68, 219-254.

[24] Labovsky J., Svandova Z., Markos J., Jelemensky L., Model-based HAZOP study of a real MTBE plant. J. of Loss Prevention Ind. 20 (3) (2007) 230-237.

[25] Lawley H. G., Operability studies and hazard analysis, Chem. Eng. Prog. 70 (4) (1974) 45-56.

[26] Leone H., A knowledge-based system for hazard studies – The Knowledge representation structure. Computers & Chemical Eng. 20 (1996) 269-274.

[27] Li S., Bahroun S., Valentin C., Jallut C., De Panthou F., Dynamic model based safety analysis of a three-phase catalytic slurry intensified continuous reactor J. of Loss Prevention Ind. 23 (2010) 437-445.

[28] Piccinini, N.; Ciarambino, I. Operability analysis devoted to the development of logic trees. Reliab. Eng. Syst. Safe. 55 (1997) 227.

[29] Ramzan N., Compart F., Witt W., 2006, Methodology for the Generation and Evaluation of Safety System Alternatives Based on Extended Hazop. AlChe 26 (1) (2006) 35-42.

[30] Raoni, R.; Secchi, A.; Demichela, M., 2018, Employing process simulation for hazardous process deviation identification and analysis. Safety Science 101 (2018) 209–219.

[31] Raoni, R.; Secchi, A., 2018a, Procedures to model and solve probabilistic dynamic system problems. Article in submission process at Reliab. Eng. Syst. Safe..

[32] Raoni, R.; Secchi, A., 2018b, Better risk understanding for a quantitative risk surface assessment. Article in submission process at Reliab. Eng. Syst. Safe..

[33] Sampera, J. B., Guillen, M., Santolino, M., 2016, What attitudes to risk underlie distortion risk measure choices?, Insurance: Mathematics and Economics 68 (2016) 101–109

[34] Siu, N., 1994, Risk assessment for dynamic systems: An overview. Reliability, Engineering and System Safety 43, 43-73.

[35] Soares, R. P., Secchi, A. R., EMSO: A new environment for modelling, simulation and optimization, Computer Aided Chemical Engineering, 14 (C) (2003), 947-952.

[36] Svandova Z., Jelemensky L., Markos J., Molnar A., Steady states analysis and dynamic simulation as a complement in the HAZOP study of chemical reactors. Process Saf. Environ. Prot. 83(B5) (2005) 463-471.

[37] Swann C. D., Preston M. L., Twenty-five years of HAZOPs. J. Loss Prev. Process Ind. 8(6) (1995) 349–53.

[38] Velardi, S.A.; Barresi A.A., 2008. Development of simplified models for the freeze-drying process and investigation of the optimal operating conditions. Chemical Engineering Research and Design, 86: 9-22.

[39] Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016, Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry, Safety Science 89 77–93.

[40] Yang, X., Haugen, S., 2015, Classification of risk to support decision-making in hazardous processes, Safety Science 80 115–126.

[41] Wang F., Gao J., A novel knowledge database construction method for operation guidance expert system based on HAZOP analysis and accident analysis. J Loss Prev Process Ind 25 (2012) 905-915.

[42] Zio, E., 2014, Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions, Nuclear Engineering and Design 280, 413–419.

[43] Crowl D. A., Louvar J. F., Chemical Process Safety Fundamentals with Applications. (2th ed.). New Jersey, 2002. Prentice Hall International Series in the Physical and Chemical Engineering Sciences.

[44] Mannan, S., Lee’s Lost Prevention in the Process Industries – Hazard Identification, Assessment and Control, Vol. 1, 3rd ed., Oxford: Elsevier Butterworth–Heinemann;, 2005.

[45] Tyler B. J., HAZOP study training from the 1970s to today. Process Saf. Environ. Prot. 90 (2012) 419-423.

[46] Babykina, G; Brînzei, N., Aubry, JF.; Deleuze, G., 2016, Modeling and simulation of a controlled steam generator in the context of dynamic reliability using a

Stochastic Hybrid Automaton, Reliability Engineering and System Safety 152, 115–136

CHAPTER VI - CONCLUSION

The purpose of this work was the introduction of new procedures for hazard assessment based on simulation, considering the whole framework of risk, which goes from the identification of the loss to be analyzed, passing through hazard identification and frequency and severity estimation, until the obtainment of the risk estimation that is used as source of information for decision making. Given that any future estimation is a prediction that may or may not occur, and that all decisions must be taken in order to allow better futures, the concept of risk is the best available tool for decision makers that seek to maintain any future occurrence in an accurate level of expectation. In this sense, the presented work had the main goal to improve the quality of the risk information, which has a huge importance for profit, safety and environmental protection of any industry.

Firstly it is important do highlight some contributions presented in CHAPTER IV, where it was introduced a new risk definition and representation. Some of the contribution were: (i) The five variable risk characterization, which clearly defines all variables that must be identified/estimated during any risk analysis: the loss to be analyzed (L), the identified event(s) (E), the frequency of the event occurrence (F), the severity of the event (S), and the uncertainties (U); (ii) the separation between frequency and uncertainty in risk definition, which defines frequency as a known variability of events occurrence and uncertainty as the difference between the strength of the knowledge (SoK) and the total information needed to correctly predict the risk; and (iii) the difference between the risk variable loss (L), the word "consequence" and the risk variable severity (S). In this latter contribution, the term Loss (L) was used to identify the kind of loss to be analyzed during a risk analysis, what can be any event consequence with human value, just as financial loss, loss of life, environmental damage, etc. Defined the risk variable loss (L) and identified the events (E) it is possible to estimate their severity (S), which are the magnitude of loss of each event. In this sense, given that several cause-consequence relationships may be made in the frame of the analyzed problem, it was decide not use the word "consequence" in the proposed risk definition to not lead to misunderstand of the risk understanding.

Furthermore, also in CHAPTER IV, it was introduced the risk surface representation, which is obtained when variability on both frequency and severity estimation is considered. In the end, given the contribution of this chapter, it was enabled a better understanding about black swan events and making a link between the risk concept applied in industries, developed and discussed in the present thesis, and the quantitative forecasting risk models that are widely applied in different risk analysis fields, principally in economics. Given these contributions, it was highlighted the importance of each risk variable, being possible to understand that any hazard analysis improvement is important to reduce the level of uncertainty of the risk estimation. Such conclusion highlights the importance of the contributions presented in CHAPTER II, CHAPTER III and CHAPTER IV.

In CHAPTER II, it was presented contributions to improve the event identification (risk variable E) of process industries, based on process simulations. The use of process simulation reduces the uncertainties of heuristic process interpretation, enabling also the quantitative understanding of the process non-linearities and dynamics. The simulation of device failure, which causes deviations in dependent process variables, has enabled abnormal process behavior investigations that are in accordance with the ones that may occur in the real process operation. This investigation characteristic and the use of process simulation contribute to identify different process deviations that may occur simultaneously during a process operation and then would need a simultaneous treatment. Furthermore, given that it is not possible to simulate the further hazard that may arise after a group of process deviation occurrence, the heuristic hazard analysis is responsible to identify such further hazard and to predict actions to mitigate their risks, concluding the proposed hazard analysis identification. In the framework of a quantitative risk analysis, such identified hazards feed both further frequency and severity estimations that are needed to estimate the process risk of some analyzed losses. Thus, it was introduced a manner to investigate hazardous process conditions that organize undesirables consequences in systematic way for further quantitative frequency and severity estimations.

Continuing with the risk analysis improvements, in CHAPTER III, procedures for better estimate the frequency (F) risk variable were presented. The available existing methods for this estimation varies from a basic probability theory and Boolean algebra, applied respectively in Event Tree and Fault Tree methods, until state spaces transitions problems that are dependent of process variables value and may be solved by the Champman-Kolmogorov equation. It is true that it is not possible to choose one as the best method to solve all kind of frequency estimation problem, but it was understood that the methods that do not consider the non-linearities and dynamics of the real world lead to more uncertainties (U) for risk estimation. In this sense, the contribution of this chapter is a sequence of procedures to be used for computing the frequencies of events that are based on any possible process understanding. For that, it was enabled to build a state space model to represent the dynamic behavior of the process based on the variability of the process variables values, using either or simultaneously both discrete and continuous random variable at the event connections. For these achievements it was needed to use Monte Carlo simulations for a probabilistic problem resolution; and the development of the deepness concept, which enables the process model simplification by joining a set of states in a unique event, and a model building that is in accordance with the available information and desired results. Then, it was presented procedures that give the required freedom to model any aimed system, enabling the frequency estimation of any possible event.

Finally, in CHAPTER V, the three complementary risk analyses methods were integrated in order to reduce uncertainties during a quantitative risk assessment. The procedure was applied on the freeze-drying, a batch process where its variables values normally vary over the normal operation, demanding a dynamic process risk investigation. Appling the proposed hazard identification method, the obtained results showed that all analyzed devices malfunctions leaded to four consequences, three with harmful impact and one with optimized process condition. These results highlighted that the proposed hazard analysis identification organizes the further consequences of the devices malfunctions and dependent process deviations in a way that facilitate the obtainment of the state space of the process for further quantitative risk estimation. Given the device failure probabilistic information, the frequency of all harmful events were estimated and, specifying the severity of the connections, it was possible to build the desired risk surface of the process financial loss solving a unique state space problem. The three-dimensional risk representation enables to estimate the probability of losing a specific amount of loss in a specified length of time, being also possible to visualize when the process starts to be unsafe according to a pre-defined risk acceptance criterion. In this sense, the proposed procedure combines the three latter proposed risk analysis procedures for a quantitative risk assessment with reduced uncertainties given their direct relation.

In this sense, the presented thesis introduced: (i) new risk definition, (ii) new process hazard identification analysis, (iii) new procedures to quantify frequency of events, (iv) new risk visualizations, and (v) integrated procedure for quantitative risk assessment. Given the wide risk perspective and despite all the presented contribution, it is highlighted that the study of some topics can still continue in order to improve the use of the proposals and the risk analysis and interpretation, just as:

(i) how the risk variable uncertainty (U) may be more deeply investigated in order to be incorporated in the risk surface or to make improvements during the decision making process;

(ii) how to improve the risk management in order to implement a dynamic risk surface updating based on new acquired system information;

(iii) how the dynamic risk visualization based on the risk surface can be used to manage better decisions that aim to minimize the long term or the time cumulative risk;

(iv) how it is possible to use all or some of the proposals in order to update the risk analysis and visualization for decisions making of different areas of interest;

(v) how it is possible to manage a multicriteria decision making, based on different analyzed loss of the same group of identified events;

(vi) how to integrate both positive and harm event severity analysis, mainly in economics perspective, in order to expand the risk perspective and the risk surface representation;

(vii) how to identify and rank the major contributors of the risk surface shape.

These researches may be continued in order to improve the risk usefulness, which is one of the most important concept for the development of different areas of interest given its importance to the probabilistic understanding of future behaviors.

APPENDIX

APPENDIX I - LIKELIHOOD ESTIMATION

Pressurized vessel model presented in CHAPTER III- *Matlab*

```
clc
clear all

%Contribuições
% 1 - Dinâmica do tamque -> exp(at)
% 2 - Válula 1 aberta -> exp(-bt)
% 3 - Válula 2 aberta -> exp(ct)
%P(t)=P0*exp(xt) (utilizar as contribuições quando for o caso)

plot1=0;
plot2=0;
plot3=0;
Pi=10; %Pa
Pc=20; %Pa
Pun=30; %Pa
a=0.05;%Parametro da pressurização noemal
b=2*a; %Parametro da pressurização de V1 (o sinal de menos está
colocado nas equações)
c=1.2*a;%Parametro da pressurização de V2
ProbF=0.05;%probabilidade de falha da V1
lam=250; %h/falha

nMC = 10000;
Nfv1=0;%Num de falha da V1
Nfv2=0;%Num de falha da V2
Nfv12=0;%Num de falha da V1 e V2
Tfv1(nMC)=0;%Tempo de falha da V1
Tfv2(nMC)=0;%Tempo de falha da V2
Tfv12(nMC)=0;%Tempo de falha da V1 e V2
Temdexp(nMC)=0;%Tempo de explosão
Tfv1min=100000;%Limite inferior do tempo de falha da V1
Tfv1max=0;%Limite superior do tempo de falha da V1
Tfv2min=100000;%Limite inferior do tempo de falha da V2
Tfv2max=0;%Limite superior do tempo de falha da V2
Tfv12min=100000;%Limite inferior do tempo de falha da V1 e V2
Tfv12max=0;%Limite superior do tempo de falha da V1 e V2
Temdexpmin=100000;%Limite inferior do tempo de explosão
Temdexpmax=0;%Limite superior do tempo de explosão

for i=1:nMC

Pl=Pi;%pressão de mudança de operação
P=Pi;%pressão inicial do sistema
t=0;

    Ac=0; %V1 acionada
    d=0; %contador de horas
    Rdv2=rand(1); %numero aleatório da V2
    tv2=icdf('Exponential',Rdv2,lam);%Tempo de falha da V2
    fv2=0;
    Pt=0;

        while P<Pun
        d=d+1;

        if fv2==0
           if d>tv2
               if P<Pc
               Pl=P;
               fv2=1;
               Nfv2=Nfv2+1;
               Tfv2(i)=d;
               end
           end
        end
        if P>Pc
            Pl=P;
            if Ac==0
              Ac=1;
              Rdv1=rand(1);
           end
        end
        if P<Pi
           Pl=P;
           Ac=0;
        end

        T=exp(a);
        P=P*T;
        if Pl>Pc
           if Rdv1 >= ProbF
           V1=exp(-b);
           P=P*V1;
           else
               if Tfv1(i)==0
               Nfv1=Nfv1+1;
               Tfv1(i)=d;
               if Tfv2(i)~=0
                   Tfv12(i)=d;
                   Nfv12=Nfv12+1;
               end
               end
           end
        end
        if fv2==1
           V2=exp(c);
           P=P*V2;
        end

         Pt(d)=P;
    end

%tt=(1:d);
%plot(tt,Pt);

Temdexp(i)=d;

if plot1==0
    if Tfv1(i)~=0
        tt=(1:d);
        plot(tt,Pt,'r');
        title('(a) V1 Failure');
        xlabel('Time (h)');
```

```
            ylabel('Pressure (Pa)');
            plot1=1;
            pause
        end
    end
    if plot2==0
        if Tfv2(i)~=0
            tt=(1:d);
            plot(tt,Pt,'r');
            title('(b) V2 Failure');
            xlabel('Time (h)');
            ylabel('Pressure (Pa)');
             plot2=1;
            pause
        end
    end
    if plot3==0
        if Tfv12(i)~=0
            tt=(1:d);
            plot(tt,Pt,'r');
            title('(c) V1 and V2 Failures');
            xlabel('Time (h)');
            ylabel('Pressure (Pa)');
            plot3=1;
            pause
        end
    end

    if Tfv1(i)~=0
        if Tfv1(i)<Tfv1min
            Tfv1min=Tfv1(i);
        end
    end
    if Tfv1(i)>Tfv1max
        Tfv1max=Tfv1(i);
    end
    if Tfv2(i)~=0
        if Tfv2(i)<Tfv2min
            Tfv2min=Tfv2(i);
        end
    end
    if Tfv2(i)>Tfv2max
        Tfv2max=Tfv2(i);
    end
    if Tfv12(i)~=0
        if Tfv12(i)<Tfv12min
            Tfv12min=Tfv12(i);
        end
    end
    if Tfv12(i)>Tfv12max
        Tfv12max=Tfv12(i);
    end
    if Temdexp(i)~=0
        if Temdexp(i)<Temdexpmin
            Temdexpmin=Temdexp(i);
        end
    end
    if Temdexp(i)>Temdexpmax
        Temdexpmax=Temdexp(i);
    end
end
```

```
np=100; %Numero de pontos para a PDF
dTv1=(Tfv1max-Tfv1min)/np; %acrescimo de tempo para o Tfv1
dTv2=(Tfv2max-Tfv2min)/np; %acrescimo de tempo para o Tfv2
dTv12=(Tfv12max-Tfv12min)/np; %acrescimo de tempo para o Tfv1 e Tfv2
dTemdexp=(Temdexpmax-Temdexpmin)/np; %acrescimo de tempo para a
explosão
CDFnfv1(np)=0;%numero de falhas para construir a CDF da V1
CDFnfv2(np)=0;%numero de falhas para construir a CDF da V2
CDFnfv12(np)=0;%numero de falhas para construir a CDF da V1 e da V2
CDFnTemdexp(np)=0;%numero de falhas para construir a CDF das explosões
CDFtfv1(np)=0;%Tempo de falha para contruir a CDF da V1
CDFtfv2(np)=0;%Tempo de falha para contruir a CDF da V2
CDFtfv12(np)=0;%Tempo de falha para contruir a CDF da V1 e da V2
CDFtTemdexp(np)=0;%Tempo de falha para contruir a CDF da explosão

for x=1:nMC
    for k=1:np
        if Tfv1(x)~=0
            if Tfv1(x)<Tfv1min+dTv1*k
                CDFnfv1(k)=CDFnfv1(k)+1;
                CDFtfv1(k)=Tfv1min+dTv1*(k-1/2);%ponto médio
            end
        end
        if Tfv2(x)~=0
            if Tfv2(x)<Tfv2min+dTv2*k
                CDFnfv2(k)=CDFnfv2(k)+1;
                CDFtfv2(k)=Tfv2min+dTv2*(k-1/2);%ponto médio
            end
        end
        if Tfv12(x)~=0
            if Tfv12(x)<Tfv12min+dTv12*k
                CDFnfv12(k)=CDFnfv12(k)+1;
                CDFtfv12(k)=Tfv12min+dTv12*(k-1/2);%ponto médio
            end
        end
        if Temdexp(x)~=0
            if Temdexp(x)<Temdexpmin+dTemdexp*k
                CDFnTemdexp(k)=CDFnTemdexp(k)+1;
                CDFtTemdexp(k)=Temdexpmin+dTemdexp*(k-1/2);%ponto
médio
            end
        end
    end

end

plot(CDFtfv1,CDFnfv1,'p');
title('(a) CDF V1 Failure');
xlabel('Time (h)');
ylabel('Failures');
pause

plot(CDFtfv2,CDFnfv2,'p');
title('(b) CDF V2 Failure');
xlabel('Time (h)');
ylabel('Failures');
pause

plot(CDFtfv12,CDFnfv12,'p');
```

```
title('(c) CDF V1 and V2 Failures');
xlabel('Time (h)');
ylabel('Failures');
pause

plot(CDFtTemdexp,CDFnTemdexp,'p');
title('(d) CDF Explosion');
xlabel('Time (h)');
ylabel('Failures');
pause
Nfv1
Nfv2
Nfv12
```

APPENDIX II - RISK CONCEPT AND REPRESENTATION I

Pressurized vessel model presented in CHAPTER IV - *Matlab*

```
clc
clear all

%Contribuições
% 1 - Dinâmica do tamque -> exp(at)
% 2 - Válula 1 aberta -> exp(-bt)
% 3 - Válula 2 aberta -> exp(ct)
%P(t)=P0*exp(xt) (utilizar as contribuições quando for o caso)

plot1=0;
plot2=0;
plot3=0;
Pi=10; %Pa
Pc=20; %Pa
Pun=30; %Pa
a=0.05;%Parametro da pressurização noemal
b=2*a; %Parametro da pressurização de V1 (o sinal de menos está
colocado nas equações)
c=1.2*a;%Parametro da pressurização de V2
ProbF=0.05;%probabilidade de falha da V1
lam=250; %h/falha



nMC = 50000;
Nfv1=0;%Num de falha da V1
Nfv2=0;%Num de falha da V2
Nfv12=0;%Num de falha da V1 e V2
Tfv1(nMC)=0;%Tempo de falha da V1
Tfv2(nMC)=0;%Tempo de falha da V2
Tfv12(nMC)=0;%Tempo de falha da V1 e V2
Temdexp(nMC)=0;%Tempo de explosão
Tfv1min=100000;%Limite inferior do tempo de falha da V1
Tfv1max=0;%Limite superior do tempo de falha da V1
Tfv2min=100000;%Limite inferior do tempo de falha da V2
Tfv2max=0;%Limite superior do tempo de falha da V2
Tfv12min=100000;%Limite inferior do tempo de falha da V1 e V2
Tfv12max=0;%Limite superior do tempo de falha da V1 e V2
Temdexpmin=100000;%Limite inferior do tempo de explosão
Temdexpmax=0;%Limite superior do tempo de explosão

sMax=0;
sMin=0;
m=10000;
devp=2000;

for i=1:nMC

Pl=Pi;%pressão de mudança de operação
P=Pi;%pressão inicial do sistema
t=0;
```

```
Ac=0; %V1 acionada
d=0; %contador de horas
Rdv2=rand(1); %numero aleatorio da V2
tv2=icdf('Exponential',Rdv2,lam);%Tempo de falha da V2
fv2=0;
Pt=0;

    while P<Pun
        d=d+1;

        if fv2==0
           if d>tv2
               if P<Pc
               Pl=P;
               fv2=1;
               Nfv2=Nfv2+1;
               Tfv2(i)=d;
               end
           end
        end
        if P>Pc
            Pl=P;
            if Ac==0
              Ac=1;
              Rdv1=rand(1);
           end
        end
        if P<Pi
           Pl=P;
           Ac=0;
        end

        T=exp(a);
        P=P*T;
        if Pl>Pc
           if Rdv1 >= ProbF
           V1=exp(-b);
           P=P*V1;
           else
               if Tfv1(i)==0
               Nfv1=Nfv1+1;
               Tfv1(i)=d;
               if Tfv2(i)~=0
                   Tfv12(i)=d;
                   Nfv12=Nfv12+1;
               end
               end
           end
        end
        if fv2==1
           V2=exp(c);
           P=P*V2;
        end

         Pt(d)=P;
    end

%tt=(1:d);
%plot(tt,Pt);
```

```
Temdexp(i)=d;

TxS(i,1)=d;
s=norminv(rand(),m,devp);
TxS(i,2)=s;

if s>sMax
    sMax=s;
end
if s<sMin
    sMin=s;
end




if plot1==0
    if Tfv1(i)~=0
        tt=(1:d);
        plot(tt,Pt,'r');
        title('(a) V1 Failure');
        xlabel('Time (h)');
        ylabel('Pressure (Pa)');
        plot1=1;
        pause
    end
end
if plot2==0
    if Tfv2(i)~=0
        tt=(1:d);
        plot(tt,Pt,'r');
        title('(b) V2 Failure');
        xlabel('Time (h)');
        ylabel('Pressure (Pa)');
         plot2=1;
        pause
    end
end
if plot3==0
    if Tfv12(i)~=0
        tt=(1:d);
        plot(tt,Pt,'r');
        title('(c) V1 and V2 Failures');
        xlabel('Time (h)');
        ylabel('Pressure (Pa)');
        plot3=1;
        pause
    end
end

if Tfv1(i)~=0
    if Tfv1(i)<Tfv1min
        Tfv1min=Tfv1(i);
    end
end
if Tfv1(i)>Tfv1max
    Tfv1max=Tfv1(i);
end
if Tfv2(i)~=0
    if Tfv2(i)<Tfv2min
```

```
            Tfv2min=Tfv2(i);
        end
    end
    if Tfv2(i)>Tfv2max
        Tfv2max=Tfv2(i);
    end
    if Tfv12(i)~=0
        if Tfv12(i)<Tfv12min
            Tfv12min=Tfv12(i);
        end
    end
    if Tfv12(i)>Tfv12max
        Tfv12max=Tfv12(i);
    end



    if Temdexp(i)~=0
        if Temdexp(i)<Temdexpmin
            Temdexpmin=Temdexp(i);
        end
    end
    if Temdexp(i)>Temdexpmax
        Temdexpmax=Temdexp(i);
    end


end


np=60; %Numero de pontos para a PDF (ou tempo)
dTemdexp=(Temdexpmax-Temdexpmin)/np; %acrescimo de tempo para a
explosão
%dTemdexp=(1000-0)/np; %acrescimo de tempo para a explosão
nps=70; %Numero de pontos para a severidade
ds=(sMax-sMin)/nps;%acrescimo de severidade para a explosão

dTv1=(Tfv1max-Tfv1min)/np; %acrescimo de tempo para o Tfv1
dTv2=(Tfv2max-Tfv2min)/np; %acrescimo de tempo para o Tfv2
dTv12=(Tfv12max-Tfv12min)/np; %acrescimo de tempo para o Tfv1 e Tfv2
CDFnfv1(np)=0;%numero de falhas para construir a CDF da V1
CDFnfv2(np)=0;%numero de falhas para construir a CDF da V2
CDFnfv12(np)=0;%numero de falhas para construir a CDF da V1 e da V2
CDFnTemdexp(np)=0;%numero de falhas para construir a CDF das explosões
CDFtfv1(np)=0;%Tempo de falha para contruir a CDF da V1
CDFtfv2(np)=0;%Tempo de falha para contruir a CDF da V2
CDFtfv12(np)=0;%Tempo de falha para contruir a CDF da V1 e da V2
CDFtTemdexp(np)=0;%Tempo de falha para contruir a CDF da explosão

for i=1:nps
  S(i)=ds/2+(i-1)*ds;
  Z(i,1)=0;
end

for k=1:np
  Tempo(k)=dTemdexp/2+(k-1)*dTemdexp;
  Z(1,k)=0;
end
```

```
for x=1:nMC
    for k=1:np
        if dTemdexp*(k-1)<TxS(x,1)
           if TxS(x,1)<dTemdexp*k
              for i=1:nps
                  if sMin+ds*(i-1)<TxS(x,2)
                      if TxS(x,2)<ds*i
                         Z(i,k)=Z(i,k)+1/nMC;

                       end
                  end
              end
           end
       end



       if Tfv1(x)~=0
            if Tfv1(x)<Tfv1min+dTv1*k
                CDFnfv1(k)=CDFnfv1(k)+1;
                CDFtfv1(k)=Tfv1min+dTv1*(k-1/2);%ponto médio
            end
        end
        if Tfv2(x)~=0
            if Tfv2(x)<Tfv2min+dTv2*k
                CDFnfv2(k)=CDFnfv2(k)+1;
                CDFtfv2(k)=Tfv2min+dTv2*(k-1/2);%ponto médio
            end
        end
        if Tfv12(x)~=0
            if Tfv12(x)<Tfv12min+dTv12*k
                CDFnfv12(k)=CDFnfv12(k)+1;
                CDFtfv12(k)=Tfv12min+dTv12*(k-1/2);%ponto médio
            end
        end
        if Temdexp(x)~=0
            if Temdexpmin+dTemdexp*(k-1)<Temdexp(x)
                if Temdexp(x)<Temdexpmin+dTemdexp*k
                    CDFnTemdexp(k)=CDFnTemdexp(k)+1/nMC;
                    CDFtTemdexp(k)=Temdexpmin+dTemdexp*(k-1/2);%ponto
médio
                end
            end
        end
    end

end


%Calculando a CDF
%_____________________
ZC(1,1)=Z(1,1);
for k=1:np
    for s=1:nps
        if s>1 && k>1
            ZC(s,k)=ZC(s,k-1)+ZC(s-1,k)-ZC(s-1,k-1)+Z(s,k);
        end
        if s==1 && k>1
```

```
            ZC(s,k)=ZC(s,k-1)+Z(s,k);
        end
        if s>1 && k==1
            ZC(s,k)=ZC(s-1,k)+Z(s,k);
        end
    end
end

plot(CDFtfv1,CDFnfv1,'p');
title('(a) CDF V1 Failure');
xlabel('Time (h)');
ylabel('Failures');
pause

plot(CDFtfv2,CDFnfv2,'p');
title('(b) CDF V2 Failure');
xlabel('Time (h)');
ylabel('Failures');
pause

plot(CDFtfv12,CDFnfv12,'p');
title('(c) CDF V1 and V2 Failures');
xlabel('Time (h)');
ylabel('Failures');
pause

plot(CDFtTemdexp,CDFnTemdexp,'p');
title('Critical pressure in the vessel');
xlabel('Time (h)');
ylabel('P(X<x)');
pause
Nfv1
Nfv2
Nfv12

surf(Tempo,S,Z);
title('(b) Risk surface');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(x,y)')
Z
Tempo
S

surf(Tempo,S,ZC);
title('(a) Risk surface');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(X<x,Y<y)')
```

APPENDIX III - RISK CONCEPT AND REPRESENTATION II

Holdup tank model presented in CHAPTER IV - *Matlab*

```
clc


%Para afetar o tempo de simulação
SS=1;%1 para simulação rápida e outro para completa

if SS==2
    Tmax=100; %tempo de simulação do processo
    MC=500;
    np=20; %Numero de pontos para a PDF (ou tempo)
    nps=20; %Numero de pontos para a severidade Tmax=100; %tempo de
simulação do processo
else
    Tmax=10000; %tempo de simulação do processo
    MC=50000;
    np=60; %Numero de pontos para a PDF (ou tempo)
    nps=60; %Numero de pontos para a severidade
end
%________________________________________

PFV=0.01; %Prob de falha da válvula em demanda
LamV=300; %h/falha
PFB1=0.03;%Prob de falha da B1 em demanda
LamB1=600; %h/falha
PFB2=0.03;%Prob de falha da B2 em demanda
LamB2=600; %h/falha
a=10;%Nivel de transbordo
alf2=8;%nivel máximo
alf1=3;%nivel mínimo
b=1;%nivel de secagem do tanque

%GrafTR=0;
%GrafES=0;
%GrafME=0;
GrafTR=1;
GrafES=1;
GrafME=1;

TR=0; %Overflow
ES=0; %Dryout
ME=0; %Stable level
TRt=0;
ESt=0;
MEt=0;
tESmin=1000;
tESmax=0;
tMEmin=1000;
tMEmax=0;
tTRmin=1000;
tTRmax=0;
TRt(MC)=0;
MEt(MC)=0;
ESt(MC)=0;
```

```
TF(3)=0;
TpF2(3)=0;

%____RISK____
LambC4=48; %h/reparo dryout
LambC5=100; %h/reparo stable level
LambC6=240; %h/reparo overfloe
SE2m=2000; %Média de dryout
SE2sd=500; %desvio padrao de dryout
SE3m=1000; %Média de stable level
SE3sd=500; %desvio padrao de stable level
SE4m=5000; %Média de overflow
SE4sd=1000; %desvio padrao de overflow
sMin=0; %Severidade mínima computada
sMax=0; %Severidade máxima computada
TxS(MC,Tmax+2000)=0;
L(Tmax+2000)=0;




for i=1:MC

    Too(i)=0; %time out of operation

    L(1)=5.5;%Nivel inicial
    OV=0;% operação da Valvula
    OB1=1;%Operação da bomba 1
    OB2=1; %Operação da bomba 2
    t=1;%contador de tempo
    F=0;%caso o problema se estabilize sem transbordar ou esvaziar
    VF=0;%Falha da válvula
    B1F=0;%Falha da B1
    B2F=0;%Falha da B2

    %Tempo de falha da válvula
    RV1=rand(1); %numero aleatorio da V para o tempo de operaçaõ
    toV=icdf('Exponential',RV1,LamV);%Tempo de falha da V para o tempo
de operação

    %Tempo de falha da bomba1
    RB1=rand(1); %numero aleatorio da B1 para o tempo de operaçaõ
    toB1=icdf('Exponential',RB1,LamB1);%Tempo de falha da V para o
tempo de operação

    %Tempo de falha da bomba2
    RB2=rand(1); %numero aleatorio da B2 para o tempo de operaçaõ
    toB2=icdf('Exponential',RB2,LamB1);%Tempo de falha da V para o
tempo de operação


    %while b<L(t) && L(t)<a && F==0
    while t<Tmax

        t=t+1;
        L(t)=L(t-1)+2/10*(-OV+OB1+OB2/2);%Acho que o 2/10 é para
contar 0.4 de vazão, que deveria ser 4/10

        %operação da válvula
        if VF==0
            if toV>t  %se a valvula falhar pelo tempo, ela permanesce
na posição de em que falhou
                if L(t)<=alf1 && L(t-1)>alf1
                   rOV=rand(1);
                   if rOV>PFV
                      OV=0;
                   else
                      TF(1)=1;
                      TpF(1)=t;
                   end
                end
               if L(t)>alf2 && L(t-1)<=alf2
                  rOV=rand(1);
                  if rOV>PFV
                     OV=1;
                  end
               else
                   TF(1)=1;
                   TpF(1)=t;
               end
            else
                VF=1;
                TF(1)=2;
                TpF(1)=t;
            end
        end

        %operação da Bomba1
        if B1F==0
            if toB1>t  %se a bomba1 falhar pelo tempo, ela permanesce
na posição de em que falhou
                if L(t)<=alf1 && L(t-1)>alf1
                   rOB1=rand(1);
                   if rOB1>PFB1
                      OB1=1;
                   end
                else
                    TF(2)=1;
                    TpF(2)=t;
                end
                if L(t)>alf2 && L(t-1)<=alf2
                   rOB1=rand(1);
                   if rOB1>PFB1
                      OB1=0;
                   end
                else
                    TF(2)=1;
                    TpF(2)=t;
                end
            else
                B1F=1;
                OB1=0;
                TF(2)=2;
                TpF(2)=t;
            end
        end

        %operação da Bomba2
        if B2F==0
```

```
            if toB2>t  %se a bomba2 falhar pelo tempo, ela permanesce
na posição de em que falhou
                if L(t)<=alf1 && L(t-1)>alf1
                   rOB2=rand(1);
                   if rOB2>PFB2
                      OB2=1;
                   end
                else
                    TF(3)=1;
                    TpF(1)=t;
                end
                if L(t)>alf2 && L(t-1)<=alf2
                   rOB2=rand(1);
                   if rOB2>PFB2
                      OB2=0;
                   end
                else
                    TF(3)=1;
                    TpF(3)=t;
                end
            else
                B2F=1;
                OB2=0;
                TF(3)=2;
                TpF(3)=t;
            end
        end
         %if t==1000
         if L(t)==L(t-1)
            F=1;
            for c=1:20
                X=L(t);
                t=t+1;
                L(t)=X;
            end
        end


    if L(t)>=a
        TR=TR+1;
        TRt(i)=t;

        s=norminv(rand(),SE4m,SE4sd);
        TxS(i,t)=s;
        tro=round(icdf('Exponential',rand(),LambC6));%Tempo reparo do
overflow
        Too(i)=Too(i)+tro;

        if  TxS(i,t)<sMin
            sMin=TxS(i,t);
        end
        if  TxS(i,t)>sMax
            sMax=TxS(i,t);
        end
        t=t+tro;


        if GrafTR==0
            tt=(1:t);
            plot(tt,L,'r');
            title('(c) Overflow');
            xlabel('Time (h)');
            ylabel('Level (m)');
            GrafTR=1;
            toV
            toB1
            toB2
            OV
            OB1
            OB2
            VF
            B1F
            B2F
            TF
            TpF
            pause
        end
        if t<tTRmin
            tTRmin=t;
        end
        if t>tTRmax
            tTRmax=t;
        end

    end
    if L(t)<=b
        ES=ES+1;
        ESt(i)=t;

        s=norminv(rand(),SE2m,SE2sd);
        TxS(i,t)=s;
        trd=round(icdf('Exponential',rand(),LambC4));%Tempo reparo do
dryout
        Too(i)=Too(i)+trd;

        if  TxS(i,t)<sMin
            sMin=TxS(i,t);
        end
        if  TxS(i,t)>sMax
            sMax=TxS(i,t);
        end
        t=t+trd;

        if GrafES==0
            tt=(1:t);
            plot(tt,L,'r');
            title('(a) Dryout');
            xlabel('Time (h)');
            ylabel('Level (m)');
            GrafES=1;
            toV
            toB1
            toB2
            OV
            OB1
            OB2
            VF
            B1F
            B2F
            TF
            TpF
            pause
        end
        if t<tESmin
            tESmin=t;
        end
        if t>tESmax
            tESmax=t;
        end
    end
    if L(t)==L(t-1)
        ME=ME+1;
        MEt(i)=t;

        s=norminv(rand(),SE3m,SE3sd);
        TxS(i,t)=s;
        trsl=round(icdf('Exponential',rand(),LambC5));%Tempo reparo do
stable level

        Too(i)=Too(i)+trsl;

        if  TxS(i,t)<sMin
            sMin=TxS(i,t);
        end
        if  TxS(i,t)>sMax
            sMax=TxS(i,t);
        end
         t=t+trsl;

        if GrafME==0
            tt=(1:t);
            plot(tt,L,'r');
            title('(b) Stable level');
            xlabel('Time (h)');
            ylabel('Level (m)');
            GrafME=1;
            toV
            toB1
            toB2
            OV
            OB1
            OB2
            VF
            B1F
            B2F
            TF
            TpF
            pause
        end
        if t<tMEmin
            tMEmin=t;
        end
        if t>tMEmax
            tMEmax=t;
        end

    end



    end
```

```
end

np=100; %Numero de pontos para a PDF
dTR=(tTRmax-tTRmin)/np; %acrescimo de tempo para o Transbordo
dME=(tMEmax-tMEmin)/np; %acrescimo de tempo para o Stable level
dES=(tESmax-tESmin)/np; %acrescimo de tempo para o Dryout
CDFnTR(np)=0;%numero de falhas para construir a CDF da Transbordo
CDFnME(np)=0;%numero de falhas para construir a CDF da Stable level
CDFnES(np)=0;%numero de falhas para construir a CDF da Dryout
CDFtTR(np)=0;%Tempo de falha para contruir a CDF da Transbordo
CDFtME(np)=0;%Tempo de falha para contruir a CDF da Stable level
CDFtES(np)=0;%Tempo de falha para contruir a CDF da Dryout

%np=50; %Numero de pontos para a PDF (ou tempo)
dTp=Tmax/np; %acrescimo de tempo para a explosão
%nps=50; %Numero de pontos para a severidade
sMin=0; %com os parametros, a perda minima estava dando negativa
ds=(sMax-sMin)/nps;%acrescimo de severidade para a explosão

for i=1:nps
  S(i)=sMin+ds/2+(i-1)*ds;
  Z(i,1)=0;
end

for k=1:np
  Tempo(k)=dTp/2+(k-1)*dTp;
  Z(1,k)=0;
end

for x=1:MC
    for k=1:np
        for y=1:Tmax
            if dTp*(k-1)<y
               if y<dTp*k
                  for i=1:nps
                      if sMin+ds*(i-1)<TxS(x,y)
                          if TxS(x,y)<sMin+ds*i
                             Z(i,k)=Z(i,k)+1/MC;
                           end
                      end
                  end
               end
            end
        end
    end
end


%Calculando a CDF
%_____________________
ZC(1,1)=Z(1,1);
for k=1:np
    for s=1:nps
        if s>1 && k>1
            ZC(s,k)=ZC(s,k-1)+ZC(s-1,k)-ZC(s-1,k-1)+Z(s,k);
        end
        if s==1 && k>1
           ZC(s,k)=ZC(s,k-1)+Z(s,k);
        end
        if s>1 && k==1
           ZC(s,k)=ZC(s-1,k)+Z(s,k);
        end
    end
end


surf(Tempo,S,Z);
title('Risk surface');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(x,y)')

surf(Tempo,S,ZC);
title('Risk surface');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(x,y)')
```

APPENDIX IV - COMPLETE QUANTITATIVE RISK ASSESSMENT CASE STUDY I

Freeze drying process simulation model presented in CHAPTER V- *EMSO*

```
Model Nitrogen

PARAMETERS

        P1 as pressure (Brief = "Feed pressure", DisplayUnit = 'Pa');
        PM as Real (Brief = "Molar mass of N2", final Unit = 'g/mol');
        T1 as temperature (Brief = "Temperatura de entrada");
        Z as Real (Brief = "Fator de complexidade");
        Y as Real (Brief = "fator de expansão Y = 0.67 em chocked flow");
        Pmin as pressure (Brief = "Feed pressure", DisplayUnit = 'Pa');
        Kp as Real (Brief = "Kp fo the FT");
        Td as time_sec (Brief = "Const de tempo da FT");
        Tm as time_sec (Brief = "tempo morto da FT");
        Cv as positive (Brief = "Coeficiente de vazão da válvula");

VARIABLES

        dP as pressure (Brief = "dP on the valve", DisplayUnit = 'Pa');
        Flow as flow_mol (Brief = "Molar flow of N2", DisplayUnit = 'mol/h');
        OutP as pressure (Brief = "Pressure after valve", DisplayUnit = 'Pa');
        W as flow_mass (Brief = "Mass flow", DisplayUnit = 'kg/h');
        Kc as positive (Brief = "Gain Constant");
        tauI as time_sec (Brief = "Integral Time Constant");
        x as fraction (Brief = "abertura da válvula");

EQUATIONS

        OutP = P1 - dP;

#Eq 8-110 Perry
        W*3600*'h/kg'=
94.8*Cv*x*(P1/(100000*'Pa'))*Y*(dP/P1*(PM*'mol/g')/(T1/'K'*Z))^(1/2);

        Flow = W/PM;

#Tipos de ajuste do controlador
#ZN
        #Kc*Kp = 0.9*Td/Tm;
        #tauI/Td = 3.33*Tm/Td;

#CC
        Kc*Kp = 0.9*Td/Tm + 0.082;
        tauI/Td = (3.33*Tm/Td*(1+Tm/Td/11))/(1+2.2*(Tm/Td));

#3C
        #Kc*Kp = 0.9*(Td/Tm)^0.946;
        #tauI/Td = 3.33*(Tm/Td)^0.583;


End


Model Chamber

PARAMETERS

        outer PP                        as Plugin       (Brief = "External Physical
Properties",Type="PP");
        Composition_N_l(3)  as fraction     (Brief = "Leakage mole composition
[water, nitrogen, oxygen]");

#Heat Flux
        Akv as Real (final Unit = 'W/(m^2*K)');
        Bkv as Real (final Unit = 'W/(m^2*K*Pa)');
        Ckv as Real (final Unit = '1/Pa');

#Sublimation flux
        Arp as Real (final Unit = 'm/s');
        Brp as Real (final Unit = '1/s');
        Crp as Real (final Unit = '1/m');

#Others
        rhofrozen as dens_mass (Brief = "density of the frozen product");
        kfrozen as Real (Brief = "thermal conductivity of the frozen product", final Unit
= 'W/(m*K)'); #Confirm if is the alfafrozen
        L as length (Brief= " Total thickness");
        dH as Real (Brief= "sublimation enthalpy", final Unit = 'J/kg');
        epsilon as fraction (Brief= "% of density betwen dried and frozen");
        s_glass as length (Brief= "thickness of the glass");
        l_glass as Real (Brief= "thermal conductivity of the glass", final Unit =
'W/(m*K)');
        Vc as volume (Brief = "Chamber volume");
        R as constant (Brief = "Gas constant", final Unit = 'J/(K*mol)');
        nv as Integer (Brief = "Number of vials");
        dv as length (Brief = "Vial diameter");
        pi as Real (Brief = "Number pi");
        k_duct as Real (Brief = "Duct resistence", final Unit = 'kmol/s/Pa');
        cpc_ref as positive (Brief = "cp of the refrigerant fluid", final Unit = 'cal/g/K');

VARIABLES
        Pcsp as pressure (Brief = "Pressure after duct (at the condenser)", DisplayUnit =
'Pa');
```

```
	Tfluid as temperature (Brief= "heating fluid temperature");
	Tfluid2 as temperature (Brief= "heating fluid temperature");
	Tfluidsp as temperature (Brief= "heating fluid temperature");
	Tfluidf as temperature (Brief = "outlet chamber temperature of the refrigerante fluid");
	Q as Real (Brief= "Heat from heater", final Unit = 'W');
	Wc_ref as flow_mass (Brief = "flow mol of the refrigerant fluid", DisplayUnit = 'kg/h');
	#J as Real (Brief= "Heat from heater", final Unit = 'J');

	kch as Real (Brief = "Resistencia da entrada de ar", final Unit = 'mol/h/Pa');
	Composition_chamber(3)  as fraction		(Brief = "Chamber mole composition");
	Mol_chamber(3)  as mol		(Brief = "Chamber total mol");
	Jq as Real (Brief= "Heat flux", final Unit = 'W/m^2'); #Unit at article = W/(m^2*K)
	Kv1 as Real (Brief= "heat transfer coefficient between the shelf and the product in the container before glass", final Unit = 'W/(m^2*K)');
	Kv as Real (Brief= "heat transfer coefficient between the shelf and the product in the container after glass", final Unit = 'W/(m^2*K)');
	Tb as temperature (Brief= "product temperature at the bottom of the container");
	Jw as Real (Brief= "Sublimation flux", final Unit = 'kg/(s*m^2)');
	Rp as Real (Brief= "dried product resistance to vapor flow", final Unit = 'm/s');
	N_l as flow_mol (Brief = "molar flow rate of leakage", DisplayUnit = 'mol/h');
	Pwi as pressure (Brief= "partial pressure of water vapor at the interface of sublimation");
	Pc as pressure (Brief= "chamber pressure", DisplayUnit = 'Pa');
	Ldried as length (Brief= "thickness of the dried product",  DisplayUnit = 'mm');
	Lfrozen as length (Brief= "thickness of the frozen product",  DisplayUnit = 'mm');
	Lfrozenadm as positive (Brief= "Frozen admentional thickness");
	Ti as temperature (Brief= "product temperature at the sublimation interface");
	rhodried as Real (Brief = "apparent density of the dried product", final Unit = 'kg/m^3');
	Sb as flow_mol (Brief = "Sublimatined water",  DisplayUnit = 'mol/h');
	TWF as flow_mol (Brief = "Total outlet water",  DisplayUnit = 'mol/h');
	TFIC as flow_mol (Brief = "Total inlet flow",  DisplayUnit = 'mol/h');
	ntot as mol (Brief = "Total mol at the chamber",  DisplayUnit = 'mol');
	VM as volume_mol (Brief = "Molar volume in the chamber");
	Tc as temperature (Brief = "Temperature of the chamber");
	Tcsp as temperature (Brief = "Temperature of the chamber");
	Asub as area (Brief="total surface of sublimation");
	av as area (Brief = "Vial area");
	TFOC as flow_mol (Brief = "Total outlet flow",  DisplayUnit = 'mol/h');
	N2 as flow_mol (Brief = "molar flow rate of controled leakage (N2)", DisplayUnit = 'kmol/s');
	#N2 as Real (Brief = "molar flow rate of controled leakage (N2)",  final Unit = 'mol/h');
	Pcon as pressure (Brief = "Pressure after duct (at the condenser)", DisplayUnit = 'Pa');
	yw as fraction (Brief = "Water mol at the chamber");
	yn as fraction (Brief = "N2 mol at the chamber");
	yo as fraction (Brief = "O2 mol at the chamber");
	on_offov as Integer (Brief = "Valv on or off");


SET

	R = 8.314462 *'J/(K*mol)';
	pi = 3.14159265358979323846;

EQUATIONS


"Entrada de ar"
N_l = kch*(1*'bar'-Pc);

#Heat Flux
"Heat_Flux"
	Jq = Kv*(Tfluid - Tb);

"Kv Equation"
#Modelado com vidro
	Kv1 = Akv + (Bkv*Pc)/(1+Ckv*Pc);
	Kv = 1/(1/Kv1 + s_glass/l_glass);

#Modelado sem vidro
	#Kv = Akv + (Bkv*Pc)/(1+Ckv*Pc);
	#Kv1 = 0*'kg/s^3/K';

"Kv Equation"
	Rp = Arp + (Brp*Ldried)/(1+Crp*Ldried);

#Jq and Jw Relationchip
"Heat balance"
	Jq = dH*Jw;

if Lfrozen > 0.0001*L then
	"Mass Balance at the frozen layer"
	diff(Lfrozen) = -1/(rhofrozen - rhodried)*Jw;

		if Pc < Pwi then
			#Sublimation flux
			"Heat_Flux"
			Jw = 1/Rp*(Pwi - Pc);
		else
			"Heat_Flux"
			Jw = 0*'kg/(s*m^2)';
		end
```

```
else
"Mass Balance at the frozen layer"
        diff(Lfrozen) = 0 * 'm/s';

#Sublimation flux
"Heat_Flux"
        Jw = 0*'kg/(s*m^2)';
end

"Thickness"
        L = Lfrozen + Ldried;

"Water pressures at the ice"
        Pwi = exp(-6140.4*'K'/Ti + 28.916)*'Pa';

"Density of dried cake"
        rhodried = rhofrozen*(1-epsilon);

"Admentional lenght"
        Lfrozenadm = Lfrozen/L;

"Sublimed water generated"
        Sb = Jw*Asub/(18*'kg/kmol');

"Total water flowing in the chamber"
        TWF = Sb + N_l*Composition_N_l(1);

"Total of mol flowing in the chamber"
        TFIC = Sb + N_l + N2;

"H2O fraction"
        yw = TWF/TFIC;

"N2 fraction"
        yn = (N_l*Composition_N_l(2)+N2)/TFIC;

"O2 fraction"
        yo = (N_l*Composition_N_l(3))/TFIC;

"Chamber mol composition"
        Composition_chamber = [yw,yn,yo];

"Total mol in the chamber"
        diff(ntot) = TFIC - TFOC;

"Molar volume in the chamber"
        VM = Vc/ntot;


"Mols in the chamber"
```

```
	Mol_chamber = ntot*Composition_chamber;

#Temperatura
"Temperatura in the chamber"
	Tc = (Ti + Tfluid)/2;

#relationship between Ti (and thus, pw,i) and TB
"Relationship equation"
#Com o vidro
	#(Tfluid - Tb)/(1/Kv + s_glass/l_glass) = (Tfluid - Ti) / (1/Kv + Lfrozen/kfrozen
+ s_glass/l_glass);

#Sem o vidro
	Tb = Tfluid - 1/Kv / (1/Kv + Lfrozen/kfrozen) * (Tfluid - Ti);	#Kv*(Tfluid -
Tb) = (Tfluid - Ti) / (1/Kv + Lfrozen/kfrozen);

"Fluxo de calor pra o gelo"
	-Jq*Asub = Wc_ref*cpc_ref*(Tfluidf - Tfluid);

"Fluxo de calor go aquecedor"
	Q = Wc_ref*cpc_ref*(Tfluid - Tfluidf);

	#Q = Wc_ref*cpc_ref*(Tfluid2 - Tfluidf);
	(Tfluid2 - Tfluid)^2=1E-8*'K^2';

"Water pressures at the top"
	Pc = ntot*R*Tc/Vc;

"Outlet flow"
	TFOC = k_duct*(on_offov+0.000000001)* (Pc - Pcon);

"Vial area"
	av = pi*dv*dv/4;

"Vials total area"
	Asub = av*nv;


end

Model Condenser

PARAMETERS

	Vcond as volume (Brief = "Volume of the condenser");
	R as constant (Brief = "Gas constant", final Unit = 'J/(K*mol)');

VARIABLES
```

```
        N_in as flow_mol (Brief = "Molar flow geting in the condenser", DisplayUnit =
'mol/h' );
        N_out as flow_mol (Brief = "Molar flow geting out of the condenser",
DisplayUnit = 'mol/h');
        N_duct as flow_mol (Brief = "Molar flow geting in the condenser", DisplayUnit
= 'mol/h' );
        composition(3) as fraction (Brief = "composition of the gas in");
        Tcond as temperature (Brief = "Temperature of the condenser");
        Tcondsp as temperature (Brief = "Temperature of the condenser");
        Pcond as pressure (Brief = "pressure at the condenser", DisplayUnit = 'Pa');
        Psub as pressure (Brief = "pressure sublimation", DisplayUnit = 'Pa');
        N_ice as flow_mol (Brief = "Molar flow of ice", DisplayUnit = 'mol/h');
        #yw as fraction (Brief = "Total mol at the condenser");

SET

        R = 8.314462 *'J/(K*mol)';

EQUATIONS

        N_in = N_duct;

        Psub = (exp((-6140.4*'K')/Tcond + 28.916))*'Pa';

        if (Vcond/(R*Tcond))*Psub/'Pa'/(60*'s')*'Pa' > composition(1)*N_duct then
                N_ice = 0*'mol/s';
        else
                N_ice = composition(1)*N_duct -
(Vcond/(R*Tcond))*Psub/'Pa'/(60*'s')*'Pa'; #/delta_t;
        end

        #N_ice = composition(1)*N_duct - (Vcond/(R*Tcond))*(exp((-
6140.4*'K')/Tcond + 28.916))/(60*'s')*'Pa'; #/delta_t;

        #yw = (N_duct*composition(1)-N_ice)/N_duct;

        diff(Pcond) = (R*Tcond/Vcond) * (N_duct - N_out - N_ice);


end


Model Pump


PARAMETERS

        x_in(16) as pressure (Brief = "Points of pump suction pressure");
        y_in(16) as flow_vol (Brief = "Points of pump flow");
        R as constant (Brief = "Gas constant", final Unit = 'J/(K*mol)');
```

```
	PM as Real (Brief = "Molar mass of N2", final Unit = 'g/mol');
	Z as Real (Brief = "Fator de complexidade");
	Y as Real (Brief = "fator de expansão Y = 0.67 em chocked flow");
	pout as pressure (Brief = "Outlet pressure");
	d as length (Brief = "diametro equivalente da bomba");
	mi as viscosity (Brief = "viscosidade do ar");
	g as Real (Brief = "aceleração da gravidade", final Unit = 'm/s^2');
	LsD as positive (Brief = "comprimento equivalente da bomba");
	pi as Real (Brief = "pi number");

VARIABLES

	Tent as temperature (Brief = "Temperature at the condenser");
	f as Real (Brief = "fator de atrito");
	Re as Real (Brief = "numero de Reynolds");
	rho as dens_mass (Brief = "Massa especifica do gas na bomba");
	v as velocity (Brief = "velocity of gas on the pump");

	n_valve as flow_mol (Brief = "Pump flow",  DisplayUnit = 'mol/h');
	v_valve as flow_vol (Brief = "Pump flow",  DisplayUnit = 'm^3/h');
	pe_valve as pressure (Brief = "Valve entrance pressure", DisplayUnit = 'Pa');
	dP_valve as pressure (Brief = "Valve dP", DisplayUnit = 'Pa');
	Cv as positive (Brief = "Coeficiente de vazão da válvula");
	W as flow_mass (Brief = "Mass flow", DisplayUnit = 'kg/h');

	p_pump as pressure (Brief = "Pump suction pressure", DisplayUnit = 'Pa');
	n_pump as flow_mol (Brief = "Pump flow",  DisplayUnit = 'mol/h');
	v_pump as flow_vol (Brief = "Pump flow",  DisplayUnit = 'm^3/h');

#Logica
	op_pump as Integer (Brief = "Condição operacional da bomba: 0 - não operante,
1 = operante");
	d_pump as Integer (Brief = "Condição de danos à bomba: 0 - sem danos, 1 - com
danos");

SET

PM = 14*'g/mol';
Z = 1;
Y = 0.67;
pout = 1*'atm';
mi = 0.01820*'cP';
d = 3*'in';
g = 9.80665*'m/s^2';
LsD = 50;
pi = 3.14;

R = 8.314462 *'J/(K*mol)';

x_in(1)=0.000001*'Pa';
x_in(2)=2.00E-01*'Pa';
x_in(3)=3.00E-01*'Pa';
x_in(4)=5.00E-01*'Pa';
x_in(5)=7.00E-01*'Pa';
x_in(6)=8.00E-01*'Pa';
x_in(7)=1.00E+00*'Pa';
x_in(8)=2.00E+00*'Pa';
x_in(9)=3.00E+00*'Pa';
x_in(10)=4.00E+00*'Pa';
x_in(11)=5.00E+00*'Pa';
x_in(12)=1.00E+01*'Pa';
x_in(13)=2.00E+01*'Pa';
x_in(14)=1.00E+02*'Pa';
x_in(15)=1.00E+03*'Pa';
x_in(16)=1.00E+04*'Pa';

#flow rate, m3/h
y_in(1)=1.33*0.0001*'m^3/h';
y_in(2)=1.33*0.1*'m^3/h';
y_in(3)=1.33*0.4*'m^3/h';
y_in(4)=1.33*2.0*'m^3/h';
y_in(5)=1.33*4.8*'m^3/h';
y_in(6)=1.33*5.8*'m^3/h';
y_in(7)=1.33*7.0*'m^3/h';
y_in(8)=1.33*9.5*'m^3/h';
y_in(9)=1.33*11.0*'m^3/h';
y_in(10)=1.33*12.0*'m^3/h';
y_in(11)=1.33*13.0*'m^3/h';
y_in(12)=1.33*14.0*'m^3/h';
y_in(13)=1.33*15.0*'m^3/h';
y_in(14)=1.33*18.0*'m^3/h';
y_in(15)=1.33*19.0*'m^3/h';
y_in(16)=1.33*19.5*'m^3/h';


EQUATIONS

#Sempre laminar
f = 64/Re;
Re = rho*v*d/mi;
v = v_pump/(pi*d^2/4);
rho = n_pump/v_pump*PM;

if op_pump equal 0 then

        if p_pump < pout then

                v_pump = 0.000001*'mm^3/s';
                d_pump = 0;
```

```
    else
        p_pump-pout = (f*LsD*v^2/(2*g))*rho*g;
        d_pump = 0;

    end
else


    if p_pump < x_in(2) then
        v_pump = ((y_in(2) - y_in(2-1)) / (x_in(2) - x_in(2-1))) * (p_pump -
x_in(2-1)) + y_in(2-1);
        d_pump = 1;
    else
        if p_pump < x_in(3) then
            v_pump = ((y_in(3) - y_in(3-1)) / (x_in(3) - x_in(3-1))) *
(p_pump - x_in(3-1)) + y_in(3-1);
            d_pump = 1;
        else
            if p_pump < x_in(4) then
                v_pump = ((y_in(4) - y_in(4-1)) / (x_in(4) - x_in(4-1))) *
(p_pump - x_in(4-1)) + y_in(4-1);
                d_pump = 1;
            else
                if p_pump < x_in(5) then
                    v_pump = ((y_in(5) - y_in(5-1)) / (x_in(5) -
x_in(5-1))) * (p_pump - x_in(5-1)) + y_in(5-1);
                    d_pump = 1;
                else
                    if p_pump < x_in(6) then
                        v_pump = ((y_in(6) - y_in(6-1)) / (x_in(6) -
x_in(6-1))) * (p_pump - x_in(6-1)) + y_in(6-1);
                        d_pump = 1;
                    else
                        if p_pump < x_in(7) then
                            v_pump = ((y_in(7) - y_in(7-1)) /
(x_in(7) - x_in(7-1))) * (p_pump - x_in(7-1)) + y_in(7-1);
                            d_pump = 0;
                        else
                            if p_pump < x_in(8) then
                                v_pump = ((y_in(8) - y_in(8-
1)) / (x_in(8) - x_in(8-1))) * (p_pump - x_in(8-1)) + y_in(8-1);
                                d_pump = 0;
                            else
                                if p_pump < x_in(9) then
                                    v_pump = ((y_in(9) -
y_in(9-1)) / (x_in(9) - x_in(9-1))) * (p_pump - x_in(9-1)) + y_in(9-1);
                                    d_pump = 0;
                                else
                                    if p_pump < x_in(10)
then
```

```
                                        v_pump =
((y_in(10) - y_in(10-1)) / (x_in(10) - x_in(10-1))) * (p_pump - x_in(10-1)) + y_in(10-
1);
                                        d_pump = 0;
                                    else
                                        if p_pump <
x_in(11) then

    v_pump = ((y_in(11) - y_in(11-1)) / (x_in(11) - x_in(11-1))) * (p_pump -
x_in(11-1)) + y_in(11-1);

    d_pump = 0;
                                        else
                                            if
p_pump < x_in(12) then

    v_pump = ((y_in(12) - y_in(12-1)) / (x_in(12) - x_in(12-1))) * (p_pump -
x_in(12-1)) + y_in(12-1);

    d_pump = 0;
                                            else


    if p_pump < x_in(13) then

    v_pump = ((y_in(13) - y_in(13-1)) / (x_in(13) - x_in(13-1))) * (p_pump -
x_in(13-1)) + y_in(13-1);

    d_pump = 0;

    else

    if p_pump < x_in(14) then

        v_pump = ((y_in(14) - y_in(14-1)) / (x_in(14) - x_in(14-1))) * (p_pump -
x_in(14-1)) + y_in(14-1);

        d_pump = 0;

    else

        if p_pump < x_in(15) then

            v_pump = ((y_in(15) - y_in(15-1)) / (x_in(15) - x_in(15-1))) *
(p_pump - x_in(15-1)) + y_in(15-1);

            d_pump = 0;

        else
```

```
            v_pump = ((y_in(16) - y_in(16-1)) / (x_in(16) - x_in(16-1))) *
(p_pump - x_in(16-1)) + y_in(16-1);

            #p_pump-pout = (f*LsD*v^2/(2*g))*rho*g;

            d_pump = 1;

        end

    end

    end
                                            end
                                        end
                                    end
                                end
                            end
                        end
                    end
                end
            end
        end
    end


end


    n_pump = n_valve;

    n_valve = (pe_valve*v_valve)/(R*Tent);

#Eq 8-110 Perry
    W*3600*'h/kg'=
94.8*Cv*(pe_valve/(100000*'Pa'))*Y*(dP_valve/pe_valve*(PM*'mol/g')/(Tent/'K'*Z))
^(1/2);
    W*3600*'h/kg'/(PM*'mol/g') = n_valve/('mol/s');

    pe_valve - dP_valve = p_pump;

    n_pump = (p_pump*v_pump)/(R*Tent);


end


FlowSheet FreezingProcess
```

```
PARAMETERS
        PP      as Plugin(Brief="Physical Properties",Type="PP",
                Components = ["water", "nitrogen", "oxygen"],
                LiquidModel = "PR",
                VapourModel = "PR"
        );

VARIABLES

        ch_PAHH as Real (Brief = "Very High pressure alarm");
        ch_PAH as Real (Brief = "High pressure alarm");
        chH2O_PAL as Real (Brief = "High pressure alarm");
        ch_TAHH as Real (Brief = "Very High temperature alarm at the fluid refrigerant
(Tfluid)");
        ch_TAH as Real (Brief = "High temperature alarm at the fluid refrigerant
(Tfluid)");
        ch_TAL as Real (Brief = "low temperature alarm at the fluid refrigerant
(Tfluid)");
        ch_TALL as Real (Brief = "Very low temperature alarm at the fluid refrigerant
(Tfluid)");
        ch_LTD as Real (Brief = "Long Time Drying");
        chfluid_TAHH as Real (Brief = "Very High temperature alarm at the fluid
refrigerant (Tfluid)");
        chfluid_TAH as Real (Brief = "High temperature alarm at the fluid refrigerant
(Tfluid)");
        chfluid_TAL as Real (Brief = "low temperature alarm at the fluid refrigerant
(Tfluid)");
        chfluid_TALL as Real (Brief = "Very low temperature alarm at the fluid
refrigerant (Tfluid)");
        chfluid_FAL as Real (Brief = "low flow alarm at the fluid refrigerant circuit");
        ch_DProd as Real (Brief = "Damage of the product");
        co_TAHH as Real (Brief = "Very High temperature alarm at the fluid refrigerant
(Tfluid)");
        co_TAH as Real (Brief = "High temperature alarm at the fluid refrigerant
(Tfluid)");
        pp_FAL as Real (Brief = "low flow alarm at the fluid refrigerant circuit");
        pp_DPump as Real (Brief = "low flow alarm at the fluid refrigerant circuit");

DEVICES

        n2        as Nitrogen;
        pidn2 as PIDIncr;
        ch   as Chamber;
        co   as Condenser;
        pp   as Pump;

CONNECTIONS

SPECIFY
```

```
#PIDIncr
	pidn2.intTime		= n2.tauI;
	pidn2.gain			= n2.Kc*(ch.Pcsp - n2.Pmin) / (n2.P1 - n2.Pmin);
	pidn2.SetPoint			= (ch.Pcsp - n2.Pmin) / (n2.P1 - n2.Pmin);

SET

#N2
	n2.PM = 14*'g/mol';
	n2.Z = 1;
	n2.T1 = (273.15+10)*'K';
	n2.Y = 0.67;
	n2.P1 = 1*'bar';
	n2.Pmin = 0.000000001*'Pa';
	n2.Cv = 0.5;

	#n2.Kp  = 83.4445; # Cv
	n2.Kp  = 46.4376590330789;
	n2.Td = 94.23*'s';
	n2.Tm = 19.52*'s';

#PIDIncr
	#Parameters
	pidn2.PID_Select	= "Ideal";
	pidn2.Action		= "Reverse";
	pidn2.Mode			= "Automatic";
	pidn2.Clip			= "Clipped";
	pidn2.alpha		= 1;
	pidn2.beta			= 1;
   pidn2.bias			= 0;
   pidn2.derivTime	= 0 *'s';
	pidn2.gamma		= 1;
	pidn2.tau			= 1*'s';
	pidn2.tauSet		= 1*'s';


#Chamber
	#Kv MatLab
	ch.Akv = 9.63407559782609*'W/(m^2*K)';
	ch.Bkv = 0.10889e6*'W/(m^2*K*bar)';
	ch.Ckv = 0.0015e6*'1/bar';
	ch.s_glass = 0.0012*'m';
	ch.l_glass = 1.25*'W/(K*m)';
	#Rp MatLab
	ch.Arp = 10000*'m/s';
	ch.Brp = 188000000*'1/s';
	ch.Crp = 820*'1/m';
	#N_l Composition (Ar com 0.2% de umidade)
	ch.Composition_N_l = [0.002, 0.780, 0.218];
	#Density
	ch.rhofrozen = 920*'kg/m^3';
	ch.epsilon = 0.95;
	#Others
	ch.kfrozen = 2.56*'W/(m*K)';
	ch.L = 0.0076 * 'm';
	ch.dH = 2687400 * 'J/kg';
	ch.Vc = 0.201*'m^3';
	ch.dv = 21*'mm';
	ch.nv = 162;
	ch.k_duct = 1e-5*'kmol/s/Pa';
	ch.cpc_ref = 5*'cal/g/K';

#Condenser
	co.Vcond = 0.1 *'m^3';


EQUATIONS

#Conections
	n2.OutP = ch.Pc;
	n2.Flow = ch.N2;
	ch.Pcon = co.Pcond;
	ch.TFOC = co.N_in;
	ch.Composition_chamber = co.composition;
	co.Pcond = pp.pe_valve;
	co.Tcond = pp.Tent;
	co.N_out = pp.n_valve;

#Controlador
	pidn2.Input = (ch.Pc - n2.Pmin) / (n2.P1 - n2.Pmin);


##SETs do Processo##

#Controle de N2
	#pidn2.Output = n2.x; #Controle (não funciona)
	#ch.Pc = ch.Pcsp; #Sem controle porém mexe no N2 mantendo a pressão da
camera igual a SP
	n2.x = 0.0613082; #Ponto operacional (Pc = 5 atm)
	#n2.x = 0; #Falha fecha

#Chamber
	#Ponto original
	ch.Tfluidsp = (273.15 - 20)*'K';
	#ch.Tfluid = ch.Tfluidsp; #colocar fator multiplicativo para realizar desvios
	ch.Tfluid = (273.15 - 20)*'K'; #colocar fator multiplicativo para realizar desvios
	##ch.Q = 20.5*'W';
	ch.Pcsp = 5*'Pa';
	#Melhor ponto: maior Tfluid e menor Pcsp, não passando o limite de -30C em
Ti.
```

```
        #ch.Tfluidsp = (270.15)*'K';
        #ch.Tfluid = (270.15)*'K';
        #ch.Pcsp = 6*'Pa'; # Achar n2.x que dê essa pressão.
        #n2.x = 0.082; #Abertura para a melhor condição de operação
        ch.Tcsp = 245.5*'K';
        ch.Wc_ref = 1*'kg/h';
        ch.on_offov = 1;#válvula na saída da camara
        ch.kch = 1.7692e-8 *'mol/h/Pa'; #Door open


#Condenser
#Normal = 213K
        co.Tcond = (213)*'K';
        #co.Tcond = (213+20)*'K';
        #n2.x = 0; #Ajuste da pressão em função da alta pressão no condensador.
        co.Tcondsp = 213*'K';

#Pump
        pp.Cv = 0.08656; #Válvula na sucção da bomba
        #pp.Cv = 10; #Falha abre
        #pp.Cv = 0.0000000001;#Falha fecha
        pp.op_pump = 1; #Operação da bomba


##Alarms and Interloks##


#Chamber

if ch.Pc > ch.Pcsp+4*'Pa' then
        ch_PAHH = 1;
else
        ch_PAHH = 0;
end

if ch.Pc > ch.Pcsp+2*'Pa' then
        ch_PAH = 1;
else
        ch_PAH = 0;
end

if ch.Composition_chamber(1) < 0.05 then
        chH2O_PAL = 1;
else
        chH2O_PAL = 0;
end

if ch.Tc > ch.Tcsp*1.2 then
ch_TAHH = 1;
else
```

```
ch_TAHH = 0;
end

if ch.Tc > ch.Tcsp*1.1 then
ch_TAH = 1;
else
ch_TAH = 0;
end

if ch.Tc < ch.Tcsp*0.9 then
ch_TAL = 1;
else
ch_TAL = 0;
end

if ch.Tc < ch.Tcsp*0.8 then
ch_TALL = 1;
else
ch_TALL = 0;
end

if ch.Tfluid > ch.Tfluidsp + 10*'K' then
chfluid_TAHH = 1;
else
chfluid_TAHH = 0;
end

if ch.Tfluid > ch.Tfluidsp + 5*'K' then
chfluid_TAH = 1;
else
chfluid_TAH = 0;
end

if ch.Tfluid < ch.Tfluidsp - 5*'K' then
chfluid_TAL = 1;
else
chfluid_TAL = 0;
end

if ch.Tfluid < ch.Tfluidsp - 10*'K' then
chfluid_TALL = 1;
else
chfluid_TALL = 0;
end

if ch.Wc_ref < 1*'kg/h' then
chfluid_FAL = 1;
else
chfluid_FAL = 0;
end
```

```
if ch.Ti > (273.15-32)*'K' then #2 graus de folga - limite -30graus
        if ch.Lfrozenadm > 0.0001 then
                ch_DProd = 1;
        else
                ch_DProd = 0;
        end
else
        ch_DProd = 0;
end


#Condenser
if co.Tcond > co.Tcondsp + 18*'K' then
co_TAHH = 1;
else
co_TAHH = 0;
end

if co.Tcond > co.Tcondsp + 10*'K' then
co_TAH = 1;
else
co_TAH = 0;
end

#Pump
if pp.v_pump < 6*'m^3/h' then
pp_FAL = 1;
else
pp_FAL = 0;
end

if pp.d_pump equal 1 then
pp_DPump = 1;
else
pp_DPump = 0;
end

if time > 75900*'s' then
        if time < 76050*'s' then
                if ch.Lfrozenadm > 0.0001 then
                        ch_LTD = 1;
                else
                        ch_LTD = 0;
                end
        else
                ch_LTD = 0;
        end
else
        ch_LTD = 0;
```

```
end

INITIAL
	ch.Lfrozen = ch.L*(1-0.0001);
	ch.Pc = 5*'Pa';
	ch.Composition_chamber = [0.002, 0.780, 0.218];
	co.Pcond = 4.9*'Pa';
	pp.op_pump = 1; #Operação da bomba
	#co.yw = 0;

GUESS

	ch.Tfluid = (273.15-20)*'K';
	ch.Ti = 230*'K';
	ch.Jq = 234*'W/m^2';
	pp.pe_valve = 5*'Pa';

OPTIONS
	TimeStep = 1;
	TimeEnd = 30*60;
	TimeUnit = 'min';
	DAESolver(File = "dassl");
#	GuessFile = 
"C:\Users\NOTEBOOK\Raoni\PEQ\Doutorado\Projetos\Italia\Estudos\Freeze
Drying\FreezingProcess_suc.rlt";
#	InitialFile = 
"C:\Users\NOTEBOOK\Raoni\PEQ\Doutorado\Projetos\Italia\Estudos\Freeze
Drying\FreezingProcess_suc_est.rlt";

end
```

APPENDIX V - COMPLETE QUANTITATIVE RISK ASSESSMENT CASE STUDY II

Freeze drying frequency and risk surface estimation presented in CHAPTER V- *Matlab*

```
clc
clear all


%lambda (L) e probabilidade discreta (D) das Conexões (1-15)

% C1: LT - vantagem não estudada
LC(1)=0;%anos/falha
DC(1)=0;
mRC(1)=0;
dpRC(1)=0;
mS(1)=0;
dpS(1)=0;



% C2: Dam - Abertura da V_N2
LC(2)=1/0.02; %anos/falha
DC(2)=0.002;
mRC(2)=72;
dpRC(2)=0.1*72;
mS(2)=5000;
dpS(2)=1000;

% C3: HT - Fechamento da V_N2
LC(3)=1/0.02;%anos/falha
DC(3)=0.009;
mRC(3)=72;
dpRC(3)=0.1*72;
mS(3)=5000;
dpS(3)=1000;

% C4: LoS - Não acionamento do aquecedor
LC(4)=1/0.0002;%anos/falha
DC(4)=0.02;
mRC(4)=24;
dpRC(4)=0.1*24;
mS(4)=5000;
dpS(4)=3000;

%C5: HT - dT=-10.1K no aquecedor
LC(5)=1/0.001; %anos/falha
DC(5)=0;
mRC(5)=12;
dpRC(5)=0.1*12;
mS(5)=3000;
dpS(5)=1000;

%C6: LT - Vantagem não estudada
LC(6)=0; %anos/falha
DC(6)=0;
```

```
mRC(6)=0;
dpRC(6)=0;
mS(6)=0;
dpS(6)=0;


%C7: Dam - dT=12K no aquecedor
LC(7)=1/0.0001; %anos/falha
DC(7)=0;
mRC(7)=12;
dpRC(7)=0.1*12;
mS(7)=3000;
dpS(7)=1000;

%C8: LoS - Shut-off da P-01 do aquecedor
LC(8)=1/0.0002; %anos/falha
DC(8)=0.04;
mRC(8)=24;
dpRC(8)=0.1*24;
mS(8)=5000;
dpS(8)=3000;

%C9: HT - Abertura da V06 (condensador)
LC(9)=1/0.02; %anos/falha
DC(9)=0.003;
mRC(9)=12;
dpRC(9)=0.1*12;
mS(9)=2000;
dpS(9)=1000;

%C10: Dam - Fechamento da V06 (condensador)
LC(10)=1/0.02; %anos/falha
DC(10)=0.003;
mRC(10)=12;
dpRC(10)=0.1*12;
mS(10)=2000;
dpS(10)=1000;

%C11: LT - Vantagem não estudada
LC(11)=0; %anos/falha
DC(11)=0;
mRC(11)=0;
dpRC(11)=0;
mS(11)=10;
dpS(11)=0;

%C12: LT - Vantagem não estudada
LC(12)=0; %anos/falha
DC(12)=0;
mRC(12)=0;
dpRC(12)=0;
mS(12)=10;
dpS(12)=0;


%C13: Dam - dT=20K do condensador
LC(13)=1/0.001; %anos/falha
DC(13)=0;
mRC(13)=24;
dpRC(13)=0.1*24;
```

```
mS(13)=5000;
dpS(13)=2000;

%C14: Dam - Fechamento da V-01 (Bomba)
LC(14)=1/0.01; %anos/falha
DC(14)=0.003;
mRC(14)=12;
dpRC(14)=0.1*12;
mS(14)=2000;
dpS(14)=1000;

%C15: Dam - Falha na VP-01 (Vacuo)
LC(15)=1/0.001; %anos/falha
DC(15)=0.04;
mRC(15)=24;
dpRC(15)=0.1*24;
mS(15)=7000;
dpS(15)=4000;


MC=10000;
%MC=100;
tIni=0;
%tIni=24*30*12*2;
tMax=24*30+tIni;  %horas
tMax=24*30*12*2+tIni;
TxS(MC,tMax+50)=0;
sMin=0;
sMax=0;
PD=300000; % $Perda de batelada
%PD=0;
Bat=0;
TxS_LoS(MC,tMax+50)=0;
TxS_Dam(MC,tMax+50)=0;
TxS_HT(MC,tMax+50)=0;

for i=1:MC

    t=tIni+1;

    while t<tMax
        Bat=Bat+1;
        c=0;

        for k=1:15
           %Ver se os equipamentos falharam em dado tempo
           %if rand()<DC(k)
||rand()<icdf('Exponential',t/(24*365),LC(k)) %lamb [=] ano/falhas ->
t em ano
           if rand()<DC(k)
||rand()<cdf('Exponential',t/(24*365),LC(k)) %lamb [=] ano/falhas -> t
em ano
               F(k)=1;
           else
               F(k)=0;
           end
        end

        %Caminho do process: Prioridades LoS - Dam - HT
        if F(5)==1
```

```
   c=5;%ss
end
if F(3)==1
   c=3;
end
if F(9)==1
   c=9;
end
if F(7)==1
   c=7;%SS
end
if F(13)==1
   c=13;%SS
end
if F(14)==1
   c=14;
end
if F(10)==1
   c=10;
end
if F(2)==1
   c=2;
end
if F(15)==1
   c=15;
end
if F(8)==1
   c=8;
end
if F(4)==1
   c=4;
end

% Nenhuma falha
if c==0
   t=t+24;
end


% C1: LT - vantagem não estudada

% C2: Dam - Abertura da V_N2
if c==2

   a=norminv(rand(),mS(2),dpS(2));
   if a>0
        TxS_Dam(i,t-tIni)=a+PD;
        TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
    else
        TxS_Dam(i,t-tIni)=PD;
        TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
   end


    if  TxS(i,t-tIni)<sMin
        sMin=TxS(i,t-tIni);
    end
    if  TxS(i,t-tIni)>sMax
        sMax=TxS(i,t-tIni);
    end
```

```
            t=t+round(norminv(rand(),mRC(2),dpRC(2))); %Tempo para
voltar à operação normal

        end

        % C3: HT - Fechamento da V_N2
        if c==3

            a=norminv(rand(),mS(3),dpS(3));
           if a>0
                TxS_HT(i,t-tIni)=a;
                TxS(i,t-tIni)=TxS_HT(i,t-tIni);
            else
                TxS_HT(i,t-tIni)=0;
                TxS(i,t-tIni)=TxS_HT(i,t-tIni);
           end

            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(3),dpRC(3))); %Tempo para
voltar à operação normal

        end

        % C4: LoS - Não acionamento do aquecedor
        if c==4

            a=norminv(rand(),mS(4),dpS(4));
           if a>0
                TxS_LoS(i,t-tIni)=a;
               TxS(i,t-tIni)=TxS_LoS(i,t-tIni);
            else
                TxS_LoS(i,t-tIni)=0;
                TxS(i,t-tIni)=TxS_LoS(i,t-tIni);
           end

            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(4),dpRC(4))); %Tempo para
voltar à operação normal

        end

        %C5: HT - dT=-10.1K no aquecedor
        if c==5

            a=norminv(rand(),mS(5),dpS(5));
           if a>0
```

```
               TxS_HT(i,t-tIni)=a;
                TxS(i,t-tIni)=TxS_HT(i,t-tIni);
            else
                TxS_HT(i,t-tIni)=0;
                TxS(i,t-tIni)=TxS_HT(i,t-tIni);
           end

            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(5),dpRC(5))); %Tempo para
voltar à operação normal

        end

        %C6: LT - Vantagem não estudada

        %C7: Dam - dT=12K no aquecedor
        if c==7

            a=norminv(rand(),mS(7),dpS(7));

            if a>0
                TxS_Dam(i,t-tIni)=a+PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
            else
                TxS_Dam(i,t-tIni)=PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           end

            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(7),dpRC(7))); %Tempo para
voltar à operação normal

        end

        %C8: LoS - Shut-off da P-01 do aquecedor
        if c==8

          a=norminv(rand(),mS(8),dpS(8));
           if a>0
                TxS_LoS(i,t-tIni)=a;
                TxS(i,t-tIni)=TxS_LoS(i,t-tIni);
            else
                TxS_LoS(i,t-tIni)=0;
               TxS(i,t-tIni)=TxS_LoS(i,t-tIni);
           end

           if  TxS(i,t-tIni)<sMin
```

```
               sMin=TxS(i,t-tIni);
           end
           if  TxS(i,t-tIni)>sMax
               sMax=TxS(i,t-tIni);
           end

            t=t+round(norminv(rand(),mRC(8),dpRC(8))); %Tempo para
voltar à operação normal
        end

        %C9: HT - Abertura da V06 (condensador)
        if c==9

           a=norminv(rand(),mS(9),dpS(9));
           if a>0
                TxS_HT(i,t-tIni)=a;
               TxS(i,t-tIni)=TxS_HT(i,t-tIni);
            else
                TxS_HT(i,t-tIni)=0;
               TxS(i,t-tIni)=TxS_HT(i,t-tIni);
           end

            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(9),dpRC(9))); %Tempo para
voltar à operação normal

        end

        %C10: Dam - Fechamento da V06 (condensador)
        if c==10

            a=norminv(rand(),mS(10),dpS(10));
           if a>0
                TxS_Dam(i,t-tIni)=a+PD;
               TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           else
                TxS_Dam(i,t-tIni)=PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           end

            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(10),dpRC(10))); %Tempo para
voltar à operação normal

        end

        %C11: LT - Vantagem não estudada
        %C12: LT - Vantagem não estudada

        %C13: Dam - dT=20K do condensador
        if c==13

            a=norminv(rand(),mS(13),dpS(13));
           if a>0
                TxS_Dam(i,t-tIni)=a+PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
            else
                TxS_Dam(i,t-tIni)=PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           end
            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(13),dpRC(13))); %Tempo para
voltar à operação normal

        end

        %C14: Dam - Fechamento da V-01 (Bomba)
        if c==14

            a=norminv(rand(),mS(14),dpS(14));
           if a>0
               TxS_Dam(i,t-tIni)=a+PD;
               TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           else
               TxS_Dam(i,t-tIni)=PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           end
            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(14),dpRC(14))); %Tempo para
voltar à operação normal

        end

        %C15: Dam - Falha na VP-01 (Vacuo)
        if c==15

           a=norminv(rand(),mS(15),dpS(15));
           if a>0
                TxS_Dam(i,t-tIni)=a+PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           else
                TxS_Dam(i,t-tIni)=PD;
                TxS(i,t-tIni)=TxS_Dam(i,t-tIni);
           end
```

```
            if  TxS(i,t-tIni)<sMin
                sMin=TxS(i,t-tIni);
            end
            if  TxS(i,t-tIni)>sMax
                sMax=TxS(i,t-tIni);
            end

            t=t+round(norminv(rand(),mRC(15),dpRC(15))); %Tempo para
voltar à operação normal

        end

    end

end




%Construção das curvas
%_____________________

npt=30; %Numero de pontos de tempo para a PDF e superficie
dTp=(tMax-tIni)/npt; %acrescimo de tempo para as curvas
CDFnLoS(npt)=0;%numero de falhas para construir a CDF da LoS
PDFnLoS(npt)=0;%numero de falhas para construir a PDF da LoS
CDFtLoS(npt)=0;%Tempo de falha para contruir a CDF da LoS
CDFnDam(npt)=0;%numero de falhas para construir a CDF da LoS
PDFnDam(npt)=0;%numero de falhas para construir a PDF da LoS
CDFtDam(npt)=0;%Tempo de falha para contruir a CDF da LoS
CDFnHT(npt)=0;%numero de falhas para construir a CDF da LoS
PDFnHT(npt)=0;%numero de falhas para construir a PDF da LoS
CDFtHT(npt)=0;%Tempo de falha para contruir a CDF da LoS

nps=30; %Numero de pontos de severidade para a superficie
sMin=0;
sMax=20000;
ds=(sMax-sMin)/nps; %acrescimo de tempo para as curvas

nps2=30; %Numero de pontos de severidade para a superficie
sMin2=PD-10000;
sMax2=PD+30000;
ds2=(sMax2-sMin2)/nps2; %acrescimo de tempo para as curvas

for i=1:nps2
   CDFs2(i)=sMin2+ds2*(i-1/2);%ponto médio
   Z2(i,1)=0;
end
for i=1:nps
   CDFs(i)=sMin+ds*(i-1/2);%ponto médio
   Z(i,1)=0;
end
for k=1:npt
  CDFt(k)=tIni+dTp*(k-1/2);%ponto médio
  Z(1,k)=0;
  Z2(1,k)=0;
end

for i=1:MC
```

```
    for k=1:npt
        for y=1:tMax-tIni
          if TxS(i,y)~=0
            if dTp*(k-1)<y
              if y<=dTp*k
                 if TxS_LoS(i,y)~=0
                    PDFnLoS(k)=PDFnLoS(k)+1; %calcular a PDF
                  end
                  if TxS_Dam(i,y)~=0
                    PDFnDam(k)=PDFnDam(k)+1; %calcular a PDF
                  end
                  if TxS_HT(i,y)~=0
                    PDFnHT(k)=PDFnHT(k)+1; %calcular a PDF
                  end
                  for s=1:nps
                     if sMin+ds*(s-1)<TxS(i,y)
                        if TxS(i,y)<sMin+ds*s
                           Z(s,k)=Z(s,k)+1/Bat;
                        end
                     end
                  end
                  for s=1:nps2
                      if sMin2+ds2*(s-1)<TxS(i,y)
                        if TxS(i,y)<sMin2+ds2*s
                           Z2(s,k)=Z2(s,k)+1/Bat;
                        end
                      end
                  end
               end
            end
          end
       end

    end
end



%Calculando a CDF
%_____________________
ZC(1,1)=Z(1,1);
ZC2(1,1)=Z2(1,1);

for k=1:npt
    for s=1:nps
        if s==1
            if k==1
               CDFnLoS(k)=PDFnLoS(k); %Lack of start
               CDFnDam(k)=PDFnDam(k); %Damage
               CDFnHT(k)=PDFnHT(k); %Higher time
            else
               CDFnLoS(k)=CDFnLoS(k-1)+PDFnLoS(k);%Lack of start
               CDFnDam(k)=CDFnDam(k-1)+PDFnDam(k);%Damage
               CDFnHT(k)=CDFnHT(k-1)+PDFnHT(k);%Higher time
            end
        end

        if s>1 && k>1
            ZC(s,k)=ZC(s,k-1)+ZC(s-1,k)-ZC(s-1,k-1)+Z(s,k);
            ZC2(s,k)=ZC2(s,k-1)+ZC2(s-1,k)-ZC2(s-1,k-1)+Z2(s,k);
        end
        if s==1 && k>1
           ZC(s,k)=ZC(s,k-1)+Z(s,k);
           ZC2(s,k)=ZC2(s,k-1)+Z2(s,k);
        end
        if s>1 && k==1
           ZC(s,k)=ZC(s-1,k)+Z(s,k);
           ZC2(s,k)=ZC2(s-1,k)+Z2(s,k);
        end
    end
end



%Plotando as curvas
%_____________________

CDFnLoSnorm=CDFnLoS/CDFnLoS(npt);%normalizado
PLoS=CDFnLoS(npt)/Bat
CDFnDamnorm=CDFnDam/CDFnDam(npt);%normalizado
PDam=CDFnDam(npt)/Bat
CDFnHTnorm=CDFnHT/CDFnHT(npt);%normalizado
PHT=CDFnHT(npt)/Bat
Bat


plot(CDFt,CDFnLoSnorm,'p');
title('(a) Lack of start');
xlabel('Time (h)');
ylabel('P(X<x)');
pause

plot(CDFt,CDFnDamnorm,'p');
title('(b) Damage to the product');
xlabel('Time (h)');
ylabel('P(X<x)');
pause

plot(CDFt,CDFnHTnorm,'p');
title('(c) Higher time');
xlabel('Time (h)');
ylabel('P(X<x)');
pause

surf(CDFt,CDFs,Z);
title('Probabilistic density risk surface');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(x,y)')
pause

surf(CDFt,CDFs,ZC);
title('Cumulative Risk surface');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(X<x,Y<y)')
pause

surf(CDFt,CDFs2,Z2);
```

```
title('Probabilistic density risk surface - Loss');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(x,y)')
pause

surf(CDFt,CDFs2,ZC2);
title('Cumulative Risk surface - Loss');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('P(X<x,Y<y)')
pause

surf(CDFt,CDFs2,ZC2*Bat/MC);
title('Cumulative Risk surface - Loss');
xlabel('Time(h)')
ylabel('Severity($)')
zlabel('F(X<x,Y<y)')
pause
```