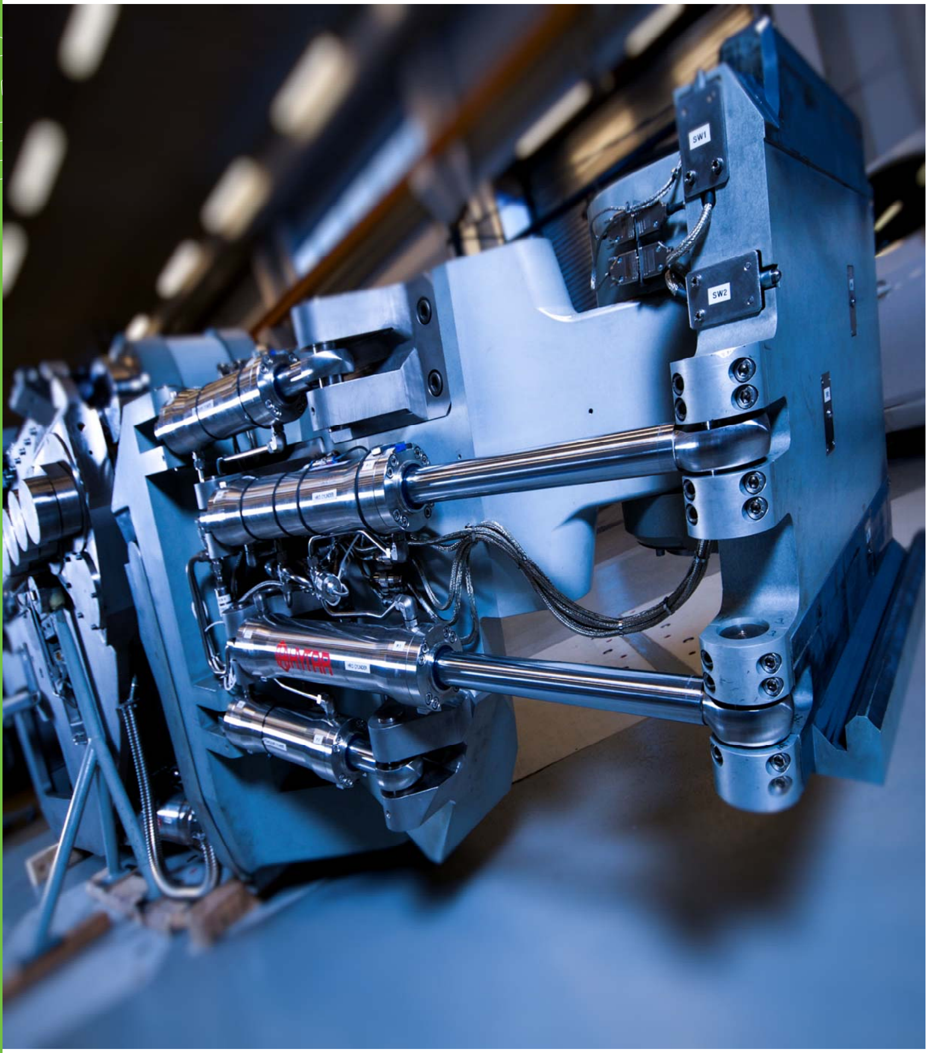


VISIONS • SCIENCE • TECHNOLOGY • RESEARCH HIGHLIGHTS

Dissertation

140

Quantitative evaluation method for the verification of complex mechatronic systems

Development of a reliability-based design process using stochastic Petri Nets

Romain Sibois

VTT SCIENCE 140

Quantitative evaluation method for the verification of complex mechatronic systems

Development of a reliability-based design process using stochastic Petri Nets

Romain Sibois

Thesis for the degree of Doctor of Science in Technology to be presented with due permission for public examination and criticism in Sähkötalo Building, Auditorium SA203, Tampere University of Technology, on the 9th of December 2016, at 12 noon.

ISBN 978-951-38-8473-4 (Soft back ed.)
ISBN 978-951-38-8472-7 (URL: http://www.vttresearch.com/impact/publications)

VTT Science 140

ISSN-L 2242-119X
ISSN 2242-119X (Print)
ISSN 2242-1203 (Online)
http://urn.fi/URN:ISBN:978-951-38-8472-7

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Cover image: CMM in ROViR laboratory - VTT

Juvenes Print, Tampere 2016

ABSTRACT

The verification of complex engineering systems from the very early phases of the design process is of primary importance, as it directly influences performance and system functionalities. Traditional design approaches aim at using simulations as a set of tools during the verification process. However, the current trend in the industry is towards simulation-based design processes in an iterative manner so as to constantly evaluate the system development. This perspective conveys the design process towards a verification-based design process. In the very early phases of the design process, evaluating different concepts for further development is not without problems, since a certain amount of product information is missing in the early phases. Therefore, traditional approaches have aimed at considering expert's opinions as the main evaluation criteria for assessing pre-concepts and concept designs. However, qualitative-based methods are highly limited according to expert's subjective judgements, level of expertise, as well as the ability to take into account multidisciplinary criteria in the case of complex systems.

This dissertation presents research work related to the verification-driven design process of complex mechatronic systems using a stochastic reliability method for evaluating the concept design from the early phases of the product development. The main objective of this thesis consists in demonstrating the advantages of an innovative system design process based on a quantitative evaluation method using reliability as the main criteria. This thesis reviews the state of the art of the verification and validation process, describes different trends in the system design processes towards simulation-based design processes and reviews the best practices of decision-making processes in the engineering field. The work conducted during this thesis consists of the development, modelling and implementation of a verification-based design approach. The method uses the stochastic Petri Net approach for modelling the operational and functional sequence of the system as well as its dysfunctional behaviour. Reliability parameters of each concept are estimated based on their level of design and thus various concepts can be evaluated against each other.

The method is applied to case studies that consist of the development of a Remote Handling system for the maintenance of a fusion reactor called DEMO. The results confirm the benefit of such a method for designing and evaluating concept designs from the very early phases of the system development. The purpose of this research is to maintain the usefulness of the findings for other developments at a larger scale and in other fields than fusion engineering.

ACKNOWLEDGMENT

I discovered the fusion world back in 2008 when I was still a master student in Troyes University of Technology in the department of Mechanical Engineering. I got the chance to perform a 6 months' internship in the Institute for Magnetic Fusion Research at the French Alternative Energies and Atomic Energy Commission (CEA). At the end of my studies, I got the opportunity to perform a second internship in VTT Technical Research Centre of Finland, located in Tampere. During these periods, I became fascinated in fusion power and all the engineering involved in such a challenging project. Fusion is the nuclear reaction that powers the Sun and the stars and it could become a potential source of safe, non-carbon emitting and virtually limitless energy. I am delighted to be part of this thrilling adventure.

The official research process started in October 2010 when I officially joined VTT as a research scientist and enrolled in the international research programme called EFDA's European Goal Oriented Training Programme on Remote Handling. The 3 years' programme aimed to train engineers for activities supporting the ITER project and the long-term fusion programme in European Associations, Fusion for Energy, industries and the ITER organization. Later, while remaining faithful to VTT, I enrolled in the Doctoral programme in Engineering Sciences of Tampere University of Technology in January 2015, to pursue my doctoral studies. Nevertheless, today is the day to think back and thank everyone who has supported me in this adventure.

First and for most, I would like to express my gratitude and my most sincere appreciation to my thesis supervisor Prof. Kalevi Huhtala for his unfailing guidance throughout my doctoral studies and for the preparation of this thesis. Besides I would like to address an endless gratitude to my thesis instructors Prof. Timo Määttä and Dr. Ali Muhammad from VTT, for believing in my research capabilities, for sharing their research philosophy and for their unlimited support even in up-and-down situations throughout this long journey full of interesting events.

I am grateful to my pre-examiners Prof. Aki Mikkola and Prof. Petri Kuosmanen for their fruitful feedbacks on my research work, methodology and interpretation of the results. I also would like to express my thankfulness to the opponent Dr. Hans Meister for his time and expertise.

I have been honoured to have Principal Scientist Mikko Siuko as my team leader for many years, for introducing me in the ROViR team and for sharing his

extensive knowledge on remote handling during my research work as well as for giving me the freedom to combine my research activities with my daily work. Likewise, I had the privilege to share my office together with Harri Mäkinen for few years. His extensive knowledge and strong expertise as well as our daily discussions made this journey even more memorable. Furthermore, a special thanks for his infinite support even in overwhelmed periods that allowed me to carry on the writing of my dissertation. I have also been fortunate to work with Karoliina Salminen, her precious support, her sympathy, her helpful advices and her own experience of the PREFIT program have been very meaningful to me. A special thanks goes to Jorma Järvenpää, our young retiree, for his wisdom, valuable support and his guidance in all circumstances.

I am deeply thankful to the entire ROViR team, VTT scientists and managers, for their continuous support: Riikka Virkkunen, Risto Kuivanen, Mikael Haag, Juha Kortelainen, Hannu Saarinen, Jarmo Alanen, Vesä Hämäläinen, Janne Lyytinen, Jari Schabel, Petri Tikka, William Brace, Jarno Videnoja, Joonas Linnosmaa and Jukka-Pekka Uusitalo.

I would like to thanks Professor Jouni Mattila, for his relevant supervision during the EFDA GOT-RH Programme as well as all the participants to this programme… I am also thankful to DEMO WPRM project members and managers, Antony Loving, Oliver Crofts, Daniel Iglesias and many more for the work performed in parallel of my thesis work and for the skilful project supervision.

A great sense of gratitude goes to Dr. Carolina Hernandez by whom this outstanding adventure in the fusion field has started back in 2008. I am blessed to have been given the opportunity to join her very interesting and challenging projects. Together with Jean Pierre Martins, they gave me the opportunity to steer my young career internationally and especially towards VTT in Finland, therefore, I am very thankful to them for that.

A special thumb up goes to my friends here in Tampere: Mia, Cliff, Waqar, Marc-Antoine, Anna & Arnaud, Anna M., Elli, Adrien, Andrea, Kusni and many more that made this Finnish adventure a true success. A particular attention goes to Dr. Li Li, a true friend that gave me essential advices for the dissertation work. And finally a special Aloha goes to my windsurf buddies: Laurent & Alizée, Christophe, Antoine, Maéva, Nicolas, and many more for travelling the world together with a unique goal: “chasing wind & waves”.

Finally, I would like to express my warmest thanks to my parents Marie-Odile and Francis Sibois, to my brother Guillaume Sibois, for their endless support and for understanding my choice of living abroad and thus far from them.

Tampere, October 24, 2016

sibois

Romain Sibois

ACADEMIC DISSERTATION

Supervisor	**Professor Kalevi Huhtala** Department Intelligent Hydraulic and Automation Tampere University of Technology Finland
Thesis instructors	**Professor Timo Määttä** Production and machine systems VTT Technical Research Centre of Finland Ltd Finland
	Doctor Ali Muhammad Production and machine systems VTT Technical Research Centre of Finland Ltd Finland
Pre-examiner	**Professor Petri Kuosmanen** Department of Mechanical Engineering Aalto University Finland
Pre-examiner and Opponent	**Professor Aki Mikkola** Department of Mechanical Engineering Lappeenranta University of Technology Finland
Opponent	**Doctor Hans Meister** Group leader ITER Diagnostics Max Planck Institute for Plasma Physics Germany

TABLE OF CONTENTS

NOMENCLATURE

A	Area
ψ^u	Design requirement of the product performance
δ	Dirac transition delay
δ	Displacement produced by a force
λ	Exponential rate parameter
F	Force
N_0	Initial number of a fault in the Jelinski-Moranda model
Φ	Intensity parameter of an exponential process
m	Lognormal average parameter
e	Lognormal error parameter
μ	Lognormal location parameter
σ	Lognormal scale parameter
υ	Poisson's ratio
P	Power
p	Pressure
$P[-]$	Probability of an event
ψ	Product performance measure
P	Steady force applied to a body
k	Stiffness
ε	Strain
T	Temperature
X	Vector of a random variable
η	Weibull mean time to failure
β	Weibull shape parameter
E	Young's Modulus

ACRONYMS

AIAA	American Institute of Aeronautics and Astronautics
AHP	Analytic Hierarchical Process
ALARA	As Low As Reasonably Achievable
APECS	Advanced Process Engineering Co-Simulator
AR	Augmented Reality
ASME	American Society of Mechatronic Engineers
CAD	Computer Aided Design
CAE	Computer Aided Engineering
CAM	Computer Aided Manufacturing
CAPP	Computer Aided Process Planning
CAx	Computer Aided technology
CC	Customer Constraint
CE	Concurrent Engineering
CEA	French Alternative Energies and Atomic Energy Commission
CFD	Computational Fluid Dynamic
CMM	Cassette Multifunction Mover
CN	Customer Need
CODAC	Control, Data Access and Communication
CSM	Computational Solid Dynamics
CTM	Cassette Toroidal Mover
CVDS	Continuous Variable Dynamic System
D	Probability of Detection
DA	Dysfunctional Analysis
DC	Direct Current

DEMO	Demonstration fusion power plant
DEDS	Discrete Event Dynamic System
DES	Discrete Event Simulation
DMU	Digital Mock-Up
DOF	Degrees Of Freedom
DRHS	Divertor Remote Handling System
DSM	Design Structure Matrix
DSPNs	Determinist Stochastic Petri Nets
DTP2	Divertor Test Platform
EFDA	European Fusion Development Agreement
ERP	Enterprise Resource Planning
EUR	European currency
FA	Functional Analysis
FAHP	Fuzzy Analytic Hierarchical Process
FEA/FEM	Finite Element Analysis / Finite Element Method
FFMEA	Functional Failure Mode and Effect Analysis
FIS	Fuzzy Interference System
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effect and Criticality Analysis
FTA	Fault Tree Analysis
GOT-RH	Goal Oriented Training Programme on Remote Handling
GRIF	GRaphical Interface for reliability Forecasting
HAZOP	Hazard and Operability Analysis
IC	Input Constraint
IEEE	Institute of Electrical and Electronics Engineering
IHA	Department of Intelligent Hydraulics and Automation of TUT
IMMP	ITER Maintenance Management Plan
INCOSE	International Council on Systems Engineering
IRFM	Institute for Magnetic Fusion Research
IRHCOP	ITER Remote Handling Code Of Practise
IRMMS	ITER Remote Maintenance Management System
ITER	International Thermonuclear Experimental Reactor
ITER-FEAT	ITER Fusion Energy Amplification Tokamak

JET	Joint European Torus at Culham, UK
JTA	Joint Tolerance Analysis
KIT	Karlsruhe Institute of Technology
KM	Knowledge Management
LCA	Life Cycle Assessment
MBS	Multibody Simulation
MES	Manufacturing Execution Systems
MIL-HDBK	Military Handbook
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
M&S	Modelling and Simulation
MW	Mega-Watt
NASA	National Aeronautics and Space Administration
NPRD	Nonelectric Parts Reliability Data
NSWC	Naval Surface Warfare Center
O	Occurrence
OPM	Object-Process Methodology
PCP	Primary Closure Plate
PDM	Product Data Management
PFC	Plasma Facing Component
PLM	Product Lifecycle Management
PMU	Physical Mock-Up
PN	Petri Network
QFD	Quality Function Deployment
RAMI	Reliability, Availability, Maintainability and Inspectability
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagram
RDR	Radial Drive
RH	Remote Handling
RMS	Remote Maintenance Strategy
ROViR	Remote Operation and Virtual Reality Centre
RP	Rapid Prototyping
RPN	Risk Priority Number

S	Severity
SCADA	Supervisory Control and Data Acquisition
SCEE	Standard Cassette End-Effector
SDM	Simulation Data Management
SE	Systems Engineering
SLM	Simulation Lifecycle Management
SysML	System Modelling Language
TBC	To Be Confirmed
TUT	Tampere University of Technology
UML	Unified Modelling Language
USD	United States Dollar
US DoD	United States Department of Defence
US DoE	United States Department of Energy
VE	Virtual Environment
VM	Virtual Model
VP	Virtual Prototyping
VR	Virtual Reality
VT	Virtual Testing
VTT	VTT Technical Research Centre of Finland Ltd, Teknologian tutkimuskeskus VTT Oy
V&V	Verification and Validation
VV	Vacuum Vessel
VV&A	Verification, Validation & Accreditation
WHMAN	Water Hydraulic Manipulator

1 INTRODUCTION

The notion of '*virtuality*' probably first appeared in Aristotelean thought [1], in which entities can be conceptualized as both actualities and potentiality: '*Entities are actual in their existence in the world, but every mode of existence is an actualization of a potentiality*'. Etymologically speaking, *Virtuality* comes from the Latin *vir* which indicates a man or manliness, but is also at the origin of the word *virtus*, which means strength; indeed, from such was derived the notion of *virility* [2]. *Virtuality* is also related to *virtue*, which indicates, according to the Oxford Dictionary, '*a behaviour showing a high moral standard*' but as well '*a good quality of a thing*'. Humans rely on their sense of perceiving information and consider *real*, an entity evolving in a known environment. Thus the notion of *virtuality* can be seen as the representation of an entity that cannot be detected by common human senses. If we turn around the notion of *virtuality* and consider that *real* is the opposite of *virtual*, thus the resulting question would be: *what makes an entity real?* To suggest a part of the answer, an entity is considered virtual until the potentiality that makes it virtual becomes an actuality in fact by an accumulation of evidence, often with the help of technology. Therefore, it leads to the notion of *evidence*. By definition evidence means '*a fact or information that indicates if a belief is true or valid*' [2]. Evidence is a way to remove the 'potentiality' side of an entity to become an actuality.

In the modern engineering field, the notion of *virtual* could be seen in a similar way than above. *Virtual prototyping* consists of representing a system that does not exist yet but thanks to technology, can be digitally represented and thus gives information to our senses, such that a prototype is digitally real. Technology basically uses a language to translate a potential entity into a digital entity which, computed by our perceiving systems, basically our brain, emerges of being in and out of our 'known' world. In other terms, a *digital prototype* is the translation of a virtual prototype using a digital language that is processed to build a representation. In that way, a digital prototype offers a solution for representing a virtual entity. The digital prototype finds its utility in the fact of transforming the potentiality of this entity into an actuality through the accumulation of evidence. As previously defined, the evidence shall consist of facts or information that indicates if a belief appears to be true or valid. With advancements in computation power and digital tools, more and more physical aspects can be accurately translated into a digital prototype and thus provides new or more representative evidence to determine if the system can actually be valid.

This leads us to the notion of *Verification and Validation* (*V&V*) in relation to the engineering field. Basically the verification and validation process aims at bringing evidence so as to give real information to our sense that the system is valid and can actually become a reality. By performing experiments using digital prototypes we can infer the evidence that will lead to removing the potentiality of, at least, some parts of the system.

From the systems engineering point of view, the Verification and Validation (V&V) process is based on requirements that it is another language that is used to represent an entity, basically considered to be a potential product. This V&V process aims to obtain evidence to validate the developed system against the initial requirements, in other words to validate the developed system against the first idea that we had about that product. In today's engineering field, the V&V process can be seen as a bridge between the virtual and real system in terms of product design (**Fig. 1**).

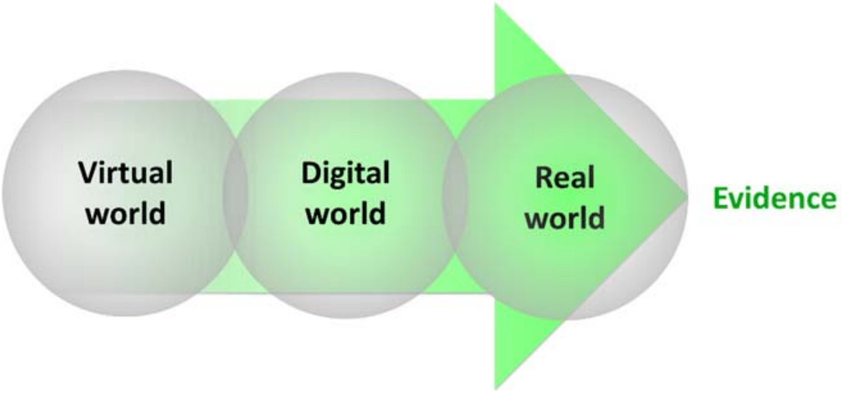


Fig. 1 – To carry evidence from virtual to real world

It is possible to perform experiments on physical prototypes, which is the conventional way to proceed in order to obtain evidence that will validate the system. However, it has some limitations especially regarding manufacturing and testing costs. Multiple iterations of physical prototypes can be very expensive, in the case of consequent and complex systems, which may become industrially impossible to realize. In addition, digital prototyping offers another advantage over physical prototyping by enabling the possibility to estimate a wide set of variables of a system. For instance, it would be really difficult or even impossible to locate good enough pressure sensors in the chamber of a hydraulic motor in order to measure the dynamic pressure. A similar difficulty applies to measuring the pressure-flow dynamic inside a servo valve. Therefore, digital models offer an exclusive and reliable solution in some specific cases.

In order to perform experiments in the digital world, a digital prototype is modelled and used as a digital support. Experiments have to be translated to access the virtual world and thus be able to interact with the virtual entity. Digital experiments, so called simulations, are used to provide information on the potential behaviour of the developed system to determine if the digital prototype can actually be made real. This new digital environment that combines the digital translation of a potential system together with the digital translation of physical experiments aims to bridge the gap between virtuality and reality. In the engineering field, this bridge or mid-platform is called a *digital mock-up*.

1.1 Background to the research

Nowadays, industries are required to provide new products with innovative and powerful features at a much faster pace. The integration of functionalities from various disciplines is a source of innovation. Increasing complexity of products results in more challenges during the development of these products. In the industry, products need to be designed, verified and validated against their requirements before being mass-produced and operated.

Digital tools are considered essential during the design process and their use is becoming progressively more common. In other words, developing complex systems and decreasing at the same time the number of physical prototypes by increasing the use of digital tools leads to increased complexity in the design processes. It is particularly true within the mechatronic industry, where the current trend is towards simulation-based system development, where simulations become a central part of the design process. However, validation in the digital world is a key objective for the industry and currently drives the research trend [3].

But many challenges remain to be overcome. The most obvious challenge is that the digital world is not the real world, and thus involves many uncertainties that have to be taken into account when designing and simulating the developed system. The increased complexity in system designs exponentially increases the complexity of the design process and thus the demands on verification and validation [4]. New methods and new digital tools need to be developed in order to deal with complex simulations. Also, new quantitative methods for evaluating simulation results are needed. A crucial aspect of the design process is the decision-making process that actually leads the design evolution of the system. Thus it requires relevant information and a clear evaluation of uncertainties in order to be able to take the right decision to develop the system further.

1.2 Motivation

The motivation behind this research work is to investigate the best practices of using verification and validation processes within industries [3, 5-7] as well as in the fusion engineering field, especially in the development of remote handling systems, from system requirements to the manufacturing phase of the physical prototype. In the industry, virtual prototyping has been adopted as a standard for several decades and companies are nowadays looking at more complex simulation possibilities, such as more interoperability between the modelling and simulation methods to allow fast and complete virtual verification [8] and to maintain their competitive edge especially in automotive or aerospace industries. There is clear evidence that the current trend is moving towards virtual validation [9-11] of the developed system upon product manufacture. This will lead to a closing of the gap between the digital and real worlds and will obviously result in a reduction in a product's time-to-market and will thus decrease development costs for complex systems [12, 13]. Such a statement is not only valid for specific industries but is relevant also to complex scientific areas, such as nuclear fusion for the development of Remote Handling (RH) systems.

The goal of this research is, therefore, to enhance the design process based on systems engineering best practices and V&V processes used in product development so as to increase the use of digital mock-ups and virtual tests during the system design and verification phase. In addition, best practices from the industry will be studied and the developed process can be derived in order to be suitable for industrial purposes. As results, a suitable method to design and validate high complexity systems, such as RH devices for fusion activities or other industries, can be formalized – increasing confidence in the product and easing decision-making – by the use of simulations. Finally, a novel criteria-based evaluation method for complex system designs that aims to enhance the decision-making process is presented in this study and assessed in case studies.

1.3 Research question

Design verification and validation in the digital environment has already been widely studied [3, 14, 15]. Digital prototyping helps engineers to virtually simulate products along the different phases of the lifecycle. It enables a better understanding of the physical behaviour of the system prior to manufacturing with less need for multiple iterations of physical prototypes. However, for very complex engineering systems, physical tests on a full-scale prototype remain a requirement. Manufacturing such prototypes is very expensive and current trends are heading towards reducing the need for multiple iterations of physical prototypes [3]. In such cases, virtual experiment outputs are compared to physical experiment outputs, with such comparisons leading to a validation of the computational code of the digital mock-up. On the other hand, the validated digital model can be used to verify the physical performance of the product.

The state of the art of this investigation shows that reducing errors and therefore increasing confidence in the system from the very early phases of the design are of primary importance and it is currently a clear research trend. In this research work, the goal is to formalize within the design process a method based on simulations in order to virtually test and verify the developed system at every phase of the design process, which means independently of its level of design. The iterative aspect of the method is very important to be able to implement it in a design process. The evaluation process will support the decision-making process; therefore, a quantitative criteria-based methodology is a requirement.

In order to evaluate complex systems from the very early phases of the design and to overcome the lack of objectivity for common decision-making processes, a new methodology for system verification and decision-making through the design process is needed. One traditional approach in systems engineering is to consider that '*The design shall be verified*'. However, what if we go one step further and consider that '*Verification shall drive the design*'? This statement represents the governing principle of the present investigation, which will aim to give a part of the answer to the following research question: *How can we evaluate and drive the design of complex systems in an iterative and quantitative manner throughout the entire design process?*

The hypothesis discussed in the present dissertation can thus be expressed as follow:

> *The formalization of an iterative design process that aims to evaluate and verify a system against its requirements by way of simulations could lead to improving confidence in the developed system from the very early phases of the design and therefore decrease the product development time. Combining with a quantitative reliability-based evaluation method could lead also to an enhanced decision-making process for complex system design.*

The suggested governing principle for such a formalized simulation-based design process is based on reliability prediction, which would evolve in an iterative manner and be used as the main quantitative criteria for the decision-making process of each new iteration.

1.4 Objectives of the thesis

The objective of the research is to investigate the best practices in the industry concerning the design process of complex systems as well as the extended use of digital mock-ups and simulations in a multidisciplinary environment. The goal is to study and develop a suitable process for designing and verifying complex systems together to support the decision-making process all across the product development using criteria-based evaluation methods.

The main objectives of the thesis are:

- To study the current scope of digital mock-ups during the design process of complex engineering systems.
- To study the best practices of verification and validation processes in the industry and the current trends in the research area.
- To study the use of decision-making tools from the early phases of the design process to the verification phase.
- To develop a novel verification-based design process to evaluate the design against the requirements and study its contribution to the decision-making process.
- To implement and formalize the criteria-based evaluation method for decision-making in a real case study.
- To perform experimental tests on a relevant case study for hypotheses validation purposes.
- To ensure the developed methods can be applied to other applications and to motivate studies by other researchers.

1.5 Scope of the research

The scope of this research mainly focuses on mechanical and mechatronic systems as well as verification and validation in the digital and physical environment. Lifecycle management systems are also covered by studying industry practices, mainly those oriented towards design processes. The research concerns primarily the development of large scale systems of high complexity, such as fusion-oriented devices. However, the contribution of this thesis can be applied to mechanical systems in a more general way. The study of the state of the art concerns mainly high complexity industry sectors, such as aerospace and automotive industries, but also extensively covers the fusion research field.

Control system designs together with software designs are not covered in this work. The personal background of the author in these areas was quite limited as well as the expected inputs that these fields could provide for this work. However, only a few basic implementation tasks within the experimental work required some knowledge of software engineering.

The experimental part of this thesis that aims to apply the developed method to existing case studies, such as fusion remote handling devices; however, the aim of this study is not oriented to reconsidering the technological solutions of those case studies that have already been verified and validated for the maintenance operations of a fusion reactor.

The theoretical discussions and results in the thesis regarding verification and validation of complex systems using a simulation and reliability-based evaluation method during the product design have been kept general without references to any particular fields. Thus the findings may be useful for future research and development, and discussions can be applied to a wider scale. However, since the motivation for the thesis derives from the fusion engineering sector, a section of the thesis focuses on this particular and fairly unique field. The case study for research validation purpose is also fusion oriented, although the influence of particular aspects of nuclear fusion, such as radiation, magnetic fields or very high temperature, are not taken into account in this study. Thus the experimental device can be considered to be a more general mechatronic system.

Concerning the mechanical failures presented in this thesis, only metallic materials (linear material properties) are considered in this study. Ceramic, plastic or composite materials are not taken into account. Moreover, the environment where the studied system has to operate is considered to be inside a very controlled nuclear area, which means a controlled temperature (from constant to +50 °C) and a clean area with no dust. Environments that are wet or humid, or with dust are not considered in this study.

1.6 Scientific contributions of this research

The main contributions of this research work are:

- Providing a state-of-the-art summary of the best verification and validation practices, design process and decision-making process of complex engineering systems.
- Reviewing the common system-design verification methods used in the industry and the current trends in the research.
- Development of an innovative verification-driven design process using a reliability-based stochastic Petri Net approach for the quantitative evaluation of the design concepts in the very early phase of product development.
- Implementation of the developed process on a real case study for the development of DEMO RH systems.
- Reliability estimation of different DEMO-related RH systems concepts.

1.7 Structure of the thesis

The structure of the thesis is divided into 6 chapters. A brief description of each chapters is described and organised as follow:

Chapter 2 provides an exhaustive state-of-the-art overview of topics relevant to the research. It includes verification and validation processes relevant to the industry as well as in the fusion field, and it also includes an extensive review of system design processes with emphasis on the simulation-based design process.

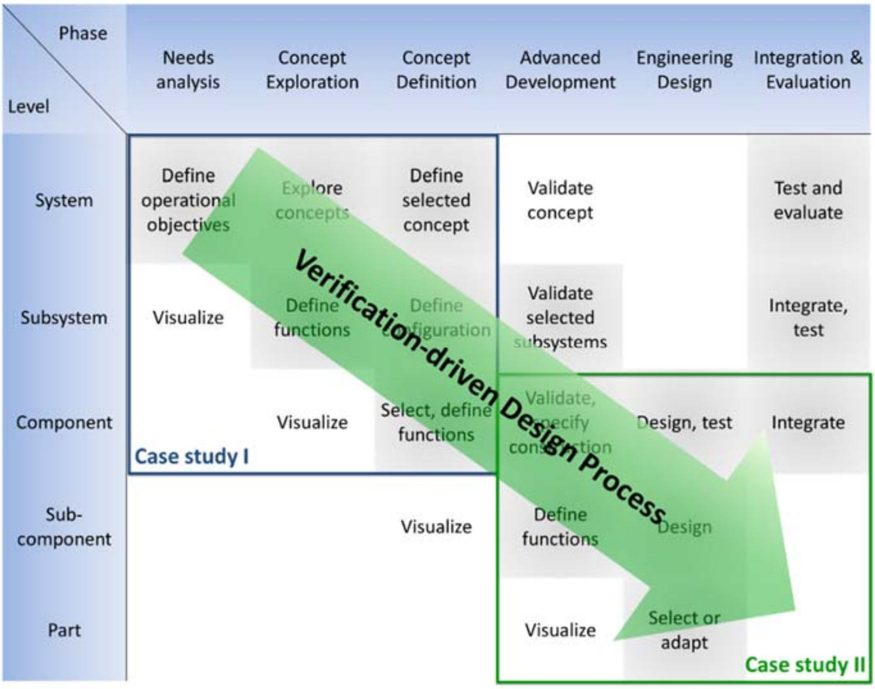
Chapter 3 focuses on the evaluation of the verification methods for the design of complex engineering systems from the very early phase of the design process. Different methods are described in this chapter and how they are connected to each other. Also, the theoretical background is described, as well as the multiple tools relevant to this thesis.

Chapter 4 is dedicated to the modelling of the developed method and its implementation using a simple case study. An evaluation assessment is performed at the end of the chapter in order to illustrate and evaluate the methodology.

Chapter 5 introduces the first relevant case study of this thesis to which the method is applied. DEMO remote handling systems are described and the innovative approach is implemented in the development of such systems. The benefits of such a method are evaluated using different concept evaluations and comparisons in the last section of the chapter.

Chapter 6 introduces the second case study of this thesis to which the developed method has been applied. The ITER Divertor Cassette Mover is described and used as a case study to implement the method. This case study is relevant for showing the benefit of the method on a more advanced phase of the design for system optimization. The concept comparison and results of the method are discussed in the last section of this chapter.

Chapter 7 presents an evaluation of the overall study, while the conclusions of the thesis are also summarized. The chapter additionally discusses topics that may require further study and suggests potential directions for future research.



Phase / Level	Needs analysis	Concept Exploration	Concept Definition	Advanced Development	Engineering Design	Integration & Evaluation
System	Define operational objectives	Explore concepts	Define selected concept	Validate concept		Test and evaluate
Subsystem	Visualize	Define functions	Define configuration	Validate selected subsystems		Integrate, test
Component		Visualize	Select, define functions	Validate, specify construction	Design, test	Integrate
Sub-component			Visualize	Define functions	Design	
Part				Visualize	Select or adapt	

Fig. 2 – Framework of the thesis

Fig. 2 illustrates the novel verification-driven design process within the design of complex systems. It illustrates the location of the two case studies for the validation of this thesis. Case study 1 will mainly focus on the early design phase of complex systems, while case study 2 will concentrate on the later phase of the design and optimization phase.

2 STATE OF THE ART

This chapter focuses on the background and current state of the art, focusing on the systems engineering verification and validation process in both digital and physical environments across the entire product lifecycle. The first section covers briefly the systems engineering approach in order to introduce the next section. In Section 2.2, the best practices of system design process are studied, while Section 2.3 mainly focuses on simulation-based design processes. Section 2.4 covers verification and validation processes and the use of a digital mock-up for verification purposes. The fifth section of this chapter reviews the current practices of using simulation tools during the product design. Production lifecycle environment is discussed in Section 2.6 and challenges related to simulation lifecycle management in Section 2.7. Issues relating to the system design process are discussed in Section 2.8, while finally the last section of this chapter focuses on the use of verification and validation method in ITER and the fusion field.

2.1 Systems engineering approach

Briefly, Systems Engineering (SE) has several formal definitions. The NASA Systems Engineering Handbook [16] describes Systems Engineering as follow:

> *SE is a methodical, disciplined approach for the design, realization, technical management, operations and retirement of a system. SE is the art and science of developing an operable system capable of meeting requirements. SE is a holistic, integrative discipline, wherein the contribution of multidiscipline are evaluated and balanced to produce a coherent whole.*

INCOSE Systems Engineering Handbook [17] define the SE approach as follow:

> *SE is an interdisciplinary, collaborative approach that derives, evolves, and verifies a life-cycle balanced system solution and means to enable the realization of successful systems. Successful systems must satisfy the needs of its customer.*

In practice, the SE process drives the design development in an iterative manner in various engineering industries. It transforms needs and requirements into a set of system products, generates information for decision-makers, and provides input for the next design phase. It brings into consideration many issues beyond the technical design challenge. Issues such as risk and derivation of the functional and physical architecture of the product come to the fore and the design synthesis becomes a supporting technology helping to ensure the decisions support the development of the system architecture of the product.

The Systems Engineering Process is often represented in the shape of a V-model as presented in **Fig. 3**. The first step is to analyse the process inputs, which are basically a set of requirements provided by the customers to represents their needs, in other words, what the system must do and how well it must perform. Functions are then analysed by decomposition in a top-down approach and therefore the decomposition defines the functions of sub-level items. On the other hand, the second part of the V-model consists of a bottom-up approach and represents the integration and verification loop for comparing the solution to the requirements. Various methods are commonly used during the verification loop, which includes analysis, modelling, simulation and testing. Product information is then collected and used as inputs for the decision-making process to decide whether more design iterations are needed for the system to fulfil the initial requirements.

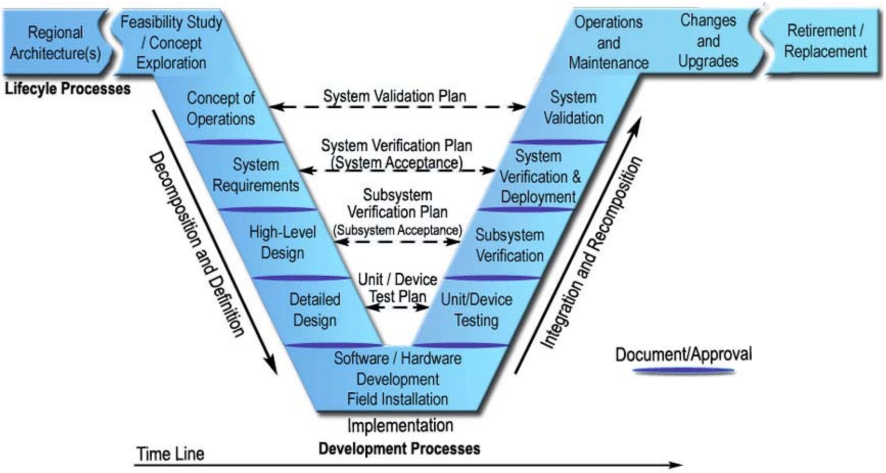


Fig. 3 – V-model of SE approach for the design of complex systems [18]

In many traditional practices, technology is the driver of the design process, however, with SE, the focus moves away from technology to consideration of the customer and what particular function the final product should have. The SE process encompasses non-technical disciplines into the product design such as production, resource, manufacturing and cost.

Unfortunately, many such disciplines do not have analytical models or any kind of model that naturally integrates with traditional engineering disciplines. Moreover, the resulting systems are very complex and it is difficult to develop sufficient understanding of behaviour to cover all eventualities. Different system elements interact in many ways and the eventual performance or behaviour may not always be as predicted. Such emergent behaviour is a real challenge for engineers.

2.2 System design process

In the literature, the design process of complex systems has been identified as one of the key areas for the final validation assessment [19]. Various processes are traditionally used within the industry, and the current trend is moving towards simulation-based system design. The following section aims to review the most common practices and identify the important aspects of each approach, as well as to clarify the evolutionary trends in the systems engineering field.

Thus the current trend in the industry is using simulation-based product lifecycle process; however, current practices show that simulations are mostly used without real interactions [20, 21]. **Fig. 4** presents the evolution of design processes from the present to the future. Currently, traditional industries are using simulation in product development, without real interactions between simulations and analyses.

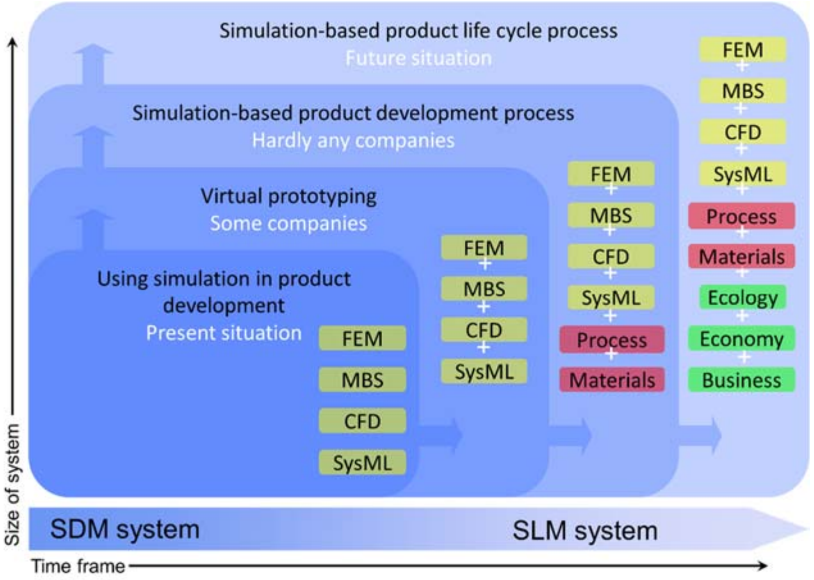

Simulation-based product life cycle process
Future situation
Simulation-based product development process
Hardly any companies
Virtual prototyping
Some companies
Using simulation in product development
Present situation
FEM
MBS
CFD
SysML
FEM + MBS + CFD + SysML
FEM + MBS + CFD + SysML + Process + Materials
FEM + MBS + CFD + SysML + Process + Materials + Ecology + Economy + Business
Size of system
SDM system
SLM system
Time frame

Fig. 4 – Evolution of the application of simulation in the product process and the increasing importance of data management [22]

This process shows the scope of improving design processes throughout the lifecycle by implementing more interactions between simulations tools and between design engineers. Combining more and more tools within the same formalized process can lead to increased confidence among engineers in the developed system. It will also reduce the risk of errors in the early design phase. A significant amount of research has shown that design errors are much more costly when discovered during the later phases of the system development [23-25].

Any development process – no matter whether the output is a product, service, process, organisation, or software – consists of the following steps [26]:

- Understanding the customers' need
- Defining the problem that must be solved to satisfy these needs
- Creating and selecting a solution
- Analysing and optimizing the proposed solution as well as verifying the solution against the customers' needs (design validation)
- Implementing the solution (either a prototype or a final product)
- Checking the resulting product against the customers' needs (implementation validation)

Different practices in the design process are commonly used, starting from product development to simulation-based product life-cycle processes and continuing through intermediate processes, such as virtual prototyping and simulation-based product development processes. In a similar timeframe, data management systems are currently moving from simulation data management systems to simulation lifecycle systems. Section 2.6 gives an overview of simulation management systems.

2.2.1 Product-based design process

In the industry, the most common practice is to use simulations within product development as a set of tools independently of each other, one by one, and one after the other (**Fig. 5**).

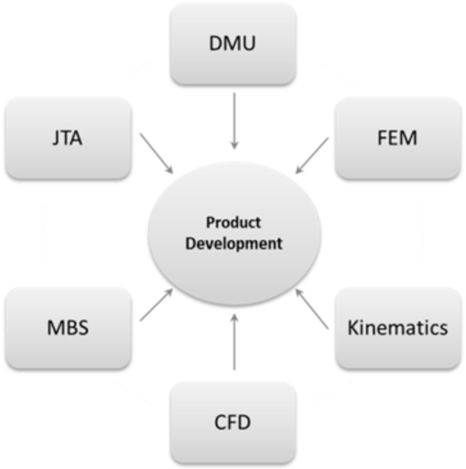


Fig. 5 – Example of product-based design process

In this product-based design process, the design team develops a new product starting from the requirements. During the development process, Digital Mock-Up (DMU) and simulations are used as tools to verify that the system of interest meets the requirements. After using one of the available tools, results need to be reported in order to express the analyst's feedback concerning how the tool has been used and what are the main results. The report is then helpful for the decision making process, to increase the confidence in the product development.

After the selected simulation has been performed, the feedback from the analyst is collected and, if needed, corrective measures related to the design are carried out. Then the next simulation can be performed. Rooks [27] clearly illustrated that using DMU during the development of Boeing airplanes reduced errors and rework by up to 80%. A major drawback with such an approach is that engineers are often using simulation models that are independently updated by the designers. When reaching the validation phase, reports are produced and simulation results have to be individually collected and interpreted often by a third party, who may not have directly collaborated on the simulations. In such cases, loss of information can happen and this can affect the final decision, such as a loss of specific simulation parameters or knowing exactly how the simulation has been performed.

Thus the product-based design process may lead to some limitations due to a potential lack of accuracy in the final decision statement. The more the information is spread around, the more difficult it is to collect them and interpret them in the most relevant way. Moreover, collecting them is often time consuming, this being true especially in the case of projects with long time spans, such as in the aerospace, automobile, nuclear and marine industries. In some cases, validation assessment may be performed some years after the entire verification process has been carried out. Sometimes data from models or simulations outputs may no longer be recoverable due for instance to compatibility issues between outdated software, requiring the simulations to be done again.

In other words, the product-based design process uses simulations as a range of tools, from which you can pick the one needed to perform a particular task. Obviously the more tools you have, the more complete is your tool box. But it does not necessarily mean that you will develop the best system that will fulfil the entire set of requirements and their interactions. As an example, we can quote the well-known story of the loss of the USD 125 million Mars orbiter because the engineering team used English units of measurement while the agency's team used the more conventional metric system for a key spacecraft operation [28]. Therefore, to help the interaction between some aspects of the tools, Product Data Management (PDM) systems may be used in order to collect, store and trace data, such as CAD models and other associated documents during the design process. Thus it becomes an important tool in the event of product development over a longer period or even while sharing within and outside the organization.

2.2.2 Virtual prototype-based design process

In order to reduce the risk of losing information during the entire design process, the current trend is towards a virtual prototype-based design (**Fig. 6**). This process is increasingly used within the industry and a lot of research has been performed on the topic [29, 30]. However, it remains challenging especially in regard to complex product development. Interoperability between software and simulation tools is a major bottleneck. The development of mechatronic systems remains challenging when the developed system involves for instance electrics, electronics, mechanical systems, hydraulic systems and control systems. Currently no software can fully provide the combination of such abilities.

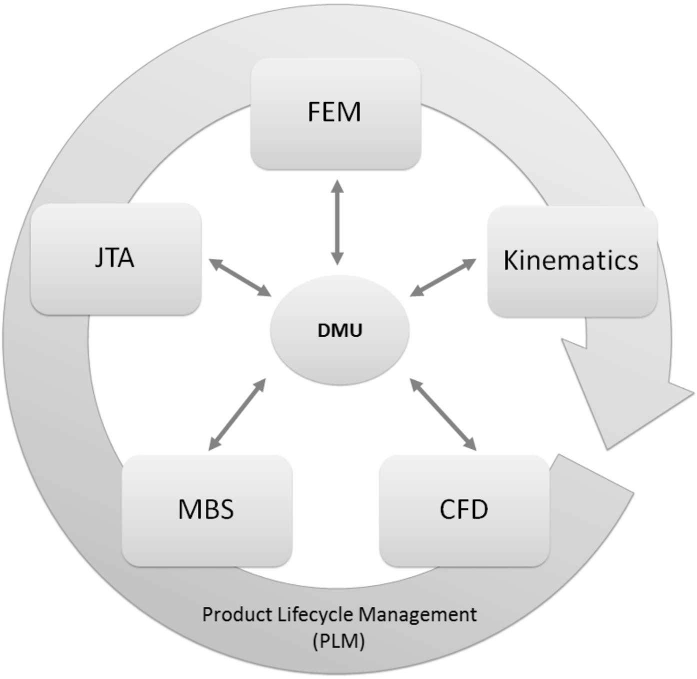


Fig. 6 – Example of virtual-prototype-based design process

A Virtual Prototype (VP) -based design process aims at connecting simulations to each other by providing a common virtual platform to engineers. The DMU of the developed system is the central part of the design process and plays the role of an interactive and collaborative platform. Designers, analysts and engineers share data on the same virtual model, by performing simulations, design updates and other measurements. For instance, the 3D model of the product can be used to perform FEA under loading conditions and the resulting deformed model can be used as inputs for the kinematic simulation. It enables for example a verification of the collision-free trajectory of the system under loading conditions. More complex aspects such as joint tolerances can be integrated into the DMU in order to take into consideration any potential deflection due to joint misalignments. Such virtual testing may be very relevant for heavy systems, in which insignificant joint misalignments on common systems become substantial for complex systems. Hence virtual prototyping-based design process delivers several benefits such as reducing design errors and reworking from the very early design phases.

However, a major limitation of this process is the process formalization and its automation during the product development phase, as well as during more advanced phases of the product lifecycle. This process enables more interactions between the tools, a better communication and help to share information among the stakeholders, but it does not necessarily ensure that the right tool has been used with the right knowledge and has called on the right experience.

In the virtual-prototype-based design process, the use of a PDM system is very common especially combined with a simulation data management (SDM) system (**Fig. 6**). Thus data resulting from the simulations can be collected, stored, traced and linked to the data previously located in the PDM system.

2.3 Simulation-based design process

In the industry, companies are constantly required to provide more innovative and powerful product features, which leads to increased complexity in the products. Physical prototyping becomes then more and more costly as well as time consuming. On the other hand, simulations enable a decrease in the need for physical testing, by virtually testing some aspects of the designed product. Nowadays digital tools for virtual testing are considered essential during the design process and are becoming more and more common during the whole product life-cycle. In order to be able to replace some physical testing aspects with virtual testing, simulations are becoming more advanced by verifying multiple aspects at one time and combining different areas of expertise. Multi-discipline simulations are not without problems and many challenges need to be solved [31, 32].

The research shows that the current trends are moving towards the simulation-based design process [32-34]. In a simulation-based design process, simulations become the central part of the development of the product. In such a process the design model is built based on simulations, unlike the VP-based design process which is centralized around the DMU for instance. Only a few companies are using this type of design process due to the numerous challenges involved. But on the other hand, when the process is well implemented, it offers new perspectives regarding the reduction of the risk of errors as well as decreasing the product's time-to-market. In some cases, full scale prototypes are integral parts of the requirements [35], thus the goal is to perform beforehand a virtual verification of the prototype before manufacturing in order to avoid multiple costly and time consuming iterations during the validation phase.

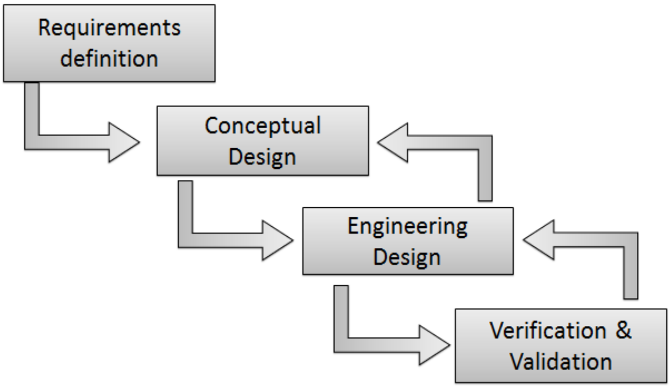


Fig. 7 – Simulation-based design process (adapted from [36])

The simulation-based design process consists of four main stages as shown in **Fig. 7**. Starting from the identification of requirements, they are used as inputs for the next phase. The design concept phase consists of the evaluated alternative product concepts, and one concept is then selected for further development. The design product phase consists of the detailed 3D model of the system on which the detailed level simulations are performed. The last stage includes the verification of the virtual model as well as the model validation by way of physical prototypes.

2.3.1 Conceptual phase

The design concept phase (**Fig. 8**) uses as inputs the initial requirements previously defined by the customer. With the help of a component library, the rough CAD model is built and used as a basis for the preliminary simulations. For each simulation aspect, alternative concept designs are evaluated according to the simulation results so as to determine which concept will be further developed. The evaluation assessment is based on the functional requirements of the system as well as some main features, such as the economic aspects of the different concepts.

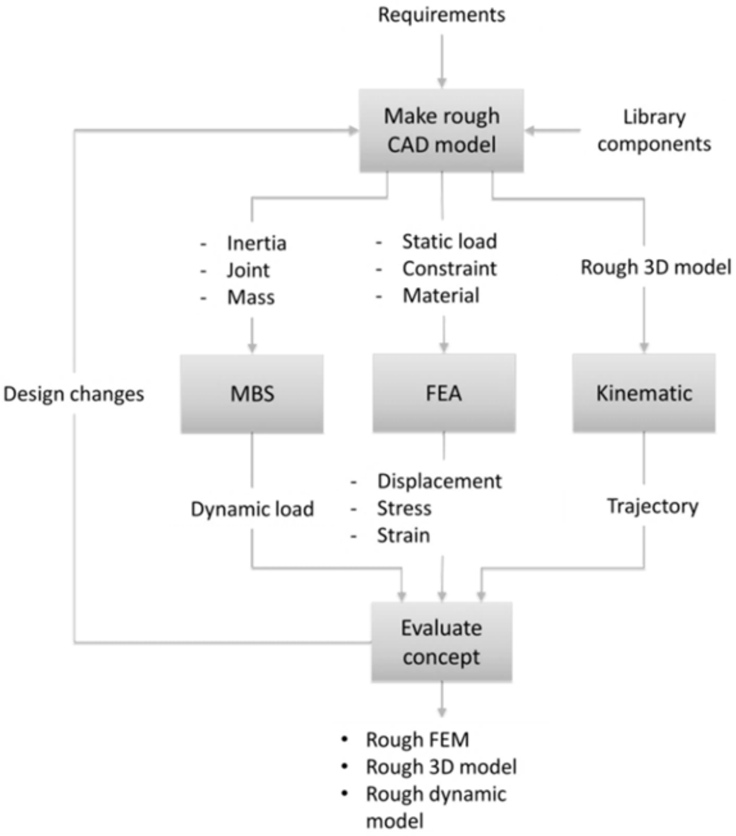


Fig. 8 – Conceptual phase (adapted from [36])

2.3.2 Engineering design phase

The third step consists of the second iterative loop of the simulation-based design process, which is represented by the detailed product design phase (**Fig. 9**). The previously built rough 3D model is used as input to build a more detailed model of the system. Thereafter FEA and MBS are performed so as to refine the model. An assessment activity closes the loop by evaluating the design and committing the design modification requests to the 3D model design phase. In such a process it is very interesting to use a well-furnished component library, in order to allow the process to pre-select the different component options according to the requirements by performing iteration simulation loops with the concepts selected in the previous phase. Taking into consideration cost, reliability and maintenance aspects from the very early stage of the design leads to a reduction in the risk of a further development of a non-conforming solution. After the concept evaluation assessment, feedback is sent to the previous design concept phase in case of a need for modifications or to the modelling phase for the detailed 3D model.

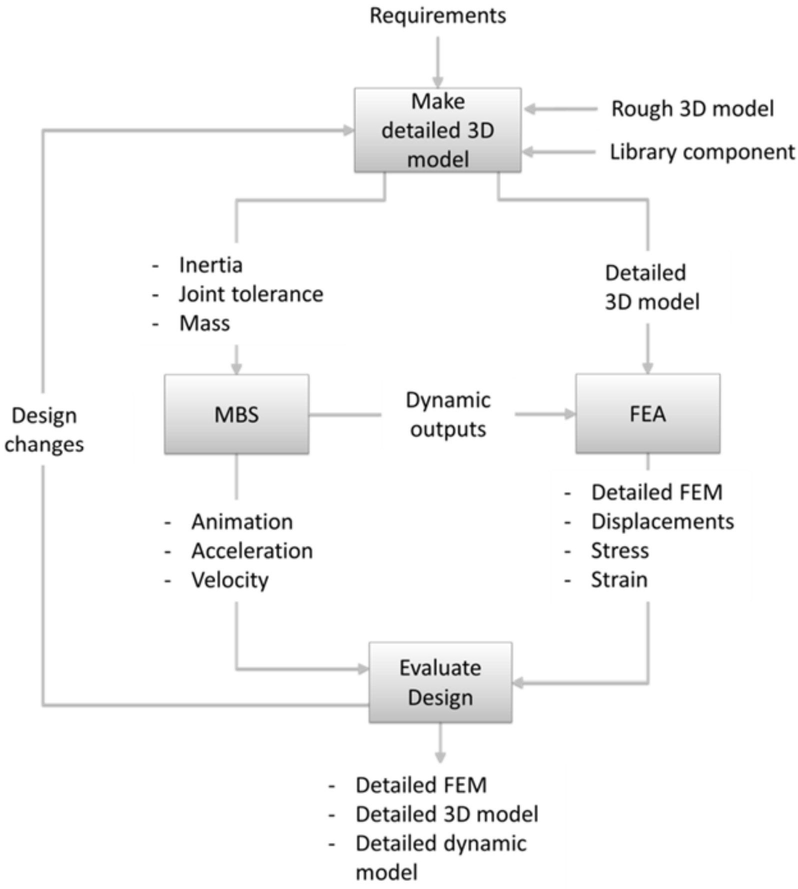


Fig. 9 – Engineering design phase (adapted from [36])

2.3.3 Verification and validation phase

For many systems with mission critical aspects, validation through physical prototypes is a requirement [37]. The aim is to verify the system in the very last stages of the development process. Multiple iterations of the physical prototypes have to be as low as possible due to the manufacturing cost and associated time, for instance. **Fig. 10** illustrates the last phase of the simulation-based design process, the V&V phase. The digital model of the system is virtually tested within its virtual operational environment. The testing phase allows for operating the system as if it was a reality. The virtual tests may consist of using a virtual reality (VR) platform involving human interaction for human-operated systems [38, 39]. The final validation assessment aims to provide evidence that the developed system meets the requirements. Virtual and physical tests are typically subjected to uncertainties that have to be quantified before reaching the validation assessment in order to be able to perform the comparison between the virtual and physical results. After the V&V phase, the product is either validated in the event that it meets the requirements or are sent back to the design concept or product phase for design updates.

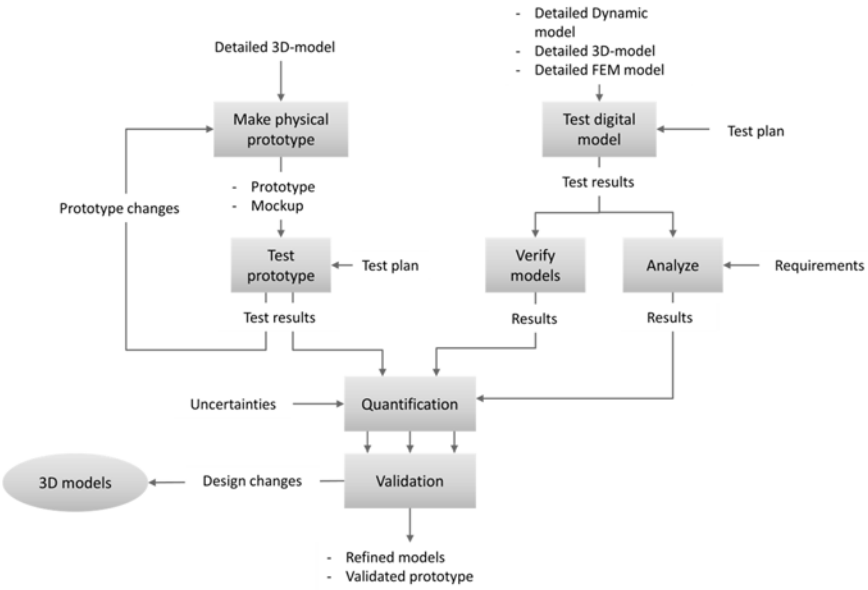


Fig. 10 – Product verification and validation phase (adapted from [36])

In such a process it is essential to use a Simulation Lifecycle Management (SLM) system since simulation becomes the fundamental part of the product development. SLM provides the platform needed to transform simulations from a specialty operation to an enterprise-level product development.

The final assessment activity of the developed V&V process in **Fig. 10** consists of collecting data from the simulation results and performing a quantitative comparison between the simulations and experimental outcomes of the system of interest. In such a process, from the very first requirement to the final experimental test of the physical prototype, some years or even decade may have passed [40], and there is a clear need for managing data throughout the design process, physical testing, and more generally all along the entire system lifecycle.

2.4 Verification and Validation process

The American Institute of Aeronautics and Astronautics (AIAA) produced the first V&V detailed guidelines in 1998: Guide for the Verification and Validation of Computational Fluid Dynamics Simulations [41]. In 2003, the US department of Defence (DoD) published as: DoD Modelling and Simulation (M&S) Verification, Validation and Accreditation (VV&A) [42]. Based on those documents, the American Society of Mechanical Engineers (ASME) edited in 2006 a 'Guide for Verification and Validation in Computational Solid Mechanics' [43] and established the V&V definition as:

> *Verification and validation (V&V) are the processes by which evidence is generated, and credibility is thereby established, that computer models have adequate accuracy and level of detail for their intended use.*

This definition has been adopted as a standard in many engineering fields, and especially among the Computational Solid Mechanics (CSM) domain through the ASME's committee, which stated: '*The objective of the V&V is to validate a model for its intended use*'. Two definitions of *model* are distinguished: the model builder considers that '*the model is validated for its intended use once its predetermined requirements for demonstration of accuracy and predictive capability have been fulfilled*'. From the perspective of the decision-maker or stakeholder: '*the intended use also defines the limitations imposed on the applicability of the model*'. In 2012 the IEEE Standards Association published the IEEE Standard for System and Software Verification and Validation [37], which provides a common language for the Systems Engineering community and describes verification as:

> *Verification is the process of providing objective evidence that the system, software, or hardware and its associated products conform to requirements for all life cycle activities during each life cycle process.*

While validation is:

> *Validation is the process of providing evidence that the system, software, or hardware and its associated products satisfy requirements allocated to it at the end of each life cycle activity, solve the right problem and satisfy intended use and user needs.*

Therefore, the clear industry trend is towards reducing physical testing by replacing suitable aspects with virtual testing. Traditionally, virtual testing is used for verification purposes, thus aiming to provide evidence that the system conforms to the requirements. Digital verification results are then compared with the experimental results. This means that in current best cases, physical prototypes are still a requirement for the final validation assessment in order to provide evidence that the system satisfies its intended use and user needs. Consequently, there is clear evidence that the design verification and validation in the digital domain is a high industrial priority and there is a research focus on such methods [3].

2.4.1 Verification and validation in the SE approach

In the engineering field, the verification of complex systems, such as automotive, airplane or aerospace industries, uses a system breakdown approach starting from the complex system requirements to item requirements [16]. Formalized processes that comply with legislative requirements are of primary importance. Moreover, engineering teams are usually spread worldwide and this requires a strong design and development methodology. The V-model [17, 44] for the verification and validation of a complex product (**Fig. 11**) is the method currently in use to ensure that a product, process or system meets its requirements and fulfils its intended purpose [45].

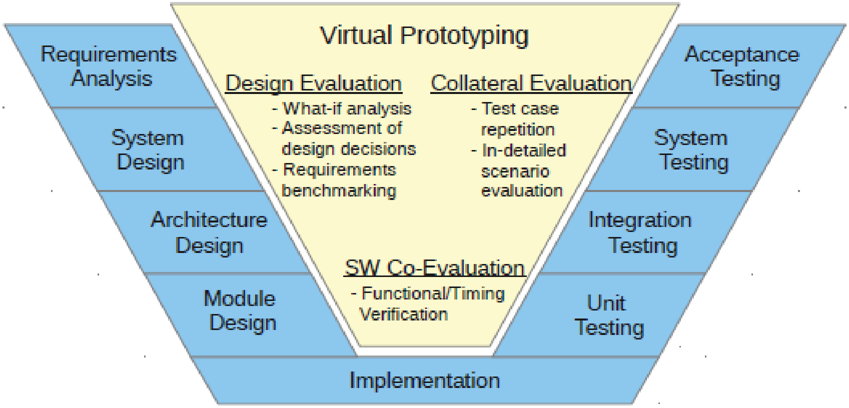


Fig. 11 – Virtual prototyping fills the evaluation gap between the design and testing phase [44]

The presented framework uses virtual prototypes to evaluate the system under development during the design process. Virtual prototypes close the gap between the initial design and the final verification tests before validation assessment [46-50].

In the product development process, it is extremely important to verify the compliance of the requirements by taking them into account from an early stage of the design, and taking into account requirements from all stages of the product lifecycle. In common industries, the traditional way is to transform customer needs from requirements towards proper product features [51]. However, it is difficult to quantify the performance of such features according to real customer needs. Thus there are different methods in the literature that aim to solve this issue. Quality function deployment (QFD) is one of the tools that rates the design requirements with respect to customer needs [52]. This method ensures that the design is driven by customer needs, and has the benefit of being a quantitative approach. The prioritisation of customer needs creates a set of criteria that are then used for the final validation assessment. QFD is a powerful tool to design and translate customer needs into quantitative parameters that are used as requirements to develop and to validate the system. This methodology also supports engineers by limiting efforts required for information search and the decision-making process [53]. The dynamics characteristic of multibody mechanical systems, including revolute joints with clearance, are investigated using a computational methodology and a quantitative analysis method [54].

Fig. 12 - adapted from [43] - represents the V&V framework for complex engineering systems. It shows the parallel approach between the design and experimental phase. The design phase through the digital prototype helps the implementation of the physical experiments. On the other hand, the physical modelling branch enables the validation of the system through a comparison between the outcomes of the physical measurements and the digital simulations. In both branches, quantifications of uncertainties have to be taken into account in order to enhance the accuracy of the validation. This framework must be applied to each level of the studied system.

A model – digital or physical – should always be able to pass a set of basic tests as well as a set of tests using the combined features of the model in order to declare that its implementation is verified and validated along with specific tests. Therefore a model can be verified for most basic aspects with a basic set of tests, depending on the case studies, with a subset of a more advanced set of tests [55].

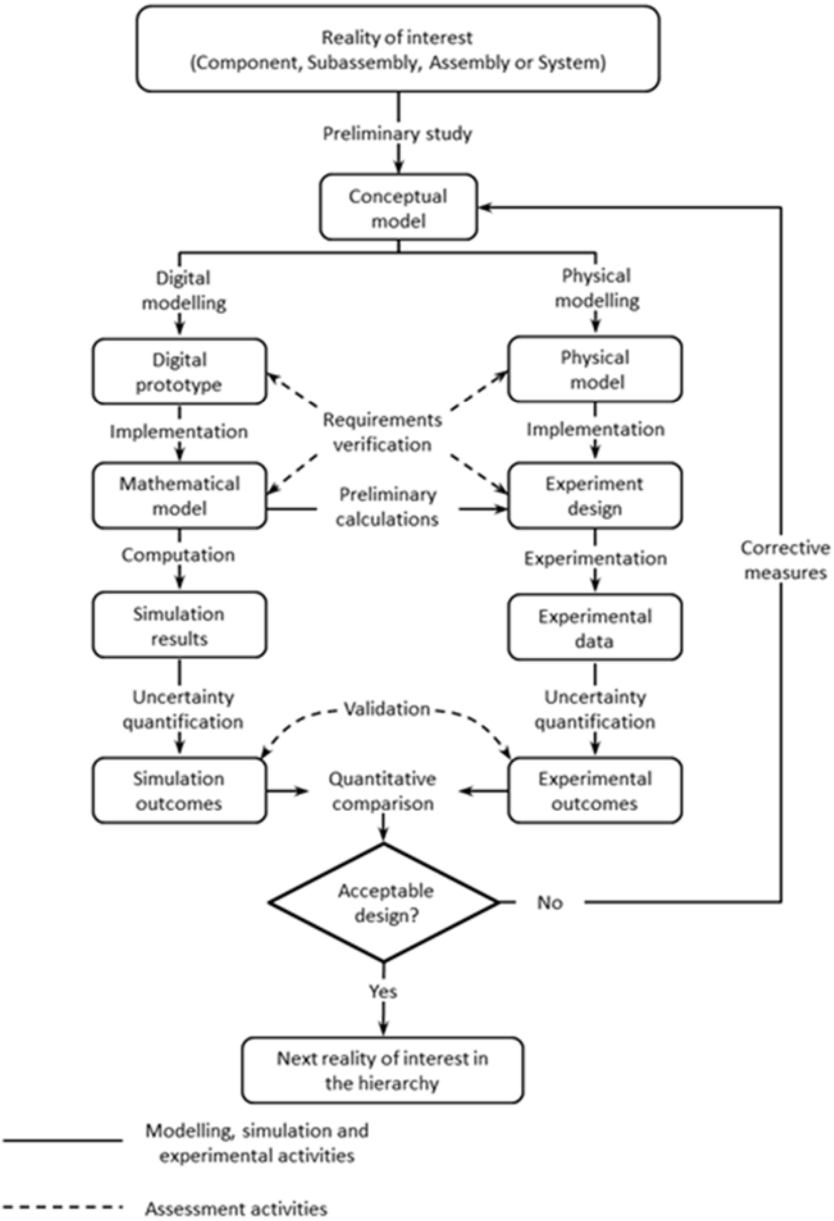


Fig. 12 – V&V framework for complex engineering systems [43]

2.4.2 The use of digital mock-ups in the V&V process

As suggested in the ASME V&V [43] and in order to address the complexity of systems, it is helpful to recognize that all full systems are hierarchical in nature. It is essential to consider a bottom-up approach between components, assemblies, subassemblies and the full system during the modelling phase as well as in the verification process. At each level of the hierarchy, simulations are performed on the virtual representation at different levels. For instance, at the component level, a strength analysis using the finite element method (FEM) aims to verify the integrity of the item of interest under loading conditions. At the sub-assembly level, kinematic simulations would lead to a verification of the operation sequence of the studied subassembly or assembly. However, a more challenging phase is to consider the system interactions between items or assemblies. Combining multibody simulations with, for example, a tolerance analysis would enable an efficient method for verifying the behaviour of the subassemblies and assemblies up until the top level of the hierarchy [56]. However, in order to be validated, joint tolerance measurements have to be performed on the corresponding system of interest in the physical prototype.

Different methods have been developed to reduce the use of physical testing while increasing the use and accuracy of virtual testing for verification and validation purposes. For instance, a hybrid method that combines virtual and physical experiments has been applied in the aircraft industry that has shown promising results [14]. It consists of a model based and a physical testing methodology that provides a product and process design verification environment by simulating variation in tolerances between hierarchical levels and uses physical measurements for higher accuracy in assembly variability predictions. Combining rapid prototyping together with virtual testing to improve the accuracy and the confidence in the V&V process is a still an area of research. However, virtual prototypes are widely used for rapid product development. Through simulations, validation of a product design can be iterated as required without worrying about the manufacturing and material cost of prototypes [57].

However, simulations have some dangers, for example, when a model is not valid for a system regarding its intended purpose. This leads to the following question: how can we verify that the model is a good and reliable model, that it is valid for its intended use? In certain cases, it can be quite difficult and sometimes only a partial answer to this question can be obtained [58]. Different techniques may be useful for at least partially verifying the validity of a model. For instance, the evaluation of the assumptions and approximations that are behind the model by comparing simple cases together with physical experiments, by way of rapid prototypes. Performing sensitivity analysis on the model may result in very small variations in the model parameters and thus give a strong confidence for believing in the validity of the model [59]. Also, cross-checking dimensions and units against the equations will lead to establishing the consistency of the model. Such a formal approach is even used for validating complex engineering systems and has brought about significant advancements in the aerospace industry [60]. The digital modelling phase within the design process plays an important role in the final validation assessment. Different approaches are used to allow for concurrent engineering practices, using management paradigms to maintain competitive edges in product development [61].

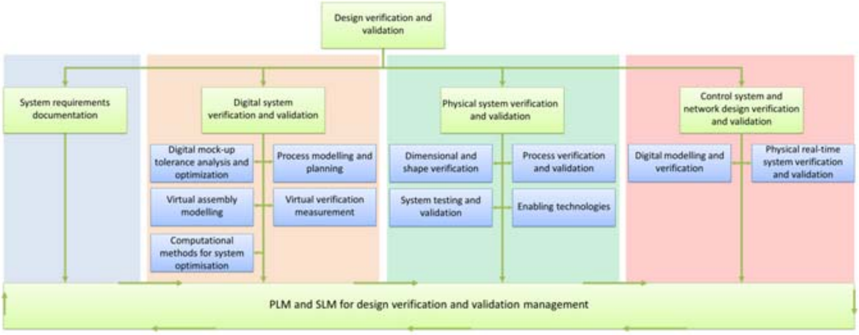

Design verification and validation
System requirements documentation
Digital system verification and validation
Physical system verification and validation
Control system and network design verification and validation
Digital mock-up tolerance analysis and optimization
Process modelling and planning
Virtual assembly modelling
Virtual verification measurement
Computational methods for system optimisation
Dimensional and shape verification
Process verification and validation
System testing and validation
Enabling technologies
Digital modelling and verification
Physical real-time system verification and validation
PLM and SLM for design verification and validation management

Fig. 13 – Conceptual framework for engineering design verification and validation (adapted from [3])

Fig. 13 shows the importance of the Product Life-cycle Management (PLM) during the design process for verification and validation purposes with digital and physical systems. It manages the traceability from the initial requirements of the system to the digital and physical experiments. In this context the advantages of such a framework are numerous: it enables the continuity of the experiments between the different teams; it avoids undesired redundancy of similar simulations, which means time savings; it manages the traceability of the amount of data that complex systems are prone to, such as the number of requirements subjected to modifications, digital mock-ups and validation results.

2.4.3 Requirements definition and management methods

Defining of the requirements is a key aspect in systems engineering for developing a system towards the final verification and validation assessment. The design process can be seen as a loop starting by defining the requirements for developing the system, but also for validating the developed system to ensure that the right system has been built and in the right way. So basically, the requirement definition starts and closes the design loop. For instance, when the developed system has been validated against the requirement, the production can then be launched.

Therefore, the first important aspect of the verification and validation process is to ensure that all the requirements have been rightly and correctly defined. In some cases, it may be possible to correctly define the requirements with only one iteration, but for more complex systems, it is sometimes very difficult to ensure a good requirement definition during the initial phase. Therefore, simulations are used to verify the developed system but they also help to define any new requirements. It is an iterative process hierarchically organised using a bottom-up approach, by verifying component, sub-assemblies, sub-systems and finally the system itself. It is also important to formalize the system, which thus leads to bridging the gap between components and assemblies, and assemblies and sub-systems.

Many real-world physical systems that would normally be subject to V&V can be very complex. To address this complexity and prepare a detailed description of the full system, it is helpful to recognize that the real-world physical system being modelled consists of hierarchical levels. As illustrated in **Fig. 14**, the physical system is typically composed of assemblies that consists of two or more sub-assemblies and a sub-assembly that is composed of individual components.

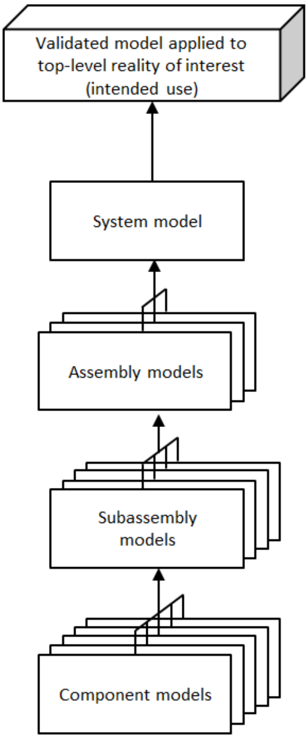

Validated model applied to top-level reality of interest (intended use)
System model
Assembly models
Subassembly models
Component models

Fig. 14 – Bottom-up approach [43]

The recommended approach to V&V is to divide the system hierarchically and then starts the product development phase from the bottom to the up (**Fig. 14**). Such a model results in a multitude set of individual models and forms the basis for defining validation experiments. Those experiments need to be conducted to ensure that for each level of the hierarchy the functions are modelled appropriately [62].

2.5 Simulation tools in the product and production lifecycle

Initially the concept for a product is developed according to the initial request regarding customer needs and is then transformed into a working prototype. The aim of the product development process is to ensure that the product and its components meet the required specifications. Thus innovative engineering approaches consist in streamlining the product engineering and the production process engineering. It enables the integration of CAD designs and CAE information into the synchronisation of the engineering processes.

Fig. 15 shows as a mapping between the product lifecycle and the production lifecycle the simulation tools commonly used in the industry. Even if DMU, FEA and CAD are very well spread along the product development phase, a proper governing principle is still missing that would link the simulation results together as common criteria for decision-making purpose.

Digital manufacturing technologies have been considered an essential part of the continuous effort towards reducing the development time and cost of a product as well as towards expanding customisation options. The simulation-based technology constitutes an essential point of digital manufacturing solutions, since they allow for the experimentation and validation of different product, process and manufacturing system configurations. In the current highly competitive business environment, which constantly faces new challenges, there is always a need for even more efficient and adaptive technologies.

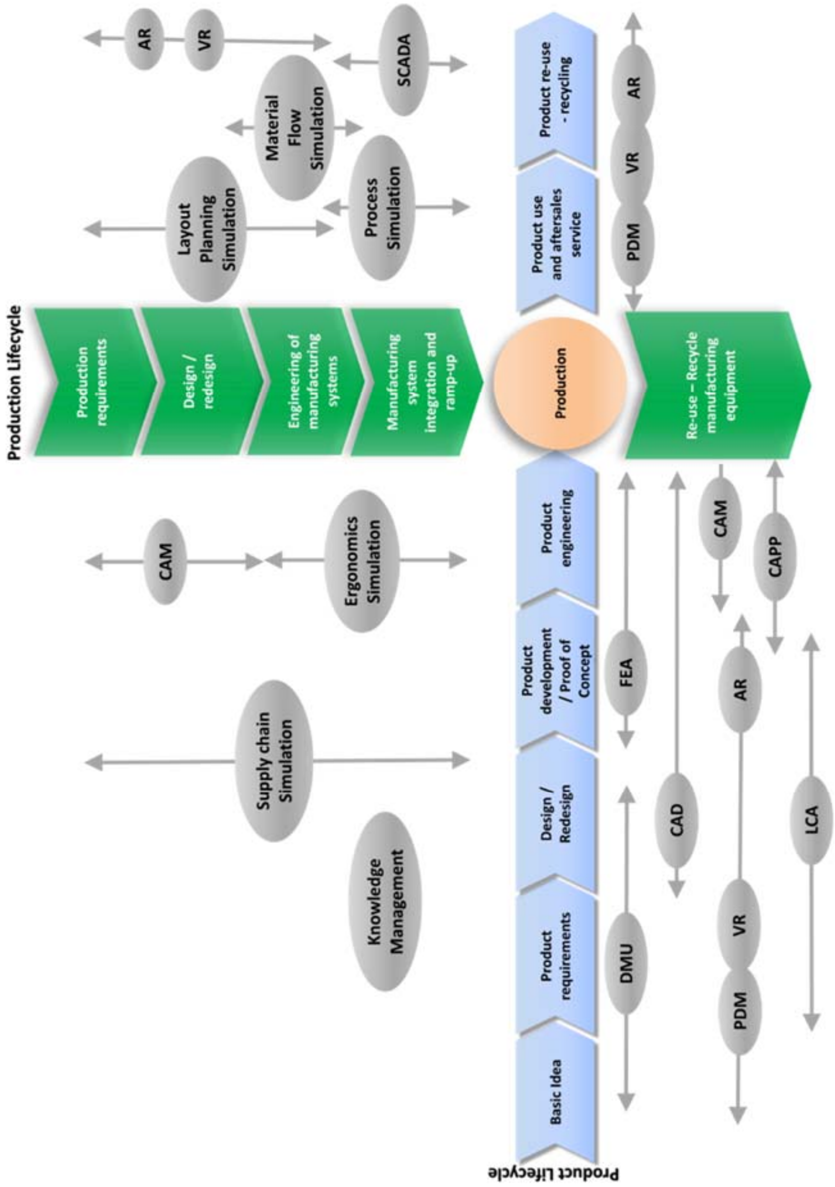


Fig. 15 – Mapping of simulation tools on Product and Production lifecycle (adapted from [63])

2.6 Product and simulation lifecycle environment

Simulation Lifecycle Management (SLM) is not a new concept and a considerable amount of research has been done in this area [64]. However, the term SLM has been used in many different contexts and it seems necessary to give clarifications for a better understanding of this thesis. Many conceptualisations of SLM are borrowed from Product Data Management (PDM) and Lifecycle Management (PLM). PDM is considered to be the administrative process by which data related to a certain product is acquired, validated, stored, protected and processed [65, 66]. As a tool, the PDM is limited by its scale, usually within engineering teams or departments within the same company. Engineering teams can use PDM in order to store and organise a CAD model and other associated documents, according to the scope to be shared within and outside the organisation. It also enables the control of the accessibility and the traceability of those data [22, 67].

The concept of PLM evolves from PDM and aims at connecting product stakeholders over the entire product lifecycle by automating processes from the design to the product retirement [68]. It is used as a business strategy for creating a product-centric environment. In other words, it provides a platform for collaboration on a product for all the stakeholders wherever they are located. **Fig. 16** represents the different phases of a product lifecycle and the respective extent of each of the management systems, starting with System Data Management (SDM) moving towards a more global SLM system.

SLM evolves from PLM by involving simulations in the product lifecycle. It also compliments PLM by associating behavioural simulation data and processes to the DMU and provides a capability to manage the simulation data and processes. The SLM system provides the capability to transform simulations from a specialty operation to an enterprise product development. Thus it enables a simulation-based design in which analysis becomes a fundamental part of the product development. In a product-centric environment, simulations are performed independently of each other; the data resulting from the simulations are then managed by the Simulation Data Management (SDM) system, which is basically similar to a PDM system but with extended capabilities that are able to manage simulation data. Yet since systems are getting more and more complex, the combination of different types of analysis within the same simulation, such as multi-discipline simulations, requires the use of an adequate management system that can handle the amount and variety of data.

The US Department of Energy (DOE) presented an Advanced Process Engineering Co-Simulator (APECS) for the high-fidelity design, analysis and optimization of energy plants [69]. They stated that continued progress in developing co-simulation technology will have profound positive impacts on the design and optimization of high-efficiency products. The traceability is currently an important issue facing the industry. Various data are created during the product lifecycle, and between the first modelling phase and the disposal, several years may have passed. In international projects such as ITER this time span can be seen in a scale of decades. A successful Virtual Prototyping process requires comprehensive integration of communication between various analytical tools so that new products are designed with the current and right inputs [70].

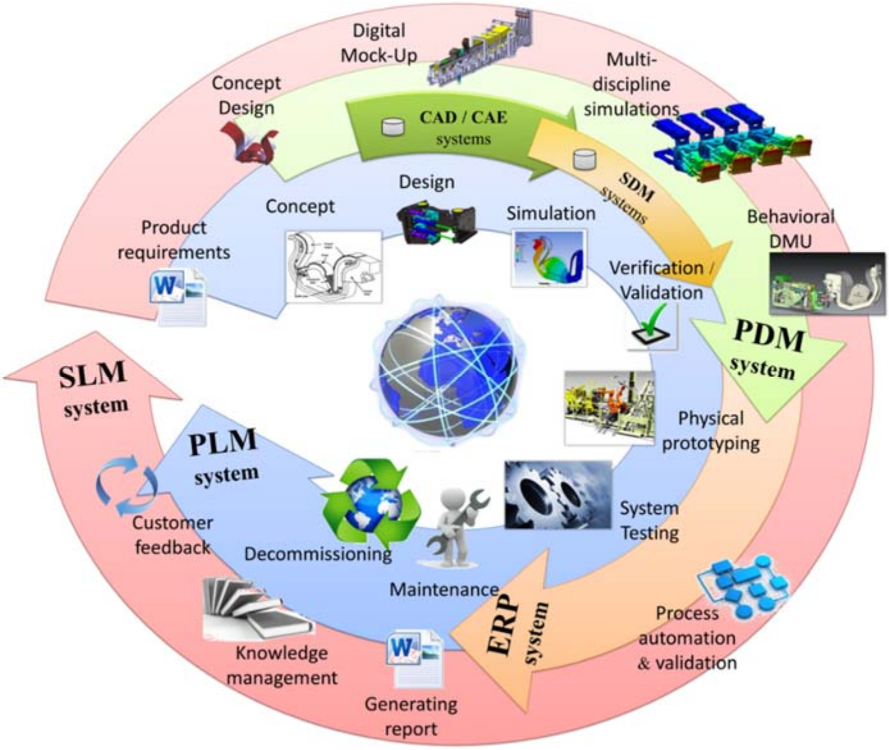


Fig. 16 – Product and Simulation lifecycle management framework

Simulation lifecycle management systems mainly focuses on the virtual world of the product lifecycle [64]. They manage simulations in a narrow collaboration with the PLM and likewise integrate the capabilities of the SDM. SLM capabilities are numerous, including things like the simulation workflow and process automation or other simulation structure management. The benefits of such a tool during the design process as well as all during the lifecycle are therefore accumulative. Considering the number of engineers and scientists involved in the design of systems, the amount of simulation data grows every day and their visibility is therefore continuously decreasing. SLM offers clearer visibility for simulation data and enables engineers and scientists to collaborate on the same simulation platform during each of the design stages.

During the V&V phase, the SLM assists the engineer in finding and collecting the right set of data in order to perform quantitative comparisons for validation purposes for instance. Additionally, reports may be generated fairly straightforwardly from the SLM system, by selecting appropriate information collected from the simulations. The procedural automation capability of the SLM system enables formalisation of the simulation process for all the stakeholders, which increases confidence in the simulation results. When stakeholders are spread worldwide, the simulation-based design process needs to deal with the factor of distance. It involves sharing and securing data worldwide. Additionally, using the same collaboration platform will lead to avoiding issues faced with traditional forms of collaboration, such as time zones and discussion interpretation. Thus the standardization of methods and processes among the engineering network must be promoted.

2.7 Challenges in product design regarding simulation lifecycle management

The design process phase itself covers numerous challenges in the field of product and simulation data management: from the complexity of the products to the number of teams involved on designing such products. Therefore, many challenges are amplified by the accumulating number of factors. The most obvious factor in many industries concerns the long time-span of the product lifecycle, which involves managing data, information and knowledge throughout the entire lifecycle, but as well for parallel and future projects. It is of primary importance to be able to store, trace and reuse data for future projects. Product and simulation data traceability is thereby essential for all during the design, operation, and maintenance, up to the decommissioning phase. In the industry, the number of simulations has considerably increased during the past fifty years [71], as well as the data per simulation, while the cost of simulations has significantly decreased. The volume of data involved in the industry is enormous and growing every day. Terabytes of data per day may be produced within each stakeholder, which may lead to uncountable sets of data produced for the entire design phase. The visibility of files and documents as well as their traceability is thereby very limited without appropriate tools. The accessibility control of simulation data is also very challenging in such situation.

Today, international projects are more and more common in the industry and therefore need to deal with the factor of distance. It involves sharing and securing data worldwide for all stakeholders. The collaboration is also more challenging, especially due to time zones, languages and cultures. Typically, collaboration during the design process is done through video conferences or other meetings. Rarely are teams working on the same model or simulation. To suggest improvement or modification, the collaboration is done by way of email exchange and discussions, but rarely on a common platform. However, using the same collaboration platform will help avoid issues faced with traditional ways of collaborating, such as time zones and interrupted discussions. Thus the standardization of methods and processes among the engineering network must be promoted.

The complexity of the simulation obviously amplifies the challenges. Nowadays multi-discipline simulations are extensively used, especially during the design process. Combining for instance MBS with virtual reality is typical of certain fields. This leads to difficulties in transferring data between tools from different disciplines, which are rarely standardized or result in data loss. Even if the current trend is towards an extended utilization of multi-discipline simulations, it remains a rather challenging task in certain cases. Compatibility between software is one of the most important capabilities for a management tool, from the most common office tool to some very specific simulation software. Usually stakeholders are from a different horizon and a wide range of software is in use, occurring over a long time span. The combination of compatibility with the time factor is an important and current issue in the industry. After discussions with the ship industry for instance, it appeared that data produced during the product design phase was sometimes not usable or even readable a few years later during the commercializing phase due to new software and obsolete data. This means that, in some cases, the product lifecycle loop may not be closed by connecting customer feedback to the design process. This issue is even more important since the time span is even longer.

2.8 Issues in design process modelling

How to model a design process that involves complicated task sequences and diverse resources is an important issue in the product design process. The objective is to capture the semantics associated with the product design process in order to provide decision support in the planning stage. A formal and comprehensive stage-modelling scheme is a prerequisite of coordinating the diversified, distributed activities associated with the design process [72, 73]. The design process identification aims at defining the design activities and identifying the resources in order to achieve the expected results. The process configuration involves multiple alternative roadmaps for designing different concept designs. Therefore, the set of configurations has to be created and evaluated in such a way as to explore the multitude possibilities. As well as the performance evaluation, in order to meet customer expectations, the verification and validation criteria have to be taken into account from the early design phases.

The quality and timeliness of product design and development decisions depends on data availability. There is a need to enhance the availability of digital data in order to make better decisions in a shorter time frame, thereby reducing the product lead-time. Airbus has identified opportunities to enhance the current utilisation of digital design data within the aerospace engineering discipline. Within companies, many decisions have to be taken throughout the product design and development process based on accessing data and information [74]. A virtual simulation-based approach to implementing the evaluations at three hierarchy levels is mainly analysed with a detailed example, which validates the feasibility and effectiveness of the evaluation architecture. Airplanes in the real world involve numerous tasks in operation; it is a huge systematic engineering task to build the simulation systems [75].

2.9 Verification and Validation process in ITER

In ITER, RH equipment classified as a class 1 activity are subjected to the verification of their operation by way of physical prototypes and physical mock-ups [35]. Those systems are usually very complex and physical prototyping can be extremely costly. So unlike most common practices in the industry, it is essential in ITER to virtually verify the developed system before starting the manufacturing phase of the prototype [38, 76, 77]. The remote handling design protocol in use in ITER is formalized by the ITER Remote Maintenance Management System (IRMMS) [78], the ITER Maintenance Management Plan (IMMP) and the ITER

Remote Handling Code Of Practice (IRHCOP) [79]. It states that all RH task methods and detailed procedures are to be validated using virtual reality simulations [80]. Hazard and Operability Analysis (HAZOP) methodology assesses the criticality of Remote handling maintenance activities and aims to identified weak points in the concept design and on the operational sequences of the system [81, 82].

In ITER design, the V&V process starts by modelling the components of the system of interest using computer-aided design (CAD) tools. From the digital representation, the finite element analysis (FEA) is performed to verify the mechanical behaviour of the components. Then the first assessment activity is performed by comparing the FEA results to the requirements. This assessment activity is followed by the assembly phase, which represents virtually the interfaces between components, on which the kinematic simulations are afterwards performed to verify the operational sequences, which are one of the key issues for the verification of RH system design [83]. The kinematic simulation output is then used to perform the dynamic simulation activity. In parallel with the assembly design activity, the joint tolerance analysis is performed to analyse the interaction within joints and between components. This activity is essential since heavy loads are involved in ITER RH equipment. It enables to take into consideration the deflection or other misalignments within the joint. The carried load may result in small deformations in the joint [84], which may lead to significant deflection at the extremity of the entire system. The multibody simulation is then performed by using the tolerance analysis outputs as input data, thereby enabling a better representation of systems under heavy loading conditions, such as with RH equipment for the ITER maintenance [85].

The final assessment activity of the V&V process consists of collecting data from the simulation results and performing a quantitative comparison between the simulations and experimental outcomes of the system of interest. In such a process, from the very first requirement to the final experimental test on the physical prototype, some years or even decades may have passed [40], and there is a clear need to manage the data throughout the design process, physical testing and more generally all through the entire system lifecycle.

3 EVALUATION OF THE VERIFICATION METHODS

This chapter focuses on the development of the verification-driven design process using a reliability-based evaluation method for the decision-making process. The first section covers the notion of digital mock-ups and virtual prototypes. In Section 2.2, the decision-making process and the different evaluation methods are described. The third section of this chapter focuses on the system reliability prediction during the design process. The fourth section covers the discrete event dynamic system and the modelling approach using the stochastic Petri Net as a graphical modelling tool.

3.1 Virtual prototype versus digital mock-up

Today the notion of a virtual prototype and digital mock-up is often confusing. Even if this technology has been widely used in the past few decades in research and in the industry [86], those terms have been used and interpreted in many different ways, which leads to confusion and misunderstanding among researchers, engineers and scientists. This section aims to clarify the different notions used in this thesis and more generally in the engineering field.

Prototypes are early models of equipment developed at full scale to be used for evaluating performance [87]. Traditionally, these are physical prototypes build to identify problems in the initial design. They are subjected to design changes and multiple iterations to optimize the design. In some cases, physical prototype reiterations can be extremely costly. Each new design takes additional time, money, and materials to realize.

In certain industries and especially in fusion engineering, components are often substantial and inherently complex. Thus physical prototypes tend to be even more resource demanding than in the common industry. Therefore and since full-scale physical prototypes are an integral part of the ITER requirements [35], the aim of their use is mainly to validate the system in the last stages of the development process. However, in order to reduce multiple iterations of the physical prototypes, virtual representations of a product are used. Many definitions exist in the state of the art concerning the definition of Virtual Prototyping (VP) and Digital Mock-Ups (DMU). Those terms are usually used and interpreted in an interdependent way. In this thesis, it is important to clarify and remove any confusion between those terms.

A prototype is defined by the Academic Press Dictionary of Science and Technology [88] as follows:

> *'A prototype is an early or original form. In Engineering, a full-scale model of a structure or piece of equipment, used in evaluating form, design, fit, and performance'*

The definition of a mock up is as follow:

> *'In Engineering, a mock up is a scale model, often full-size, of a structure, apparatus, or vehicle, used for study, training, or testing and to determine if the apparatus can be manufactured easily and economically.'*

Both definitions involve a full-scale model of a structure, component, part of the product or the product itself. However, the prototype is more self-oriented in its usability than the mock up. The mock up includes the concept of study and testing, but also training, which involves the notion of the external environment as well as the behaviour of the system. It somehow involves the operator, who constitutes typically the main external factor that can interact with the tested system. While the prototype is more self-oriented, and thus limited in its scope and interaction with external aspects, it leads the design changes by giving a representation of the developed system, but its interaction with the external aspect of its environment such as the operator and its behaviour under certain condition are limited. To summarise, a mock up can be considered as one or a set of prototypes that are implemented into an environment and enable interaction with it [20].

3.1.1 Virtual, digital and real worlds

In this thesis, three different worlds are conceptualized in order to give representation to the notion of a system design or product design by using technology to make this design process more efficient. It aims to increase confidence in the product design while decreasing the risk of errors as well as the amount of resources required.

The introduction of this thesis briefly described the differences and interaction between the three main worlds that are faced in this research work: the virtual world, the digital world and the real world. The virtual world can be seen as an environment that cannot be detected by the common human senses. In the engineering field, a virtual prototype is the notion of a system that is at a very early stage of its design, thereby expressing ideas or offering an interpretation of needs. Thus, the virtual world is used to describe a potential system that needs to be conceptualized and built to then become part of the real world. The conceptualization of the potential system is performed in the digital world. For simple systems, the digitalisation of the system may not be needed and rapid prototyping, which consists of building the prototype from the very early design stage, may be preferred [89]. However, in the modern engineering field, systems are more and more complex and multiple physical iterations may not be cost efficient. In such cases, digitalisation of the system finds its value. It aims to bridge the gap between the virtual world and the physical world (**Fig. 17**).

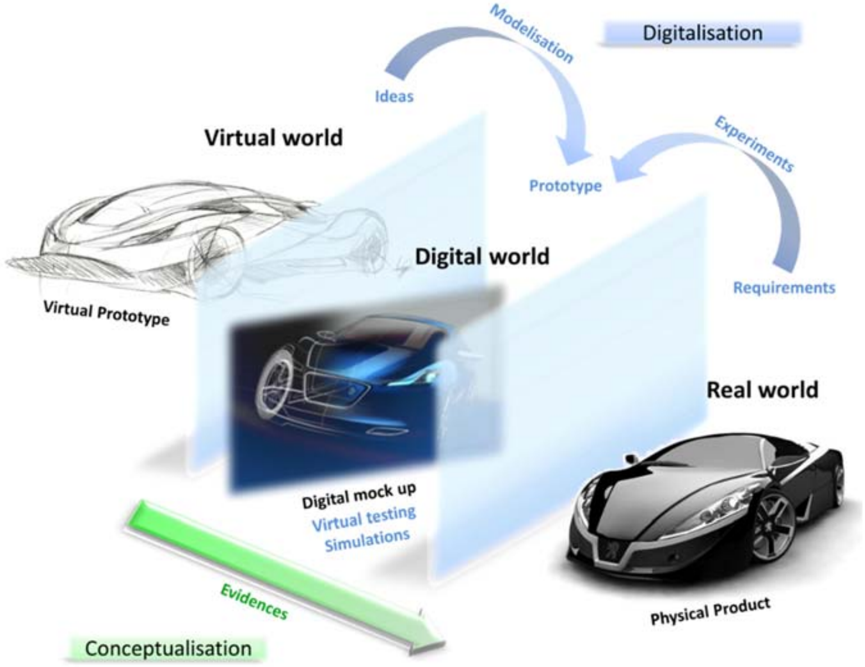


Fig. 17 – From virtual to real prototype

Virtual prototyping consists of representing a system that does not exist yet but thanks to technology, can be digitally represented and thus gives information to our senses that this prototype is digitally real. Technology basically uses a language to translate a potential entity into a digital entity which, computed by our perceiving systems, basically our brain, emerges in and out of the real world. A virtual prototype can be seen as a digital mock-up (DMU) that consists of 3D models that integrate the mechanical structure of a system, its material characteristics or other visual aspects. From a virtual prototype emerges a digital prototype that is integrated into a digital environment. This whole set up constitutes the Digital Mock-Up (DMU). Virtual experiments (commonly called simulations) can then be performed, while design modifications on the virtual model are less resource consuming than on a physical prototype. Simulations performed with a DMU can include, for instance, kinematics, dynamics, strength and thermodynamics. This leads to a better cost efficiency when decreasing the time of the development process. Furthermore, one of the most important advantages of this kind of simulation is the possibility to perform virtual measurements at any point. This is not always possible in real cases due, for instance, to the lack of space [90]. At the start of the new millennium, the goal of DMU was to replace the traditional business to process, based on a Physical Mock-Up (PMU). The visionary goal was a process with only a single PMU for final verification, certification, and release to volume manufacturing. The goal is nowadays to perform verifications as early as possible, front-loading the engineering, manufacturing, service, manufacturing, and recycling tasks to the concept phase [91]. Additionally DMU enables better cooperation between stakeholders who are spread worldwide and leads to a cut in the time delay between new ideas and feedback [67]. Ideally, virtual prototyping should comply with the Concurrent Engineering (CE) approach and must therefore allow simultaneous collaboration by various engineering teams. Virtual prototyping is used in a wide range of industries, such as mechanical related fields like aeronautics [74]. The evaluation of the prototype should include a prediction and simulation of manufacturing processes and production planning, both during the conceptual design when the design data are incomplete [70].

VP is used in a wide range of industries. Starting in the automotive industries, industries from all over the world have heavily invested in VP technology for the last few decades, which has led to higher quality vehicles with lower development costs as well as fewer prototypes and reduced design errors [92]. The aerospace industry has lead the development of VP tools and played an important role in the adoption of VP in the standardisation of the design process [93]. The communication and information-exchange between the tools have been an area of research, since stakeholders have usually been spread worldwide in such domains. However, to maintain their competitive edge, companies are pursuing system validation by using digital mock-ups [94].

Digital manufacturing has shown some benefits in the industry in terms of reduced production costs and reduced overall time-to-market but also in terms of increased production outputs [95].

3.1.2 Virtual Reality

Many other terms gravitate around virtual and digital notions, such as Virtual Reality (VR), Virtual Environment (VE), Virtual Testing (VT), and Virtual Model (VM), leading to even more confusion. It is therefore important at this point to clarify matters.

Virtual reality can be defined as follow:

> *Virtual Reality is a way for humans to visualize, manipulate and interact with computers and extremely complex data.* [96]

The visualization part refers to the digitalisation of visual, auditory or other sensual aspects for the user through the computer. This environment may be a CAD model, a simulation, or a database for instance. Virtual Reality (VR) is one of the VP modelling tools that give the illusion to the user of being in the same environment as the model [11, 97]. VP consists of three domains [98]: VR, simulation, and manufacturing process design. However, almost any form of computer model will serve for some purpose as a virtual prototype, and VP terminology should not be restricted to the domain of VR [86, 99]. Most of the CAE commercial packages also refer to digital modelling as VP, without necessarily specifying any application of VR. However, VR can be a powerful tool for testing and evaluating new products and ideas, decreasing the time to market and reducing product cost. Manufacturing processes and design can be defined, modelled and verified before they can be actually implemented. Virtual reality offers ways of not only visualising problems but also of interacting with the virtual environment (VE) to solve different problems effectively and efficiently [100]. These visualisations, combined with interaction can improve the decision-making capabilities of engineers, thereby improving quality and reducing the development time for new products. If VR technologies are effectively implemented, it can result in improved product design, with superior quality leading to better customer satisfaction [101].

The current trend in the industry is to rapidly increase product complexity together with decreasing development budgets and time-to-market pressures. Thus it leads to the development of alternatives to the reliance on physical testing [102]. Thus, the use of VP applications, such as computer aided technology (CAx) in technical projects is a way to increase the efficiency of technical problem-solving. CAx and product lifecycle management applications (PLM) can be used in addition to engineering solutions [103] to increase confidence in the developed system, from the early design phase towards the verification and validation process. One of the restrictions of present VP technologies is the lack of methods for exchanging data among different tools [70, 104].

3.1.3 Virtual Testing

Virtual Testing (VT) is an integral part of the digital mock-up that aims to translate a physical experiment into computer models in order to interact with the virtual prototype. So basically an experiment is the process of extracting information from a system by exercising its inputs [105]. Additionally, to be able to perform an experiment on a system, it is required to be both controllable and observable. A model of a system is anything that an experiment can be applied to in order to answer questions about that system. Therefore a simulation is a virtual experiment or test performed on a virtual prototype [58].

Nowadays, simulations are widely used among the industry, and the current trend is clearly towards developing new methods for more accurately simulating the performance of a system. Multidisciplinary simulations, such as the combination of the finite elements method and multi-body simulation [106] or continuous collision detection combined with constraint-based dynamics [107] are sources of innovations within the design process and aim to increase confidence in the developed system from the early design phase [108]. Taking into account manufacturing errors from the very early design phases is also very important and influences production costs in a big way [109]. Tolerance design via virtual testing enables engineers to optimize design tolerances and manufacturing variation to achieve the highest quality at the most cost effective price during the design and planning stage [110]. VT is also widely used in other industries such as the construction industry, to assist planners in verifying their plans to eliminate construction risks before the commencement of the construction phase [111].

In ITER, VR simulations are used to analyse the maintenance process, to predict the mean time to repair and to ensure the RH compatibility of sub-systems, especially during the development of procedures and the identification of tooling requirements. The VR analysis together with a dedicated digital mock-up help to demonstrate the RH compatibility of the system and provide input to the design and to support the development of RH maintenance tooling [112, 113].

3.1.4 Rapid prototyping

Solving problems in the virtual domain helps to reduce physical prototyping costs and time. However, VP has high initial investment costs in terms of hardware and software and demands skilled and experienced operators to extract the full benefit from the software [89]. Rapid prototyping (RP) is sometimes preferred to VP for kinematic simulation, assembly, fit and interference checking. As a physical part, RP allows the user to gauge the size of the prototype. It is also used for ergonomic and tactile evaluations [114]. Therefore, RP may be preferred in some cases, particularly for simple and uni-disciplinary systems. Some studies present hybrid approaches that combine both rapid and virtual prototypes. It consists of a virtual prototyping system that integrates virtual reality with rapid prototyping in order to enhance digital prototypes and increase confidence during product development [29, 115].

3.2 Decision-making process

The decision process is usually based on the verification and validation process. The aim is to generate, collect and analyse design information during the product development phase for decision-makers. The purpose of the decision-making process is to determine whether further technology development is required, or to choose a design concept to be later validated for its intended use. Design information is used to analyse product performance, reliability, and manufacturing costs early in the product development stage and in conducting quantitative trade-offs for design decision-making. Virtual prototyping can shorten the overall product development cycle, improve product quality, and reduce product cost [116].

Fixing problems after they have occurred is not satisfactory in today’s competitive market situation. Therefore, preventive measures for potential failures are fundamental during the entire design process of a new product. Preventive measures will lead to decreased manufacturing costs, but will also increase customer satisfaction, since potential failures are pointed out before they reach the customer. Reliability is an important parameter in terms of confidence in the design. Several methods that help to evaluate the reliability of a system during its development are of primary importance as well as methods for supporting design decision-making through a quantitative approach for both concept designs and detail designs.

Two methods are commonly used during the decision-making process for evaluating a design. The first tool is the commonly used Failure Mode and Effect Analysis (FMEA). The second one is the Fuzzy Analytical Hierarchy Process (FAHP). These methods are different approaches to prioritise and failure modes during the design process.

3.2.1 Failure Mode and Effect Analysis (FMEA)

The FMEA is a method used to identify potential failures from the early design stages. In this method, potential failure modes, effects of failures, prioritisation of the failures as well as corrective measures are identified. It is therefore a powerful tool for guiding the development of a new product, since a new product design is a pretty difficult process and requires expert knowledge in different areas such as customer expectations, product specification and operational needs. However, interactions between these variable are always a difficult task, even for the most advanced expert. The extensive experience of an expert is a key point in the concept design, but it is not always possible to have access to experienced and knowledgeable people. Thus, standardized methods are necessary.

In the FMEA approach, the main objective is to identify and prevent potential failure modes that can occur during the development of a system. To be efficient, the FMEA design should start before the design process and should be finalized before the end of the design process. The aim is for the last stage of the design process to be the Validation assessment and FMEA results to be used as input for the validation assessment of the developed system.

As part of the FMEA family, the Functional Failure Mode and Effect Analysis (FFMEA) approach is based on the system functionality. It focuses on the functional level of the developed system during the design process. Its main goal is not to determine corrective actions as with FMEA, but rather to avoid them in the first place. Basically it consists of thinking about generic system functional failure modes from the early design phases but also all through the design process. Thus the design is based on the FFMEA analysis in order to identify new functionality that can prevent failure.

The FFMEA process is organised into a few steps as shown in **Fig. 18**:

- Identify and list the system functions and build a hierarchical structure and divide the system into sub-systems, assemblies and components.
- For each function identify potential failure modes
- For each failure mode identify effects experienced by the user
- For each failure mode identify causes
- For each failure mode identify current detection methods employed
- Rate the probability of Occurrence (O), Severity (S) and the probability of Detection (D)
- Determine the Risk Priority Number (RPN)
- Consider high RPN for new functionality or design ideas

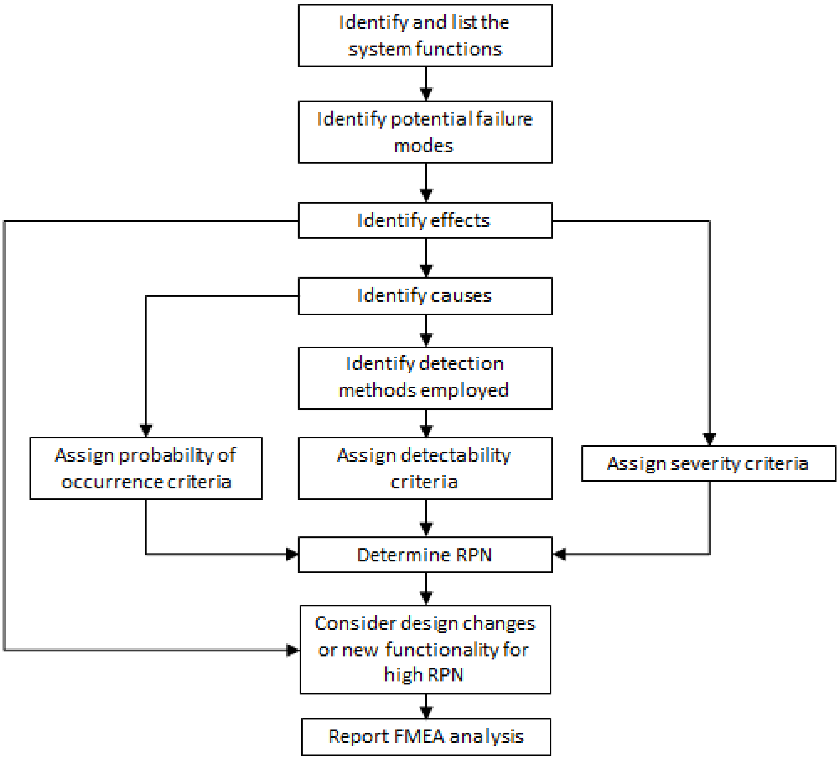

Identify and list the system functions
Identify potential failure modes
Identify effects
Identify causes
Identify detection methods employed
Assign probability of occurrence criteria
Assign detectability criteria
Assign severity criteria
Determine RPN
Consider design changes or new functionality for high RPN
Report FMEA analysis

Fig. 18 – FFMEA traditional procedure

FFMEA is a useful tool to discover failures in products and processes. However, there are some limitations to the use of such a tool. For instance, different combinations of O, S and D may produce exactly the same value of RPN, though their risk implications may be totally different. In this method it is assumed that each risk factor has weight, thus the priority of severity, occurrence and detection are not taken into account. Moreover, this may not be always the case in the reality.

It is important to note that FFMEA is a relative and subjective analysis, which means that the qualitative judgment in this method, through the use of words such as 'more' and 'less', increase the uncertainty of the judgment. For instance, if two different teams perform an FFMEA on the same function, the ratings given are likely to be different. Yet the final ranking of the failure according to the final RPN may likely to be the same. However, this qualitative analysis may not be appropriate in certain processes, such as in the verification and validation process.

3.2.2 Fuzzy Analytic Hierarchy Process (AHP)

To overcome the limitation of traditional analysis, the Fuzzy Analytic Hierarchy Process (AHP) method has been developed. It allows the assigning of different weight to each of the risk factors used in the FFMEA analysis [117]. The Fuzzy AHP method is described in the next section 3.2.3. Many decision-making and problem-solving tasks are too complex to be understood quantitatively. In a decision-making process, it is really important to understand the different aspects of human language. Thus to deal with this vagueness of human thought, Zadeh [118] first introduced the fuzzy set theory, which was oriented to the rationality of uncertainty due to vagueness or imprecision.

The AHP involves pairwise comparisons in order to identify the preferred concept alternative. It consists of 5 major steps: (1) goal statement, (2) decomposition, (3) hierarchical structuring, (4) pairwise comparison and (5) synthesis [119]. During goal statement and decomposition, the design objectives are identified and decomposed to include all conceived attribute elements relevant to the design space. Based on their established significance, a hierarchical framework of the goal and attributes is generated. During the pairwise comparison a matrix is developed to compare and rank pairs of potential concept alternatives. In the final synthesis step the quantified rankings of the various alternatives are compared with the highest alternative ranking, eventually revealing the best possible concept [120].

The fuzzy approach is a solution that enables a more accurate ranking of potential risks. The Fuzzy Analytic Hierarchy Process (AHP) is a decision-making tool [121] that is increasingly used as standard within the FMEA analysis. One of the main advantages of this method is its ease to assess multiple criteria at the same time. It is a knowledge-based method that is built from expert opinion and experience in the form of fuzzy IF-THEN rules. Usually, the traditional approaches, such as FMEA, cannot really take into account the human mind in a realistic way [122, 123]. However, by including the fuzzy logic into the FMEA process it aims to provide a more reasonable and convenient analysis.

3.2.3 AHP applied to FMEA

The fuzzy method is used to determine the risk priority number (RPN) of the Design FMEA analysis [117, 124, 125]. Between customer requirements, design information and expert opinion, FMEA inputs are often uncertain or vague during the conceptual design phase. The relationships between failure modes and their effects are very complex, subjective and qualitative. Therefore, the fuzzy approach aims to improve the effectiveness of the FMEA process.

The overall picture of the fuzzy AHP approach is shown in **Fig. 19**:

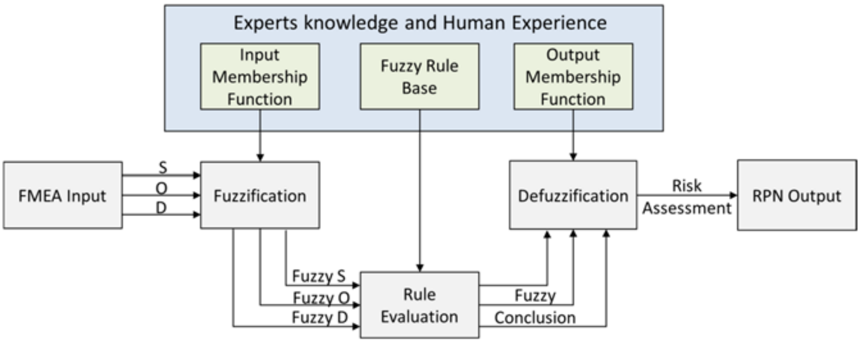


Fig. 19 – Structure of the FFMEA based on Fuzzy AHP

The three inputs *Severity (S)*, *Occurrence (O)* and *Detectability (D)* are fuzzified. This fuzzification step uses linguistic variables to describe the severity, occurrence and detectability of the failure and their degree of membership. **Table 1** shows the five terms to describe the inputs: *Remote (R), Low (L), Moderate (M), High (H) and Very High (VH)*. The input is then transformed into a fuzzy input to be processed by the rule evaluation.

Table 1 - Severity, Occurrence and Detectability evaluation criteria

Rank	O / S / D	Linguistic variable
9, 10	Very High	VH
7, 8	High	H
4, 5, 6	Moderate	M
3	Low	L
1, 2	Very Low	VL

The second step consists of using the IF-THEN rules made by experts and engineers. They are integrated into the fuzzy rule base that can be associated with a mapping from fuzzy inputs to a fuzzy conclusion. Finally, the third step consists of defining the membership functions of output fuzzy sets and the defuzzifier, which can be transformed into a real-valued risk representation.

Basically experts and designers define the membership functions. Let's assume that each expert has a degree of competence $W_i(i = 1, \ldots, n)$ based on their experience and knowledge and the sum of the degree of competence of the team must be one. Then the Trapezoidal fuzzy number is used to develop the membership function [126].

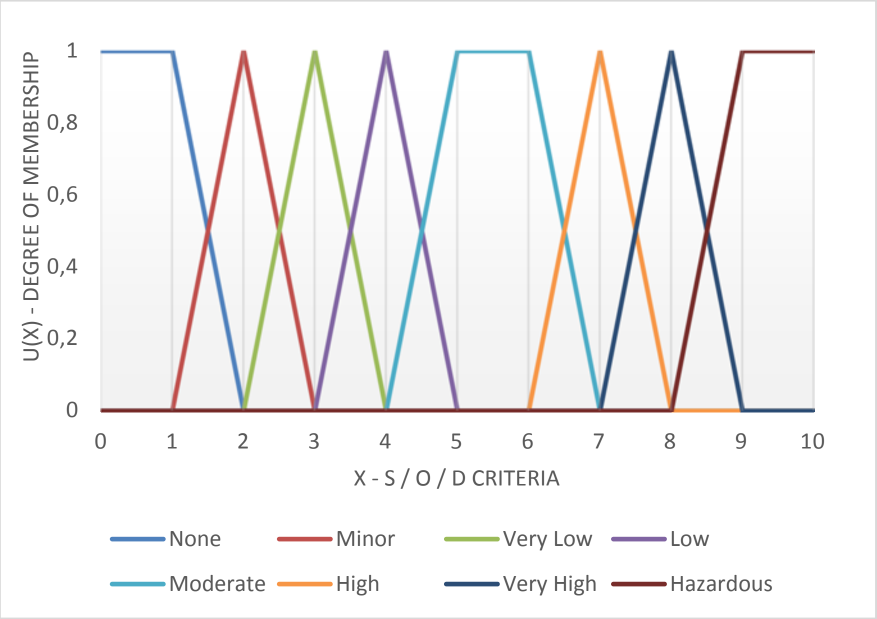


Fig. 20 – Membership functions

In **Fig. 20**, *x* represents the rating of the occurrence, severity or detection and *u(x)* represents the degree of membership. In order to evaluate the degree of membership, each expert is asked to give criteria for the failure (represented by *a, b, c* and *d* on the figure) in the interval of [1-10]. Then the value of the membership function is 0, such as *u(a)* or *u(d)* on the figure, when the rating does not belong to the linguistic term. However, the value of the membership function is 1, such as *u(b)* or *u(c)* on the figure, when the rating completely belongs to the linguistic term. In-between the rating belongs to a degree of membership between 0 and 1. In a fuzzy interference system (FIS) an expert's knowledge is represented with a rule base comprising fuzzy production rules that have an antecedent (input) and consequent (output).

3.3 Reliability prediction

The prediction of reliability is performed during the requirement definition and design phases. It helps the decision-making process for concept design selection so as to ensure the proper functional behaviour of the system during system development. The complication related to the reliability prediction of complex systems such as mechatronics is located in the interaction of different technologies that interact with each other [127]. In other words, it needs to take into account the potential failure that can occur between the control system and the actuator.

In order to design the reliability of a complex system, it is necessary to use a formalized evaluation method that takes into account different parameters, such as: the hierarchical interaction of components, the functional and dysfunctional behaviour, the data sources for component reliability, and the technology of the component. The Determinist Stochastic Petri Nets (DSPNs) method has been developed to provide a solution to these constraints [128]. MIL-HDBK-217 (Electronics Reliability Prediction) [129], Bellcore/Telcordia (Electronics Reliability Prediction) and NSWC (Mechanical Reliability Prediction) [130] provide failure rate and MTBF (Mean Time Between Failures) data for electronic and mechanical parts and equipment [131].

A product reliability evaluation through simulations focuses on the probability of specific failure events (or failure modes). The failure event corresponds to a product performance measure, such as the flexibility of a mechanical component. For the reliability analysis of a single failure event, the failure function is defined as [132]:

(1)

$$\mathrm{g}(X) = \psi^{u} - \psi(X)$$

Where ψ is a product performance measure, $\psi^{u}$is the design requirement of the product performance and X is the vector of random variables.

When product performance does not meet the requirement, which means when $\psi^{u} \leq \psi(X)$, the event fails. Therefore, the probability of failure $P_f$of the event $g(X) \leq 0$ is

(2)

$$P_f = P[g(X) \leq 0]$$

Where P is the event probability.

Given the join probability density function $F_x(x)$ of the random variable$\mathrm{X}$, the probability of failure for a single event of a mechanical component can be expressed as:

(3)

$$P_f = P[g(X) \leq 0] = \int \int_{g(X)\leq 0} \dots \int f_X(x) dx$$

Once the probability of several failure events in sub-systems or components are computed, the system reliability can be obtained using the fault tree analysis method for instance [133, 134]. Ultimately, the results obtained by performing a reliability prediction analysis can be useful when conducting further analyses like a FMECA (Failure Modes, Effects and Criticality Analysis), RBD (Reliability Block Diagram) or a Fault Tree analysis. The reliability predictions are used to evaluate the probabilities of failure events described in these alternate failure analysis models [135]. In order to model the reliability of a system or component, various probability distribution models can be used to model different behaviour. The two most common distribution functions are described below: the exponential distribution and the Weibull distribution.

3.3.1 Exponential distribution

The exponential distribution plays an important role in reliability engineering because it has a constant failure rate [136]. It represents component lifetimes that have sudden failure modes. Usually this distribution is used to model the lifetime of electronic and electrical components and systems. A component that has not failed yet is considered to be an as-good-as-new component.

The exponential reliability is characterized by:

- Reliability:

(4)

$$R(t) = e^{-\lambda t}$$

- Probability of density:

(5)

$$f(t) = \lambda e^{-\lambda t}$$

- Failure rate:

(6)

$$\lambda(t) = \lambda$$

The failure rate for this distribution is λ, a constant, which is the main reason for this widely used distribution. Because of its constant failure rate property, the exponential is an excellent model for the long flat 'intrinsic failure' portion of the 18 System Software Reliability bathtub curve.

3.3.2 Weibull distribution

The exponential distribution is often limited in applicability owing to the memoryless property. The Weibull distribution is a generalization of the exponential distribution and is commonly used to represent among other things fatigue life and ball bearing life [137]. The Weibull distribution is used to model component behaviour in the three phases of the component's lifetime, using the shape parameter β (**Fig. 21**).

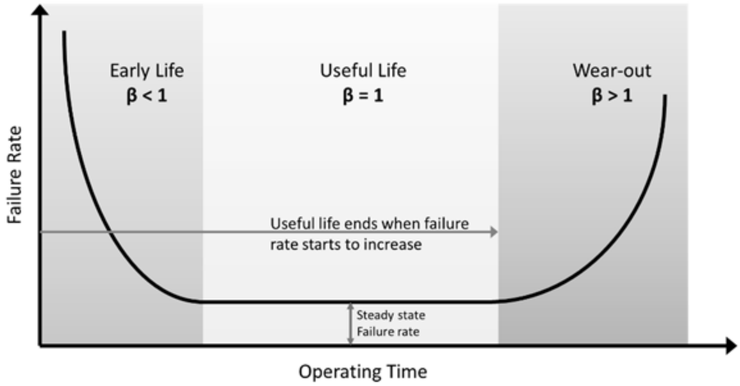


Fig. 21 – Bathtub curve modelled with a Weibull Distribution

The reliability of a mechanical component characterized by a Weibull distribution is given by:

(7)
$$R(t) = e^{-\left(\frac{t}{\theta}\right)^{\beta}}$$

Where:
θ : scale parameter
β : shape parameter

Its probability density function is:

(8)
$$f(t) = \frac{\beta t^{\beta-1}}{\theta^{\beta}} e^{-\left(\frac{t}{\theta}\right)^{\beta}}$$

And the failure rate is:

(9)
$$\lambda(t) = \frac{\beta t^{\beta-1}}{\theta^{\beta}}$$

3.3.3 Other distributions

Other distribution functions exist such as binomial distribution, which is used in reliability testing for dealing with a situation in which an event is either a success or a failure; the Poisson distribution which is commonly used to deal with events in which the sample size is unknown; the normal distribution may be used to model a system in which a failure results due to a wear out effect, especially for mechanical components, and Log-normal distribution is used mainly in maintainability engineering to model, for instance, failure probabilities of repairable systems.

3.4 Discrete event dynamic systems

Briefly, the Petri Net concept is a graphic and mathematical tool for modelling, analysing and designing discrete events and discrete states of systems. It consists of a graphical representation of places and transition networks. The discrete aspect of the Petri Net model allows modelling of the operational and functional sequence of the system. Each place, represented by a circle, indicates the state of the system or the operation. The token represents the current state of the sequence at a time t. A fundamental aspect of stochastic PN is that each place is always followed by a transition. This transition sets the operational time in which the system needs to perform the task represented by the place.

The operational sequence of a system is modelled as a discrete event dynamic Petri Net. Tokens represent the current state of the operations. Transitions are set with a time delay that allows for providing a lapse time for each phase of the operation. The discrete event dynamic system represents the higher Petri Net level in this approach. The modelling approach in the Stochastic Petri Net consists in using Dirac distribution to model the immediate transition of the discrete event dynamic system.

The Dirac distribution δ(x) is defined by:

(10)

$$\int_{-\infty}^{\infty} \delta(x)dx = 1$$

The distribution is usually depicted by the arrow of unit length (See **Fig. 22**).

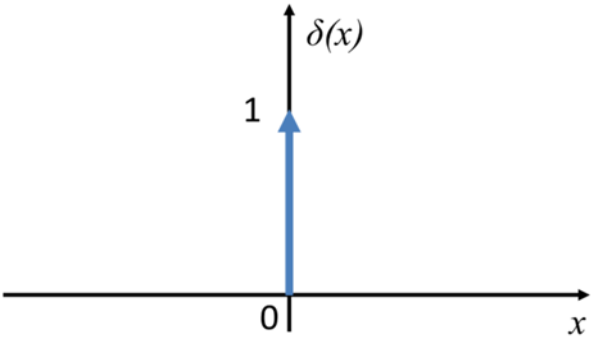


Fig. 22 – Representation of Dirac distribution δ(x)

3.4.1 Function-based Petri Network model

Petri Net is a graphic and mathematical tool for modelling, analysis and design of discrete events dynamic systems (DEDS) [128]. Basically a Petri Net model of a system is built by using a top-down approach. Firstly, the conceptual model is built and then it is refined into a functional model.

The Petri network provides a convenient graphical representation [138] of a place transition net comprised of the following components:

- Places: represented by circles and indicating conditions or objects
- Tokens: represented by black dots and indicating the specific value of the condition or objects
- Transitions: represented by rectangles and indicating activities that change the values of conditions and objects
- Arcs: represented by arrows and indicating the connections between places and transitions that give the information on which object is changed by which activity.

The second hierarchical level of the approach consists in modelling the system functional Petri Net, which is basically the possible modes of a system: standby, working or failure modes. In this level, the functional Petri net consists of timeless transitions, since the state of the system is led by the higher hierarchical event dynamic system. However, transitions from working and standby modes towards a failure mode of a component or a function are following a reliability distribution relative to the function or the component. Hierarchical levels are interacting with each other using different types of variables. These variables are used to fire a token from standby to working modes when the operational task requires the activation of a certain system. Therefore, discrete event dynamic systems using stochastic Petri nets are used in this study to model the operational sequence of the system as well as the entire system design from the functional level up to the component level when the design process is in a more advanced phase. The dynamic discrete sequence event becomes the basis of the Functional Stochastic Petri Net approach.

3.4.2 From discrete to continuous Petri Net

The marking of a place in a Petri Net may correspond to the state of a device, e.g. a machine is or is not available. This marking can be compared to a Boolean variable. A marking can also be associated with an integer, e.g. the number of parts in the input buffer of a machine. In this second case, the number of tokens may be a large number. This may result in such a large number of reachable markings that a limit is formed for use of PNs. In some fields, systems may have a very large numbers of states: telecommunication systems, traffic systems, logistics. Modelling the evolution of a large number of discrete entities by a continuous model is known to provide a good approximation. Let us consider a very simple though quite illustrative system: an hourglass.

As illustrated in **Fig. 23**, some amount of time T is measured by passing a large number of grains, N, from the upper part to the lower part of the hourglass. The number of grains in the upper part is a discrete number. However, a continuous approximation of this number may be convenient.

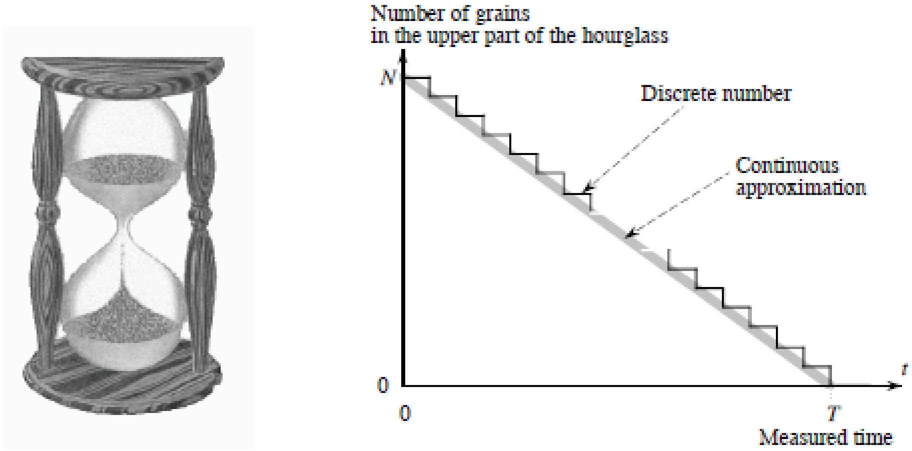


Fig. 23 – From discrete to continuous Petri Net [139]

3.4.3 Hybrid Petri Nets

Continuous PNs are particularly suitable for modelling flows: liquid flow or continuous production of a machine. However, a flow may be suddenly interrupted, as with closing a valve or machine breakdown, for example. This is equivalent to suddenly having another continuous PN. This situation can be modelled by a hybrid PN containing continuous places and transitions (C-places and C-transitions) and discrete places and transitions (D-places and D-transitions). In addition, in a hybrid PN, a discrete marking may be converted into a continuous marking and vice-versa. The marking of a C-place is represented by a real number, whose unit is called a mark, and the marking of a D-place is represented by dots, called tokens (or marks when a common word is useful). The classification of a system as 'hybrid' concerns the nature of the variables used when building system models. In this sense, for modelling purposes, systems could be classified as Discrete Event Dynamic Systems (DEDS), where state variables can be represented by integer numbers or logic variables, or as Continuous Variables Dynamic Systems (CVDS), where state variables can be represented by real numbers [140].

Hybrid systems [141] mix the characteristics of DEDS and CVDS, including both discrete and continuous variables. They can be the result of, for example, the integration of a continuous industrial process, such as those in the chemical and food industries, with a discrete supervisory system. Hybrid systems are systems whose modelling requires discrete as well as continuous variables. Time may be either continuous or discrete. Design processes have to consider continuous elements (hydraulics and system flexibility) and discrete ones (the state of a system is transformed between a start event and a termination one). The sequence of the operation is described by an operation process. The function of a system is likely to vary in the function of the operation that has to be performed. Let's consider the pendulum system as a hybrid system. The position of the pendulum has to be characterized by a real number expressing the position in measurement units. Consequently, continuous state variables are necessary. On the other hand, the sequence of a function is characterized by a starting point and a termination point, which are qualitative discrete states. As a consequence, a comprehensive model of a system functional-based model has to include discrete event aspects as well as continuous one.

It is usually very difficult to simultaneously deal with discrete and continuous variables. Their mathematical backgrounds are completely different, a recurrence versus differential equation. In a pendulum system, the most frequent functions encountered in the functional analysis is lifting (filling the hydraulic cylinder) and lowering (discharging the hydraulic cylinder). Starting and terminating this kind of operation are the discrete events. In this case the Petri Net method can be naturally used, since each position is represented as a token in place, which corresponds to a system state. In order to control that the pendulum has reached a state, the position of the pendulum has to be known at each time point. This can be achieved by measuring the amount of fluid in the actuator at each time point.

The volume of fluid in the actuator shown on **Fig. 24** is denoted by *V*, the input flow by *q_i* and the output flow by *q_o*.

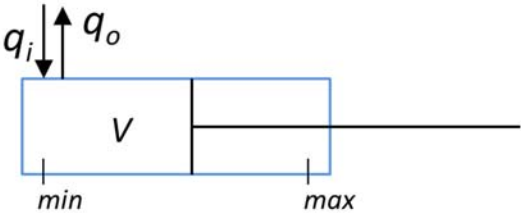


Fig. 24 – A simple actuator model

The modelling of physical systems can be carried out through differential equations. The obtained model is such that the system state is completely represented by continuous variables (real numbers) which are functions of time. Time is also continuous. The differential equation that describes the evolution of the volume V of a fluid that is contained in the cylinder is:

(11) $$\frac{\mathrm{dV}}{dt} = q_i - q_o$$

The volume of fluid in the cylinder can be compute by integrating this equation. If this integration is computed by a computer, the state variables, although continuous (real numbers) are only known at discrete time points: time is discrete. The model of the volume of fluid contained in the cylinder is:

(12) $$V(t_{n+1}) - \mathrm{V}(t_n) = [q_i(t_n) - q_o(t_n)](t_{n+1} - t_n)$$

In the first equation, V as a state variable and time are continuous. However, in the second equation, time is discrete but V is continuous, since it takes its values in the set of real numbers. In a discrete event model, time is discrete and state variables are discrete. They can be interpreted as logic propositions. Petri-nets are commonly used to represent systems by means of a discrete event model. A marked Petri net contains an integer number (positive or equal to zero) of marks or tokens which are distributed in places. This token distribution is the discrete state of the model. A transition firing denotes an event in the model. It is a significant time point at which the discrete state changes. The sequence of transition firings corresponds to the sequence of time points considered in the model. Time is therefore discrete. In a way it is a 'qualitative discrete' time because if the order of the event is specified, no quantified duration is specified. A Petri net is thus a typical discrete event model because the time and state variables are discrete.

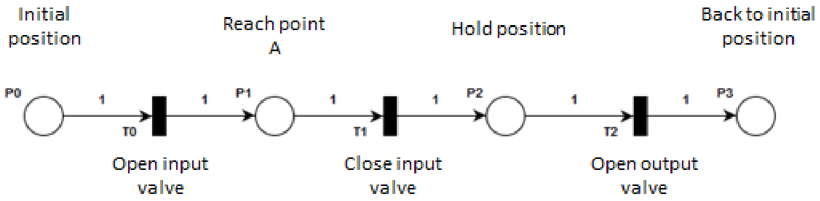


Fig. 25 – Pendulum simple sequence

Fig. 25 represents a possible discrete view of the pendulum activity. The initial position of the pendulum is at the lowest position. The actuator state is then at the minimum position and both input and output valves are closed. Before starting the sequence, volume V is basically empty. Then the input valve is in the state of open and the volume V starts to fill. After a certain amount of fluid has been injected into the cylinder, point A has been reached. In order to hold this position, the input valve has to be closed. State P2 is then reached. Finally, to get back to the initial position, the output valve is opened and the amount of fluid V is removed from the cylinder. Four configurations are present and **Fig. 25** represents the discrete states event using the Petri net approach. The only information given by the model concerning the volume is that V is empty, V is being filled, V is constant or V is being emptied. The time scale consists of the three time points that are the three events associated with the three transitions.

Continuous models describe the detailed dynamics when the discrete representation by the Petri net approach represents the sequence, but does not give information on the detailed variation of volume. Implicitly, it can be interpreted that T0 corresponds to V=0, at T1, V≠0 and T2 V=0. Therefore, continuous and discrete events are complementary.

In the two models, the value of V can be derived at the time point. In equation 2 it is explicit that the value of V between *tn* and *tn+1* can be derived by linear interpolation. On the other hand, if the value of V can be derived at the time points corresponding to the transition firings of the Petri net, it can be derived through the interpretation of the Petri net. If the label of place P1 was 'lifting for 10 seconds' it would be impossible to derive the exact position of the pendulum at the end of the operation. There are no possibilities to derive the exact value of V between two events. As a conclusion the approximation of equation 1 by means of equation 2 is not a way towards obtaining hybrid models.

There are different approaches to model hybrid systems: a continuous model extended with Boolean variables, timed Petri-nets and hybrid Petri-nets.

The first approach consists of adding Boolean variables to the differential equations:

$$\textbf{(13)} \qquad \frac{\mathrm{dV}}{dt} = b_i q_i - b_o q_o$$

Where b_i and b_o are Boolean variables. They are used to capture the dynamics of the volume during all the configurations. During the lifting phase, $b_i = 1$ and $b_o = 0$. However, during the initial and final state, $b_i = 0$ and $b_o = 0$. It basically represents the state of the valve, open or closed. It can be noticed that if the dynamic of the volume V is represented, the sequence of the operation is not modelled.

The second approach consists of timed Petri-nets, which is a typical way to take into account continuous phenomena in a discrete model by representing their duration. These durations are continuous values and as a consequence, a kind of hybrid model is obtained. With this approach, the system can be represented by **Fig. 26**. The lifting operation duration are represented by the duration associated with transition.

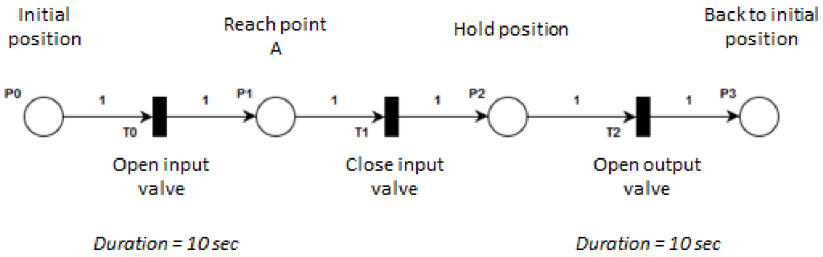


Fig. 26 – Timed Petri Net model

In this model, the discrete part is represented by places and the transition of the Petri-net represents the sequence. The unique continuous variable is the time, which entails that all the continuous variables of interest have to be simple expressions of time. If we consider the input flow as constant, the volume V can be computed at any time and therefore also the position of the pendulum. This approach requires a good evaluation of the durations of each state and has to be independent of the past evolution of the system. For instance, in the case of the pendulum, the force provided by the cylinder is dependant of the position of the mass, in other words it is dependent of the angular position of the pendulum. Therefore, the use of timed Petri-nets is not appropriate for this type of system.

The third approach consists of the Hybrid Petri-net which unifies the representation of continuous variables represented as continuous place token counts (real numbers) and discrete ones represented as discrete place token counts (integers). A continuous place is represented by a double circle and a continuous transition by a double bar. A continuous place is said to be fed if there is at least one of its input continuous transitions which is being fired. A continuous transition is strongly enabled if the token count of all its input places is strictly positive. A continuous transition is said to be weakly enabled if at least one of its input places is fed and the token counts of the others are strictly positive. A continuous transition is fired with a speed v(t). That means between *t* and *t+dt* a quantity *v(t).dt* of a token is removed from its continuous input places and is added to the token count of its continuous output places. In a cylinder, the continuous places represent the cylinder and the continuous transitions the flow of fluid.

The modelling of an actuator is represented in **Fig. 27**. The firing speed of the transition T_3 represents the input flow q_i and the firing speed of the transition T_4 represents the output flow q_o. The number of tokens in the continuous place P_3 represents the volume V of fluid inside the actuator. The process is represented with discrete places and transitions of the Petri Net: between the firing of T_1 and T_2, the actuator is being filled. The interaction between the discrete part and the continuous part is denoted by the self-loop between P_2 and T_3. When there is a token count in P_2, the firing speed of T_3 is q_i, otherwise T_3 is not enabled and cannot be fired. The interaction of the continuous part on the discrete part is denoted by the self-loop between P_3 and T_2. When the token count in P_3 is $V=V_{max}$, then T_2 is fired, and the token in P_2 is removed. The input valve is closed.

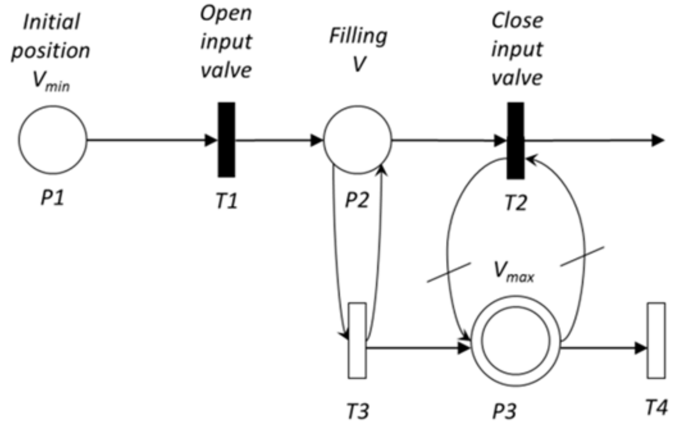
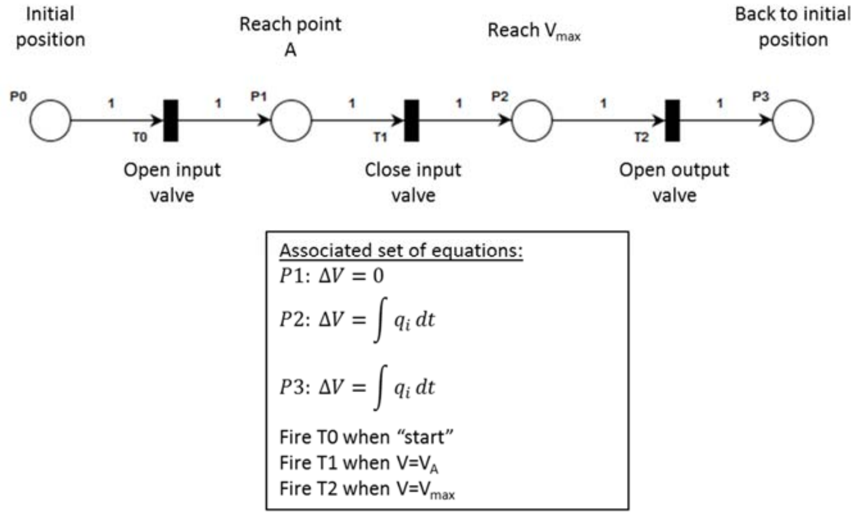


Fig. 27 – Hybrid Petri Net model of a hydraulic actuator

This model can only describe real values (continuous variable) which are non-negative; moreover, a continuous place represents only one continuous variable. The unique way of describing interactions between the continuous part and the discrete one is by means of self-loops.

Combining differential equations and Petri nets is another approach to simultaneously dealing with discrete and continuous models (**Fig. 28**). The only difference is to represent continuous places and transitions by differential equations instead of self-loop between the discrete and continuous part. A token put into a place starts the integration of the corresponding equation. Therefore, the interaction between the two models is achieved. Each threshold is associated with a transition which is an output transition of the marked place. When the threshold is crossed, it means that the corresponding event is occurring and the attached transition is fired. The new marking is computed and the integration of a new system starts. In the example of the cylinder, the systems attached to places P2 and P3 are identical. However, the thresholds which have to be monitored differ. In the first case, $V=V_A$ and transition T_1 is fired. In the second case $V=V_{max}$ and transition T_3 is fired.



Associated set of equations:
$P1\colon \Delta V = 0$
$P2\colon \Delta V = \int q_i \, dt$
$P3\colon \Delta V = \int q_i \, dt$
Fire T0 when "start"
Fire T1 when $V=V_A$
Fire T2 when $V=V_{max}$

Fig. 28 – Differential equations associated with Petri Net

Therefore, the Petri Net supervises the system of differential-algebraic equations whose structure changes each time a transition is fired. It can also be said that the system of equations controls the Petri net evolution by enforcing the firing of its transitions. In this model the discrete part is represented by the Petri net and the continuous part by the set of differential equations.

3.4.4 Petri Net-based object-oriented approach

Villani and colleagues [142] have developed an approach for modelling hybrid productive systems based on the Petri Net. The Petri Net represents the discrete part; the continuous part is represented through differential equations and an object-oriented paradigm to deal with the complexity of the system. Its implementation uses Unified Modelling Language (UML) in order to support the description of different aspects and identify different hybrid characteristics of the system.

Basically, the approach consists of considering that the model of a system is composed of a set of objects that are organized in classes. A class is the description of a set of objects that share the same attributes (data), operations, relations and semantics.

Ni is a finite set of marked sub-nets where C is the number/name of classes that models the system dynamics: N_i= (N_{1_i}, N_{2_i}, N_{3_i},… N_{C_i}).

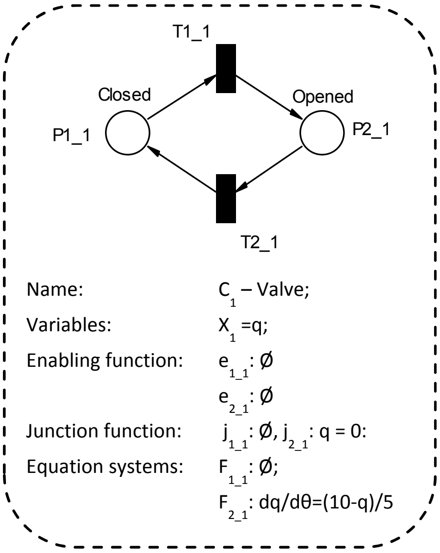
A marked subnet is composed as follow: $N_i =< C_i, R_i, A_i, M_{0\_i} >$, where:

- C_i is the name of the class.
- R_i is a Petri net defined by <P_i, T_i, Pre_i, Pos_i>, where:
  - P_i = [p_{1_i}, p_{2_i}, …, p_{m_i}] is a finite set of places
  - T_i= [t_{1_i}, t_{2_i},…,t_{n_i}] is a finite state of transitions
  - $P_i \cap T_i = \emptyset,\ P_i \cup T_i \neq \emptyset,$
  - $Pre_i: P_i \times T_i \rightarrow (0,1)$
  - $Pos_i: P_i \times T_i \rightarrow (0,1)$
- A_i is the inscription of the Ni: $\mathrm{A_i =< X_i, X_{pk\_i}, e_{k\_i}, j_{k_i}, F_{k\_i} >}$, where:
  - X_i is a set of formal variables
  - X_{pk_i} is a subset of X_i associated with each places p_{k_i}.
  - E_{k_i} is an enabling function that is associated with each transition t_{k_i}. The input parameters of e_{k_i} are variables of X_i.
  - J_{k_i} is a junction function that is associated with each transition t_{k_i}. It defines the value of X_i after the firing of t_{k_i}: $X_i(\theta^+) = j_{k\_i}(X_i(\theta^-))$ where $\theta^+$and θ^- are the time immediately after and before the firing of t_{k_i}.
  - F_{k_i} is a differential equation system that is associated with each place p_{k_i}. It has X_{pk_i} as variables and X_i as input parameters.

(14)
$$F_{k\_i}(\dot{X}_{pk\_i}, X_i) = \begin{bmatrix} f_{k\_i1}(\dot{X}_{pk\_i}, X_i) = 0 \\ \vdots \\ f_{k\_in}(\dot{X}_{pk\_i}, X_i) = 0 \end{bmatrix}$$

- M_{0_i} is the initial marking of the sub-net.

For the previous example, the cylinder consists of 2 valves (input and output) and a tank that is filled or unfilled. The 2 valves are similar; however, they are independently operated. Therefore, they are part of the same class C_1 (**Fig. 29**). The tank is part of a second class C_2.



Name: C_1 – Valve;

Variables: X_1 =q;

Enabling function: e_{1_1}: Ø

e_{2_1}: Ø

Junction function: j_{1_1}: Ø, j_{2_1}: q = 0:

Equation systems: F_{1_1}: Ø;

F_{2_1}: dq/dθ=(10-q)/5

Fig. 29 – Example of object-oriented differential predicate transition Petri Net

The discrete state of the Class C_1 has only two states, '*Opened*' or '*Closed*'. Let's name the input valve C_{1_1} and the output valve C_{1_2}. These classes model the behaviour of a system; 'q' is the current flow through the valve.

4 MODELLING OF THE RELIABILITY-BASED VERIFICATION METHOD

The current practices on verification and validation as well as the state of the art using digital mock-ups within the entire lifecycle have been presented in the previous chapter. Based on this literature survey, this chapter suggests modelling and implementing a verification-driven design process for the design of complex engineering systems, using a reliability-based evaluation approach to support the decision-making process. The first section of this chapter introduces system functional analysis and representation at different phases of the design. The second section uses a simple example to illustrate the different functional representation approaches. Section 4.3 focuses on functional and dysfunctional analysis of the example. Finally, Section 4.4 illustrates an overview of the verification-driven design process that will be applied to proper case studies in Chapters 5 and 6.

4.1 Functional analysis and hierarchical design

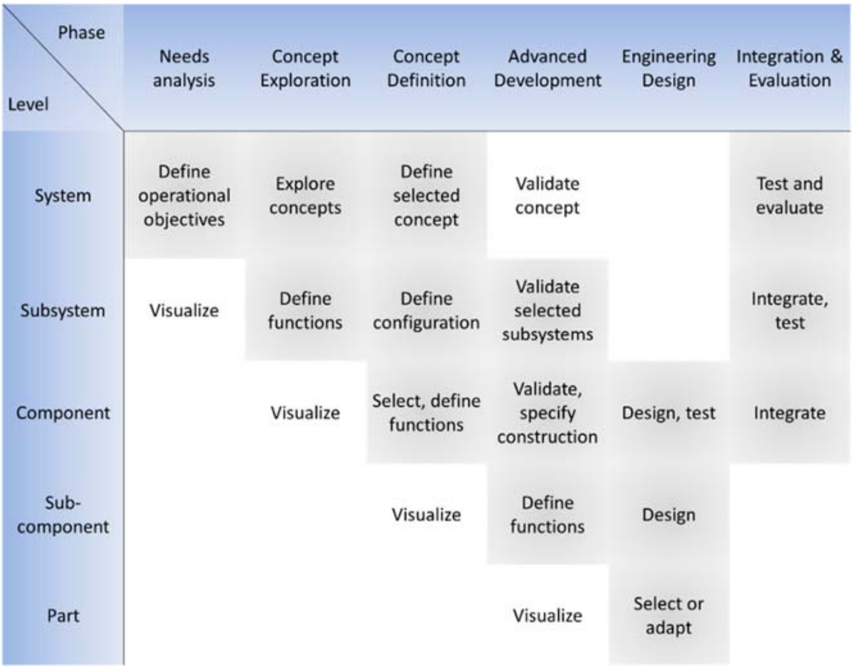
The proposed method employed for defining and evaluating the reliability prediction follows the V-model of the systems engineering approach and the system materialization approach. Starting from the requirement definition and specifications of the system, it continues to the Functional Analysis (FA) of the system, where the system architecture is defined. It is then completed by a Dysfunctional Analysis (DA) that uses different tools such as FMEA and Petri networks. The different tools that are used to perform this study are FA, FMEA and DA. As a result, it gives the failure modes of the components and related causes.

4.1.1 System materialization

The development of a new system can be seen as a progressive ‘materialization’ process from a need to an assemblage of actual components cooperating to perform a set of complex functions to fulfil that need. To illustrate this process: **Table 2** traces the growth of materialisation throughout the phases of the project life cycle. The rows represent the level of system subdivision, from the System itself to the top of the Part level at the bottom. Beside the columns are successive phases of the system lifecycle. The entries are primary activities at each system level and phase, as well as their degree of materialization.

The process aims at materializing the system in a top-down approach, starting from the system itself down to each single component and parts of the system. By analysing each row, from the sub-systems to the part level, shows that the process starts with visualisation and then proceeds to function definition (functional design – what it must do), and finally the implementation (detailed design – how it will do it).

Table 2 –System Materialization matrix through the system design process [143]



Phase Level	Needs analysis	Concept Exploration	Concept Definition	Advanced Development	Engineering Design	Integration & Evaluation
System	Define operational objectives	Explore concepts	Define selected concept	Validate concept		Test and evaluate
Subsystem	Visualize	Define functions	Define configuration	Validate selected subsystems		Integrate, test
Component		Visualize	Select, define functions	Validate, specify construction	Design, test	Integrate
Sub-component			Visualize	Define functions	Design	
Part				Visualize	Select or adapt	

It is important to notice that while the detailed design of the system is not completed until near the end of its development, its general characteristics must be visualized very early in the process. This can be understood by the fact that the selection of the specific system concept requires a realistic estimate of the cost to develop and produce it, which requires a visualisation of its general physical implementation as well as its functionality. In fact, it is essential to have a general vision of the physical embodiment of the system functions during even the earliest investigations of technical feasibility.

At any point of the cycle, the system is seen as the current system model. During the development stage the system model includes only the system functional model made with descriptive materials, diagrams, tables of parameters, together with a combination of simulation used to analyse the relationships between system-level performance and the specific features and capabilities of individual system elements. During the advanced phase of the product development, this model is augmented by gradual addition of hardware and software designs from each level of the system structure, leading to a complete engineering model.

4.1.2 Hierarchical structure

The simplest way to represent the architecture of a system is probably a hierarchical tree structure. With this representation, a system is decomposed into sub-systems and assemblies, up to the component level. **Fig. 30** gives a representation of a tree structure:

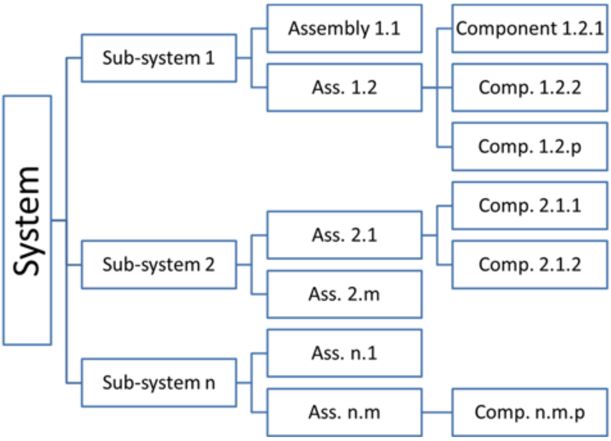


Fig. 30 – Example of a hierarchical tree structure

This representation enables us to look at different levels of abstraction, and helps in visualising the organisation of the system and the degree of relationship between sub-systems, assemblies and components.

4.1.3 Functional representation

The functional definition includes functional analysis and allocation. The typical activities include:

- Translating requirements (why) into functions (actions, tasks) that the system must accomplish (what).
- Partitioning (allocating) requirements into functional building blocks.
- Defining interactions among functional elements to lay a basis for their organization into a modular configuration.

To represent the functional features of a system, the functional decomposition block diagram is used to represent the architecture of all products' functions. These function structures include all the material, energy and information flows as arrows between the functional blocks (**Fig. 31**).

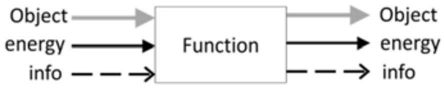
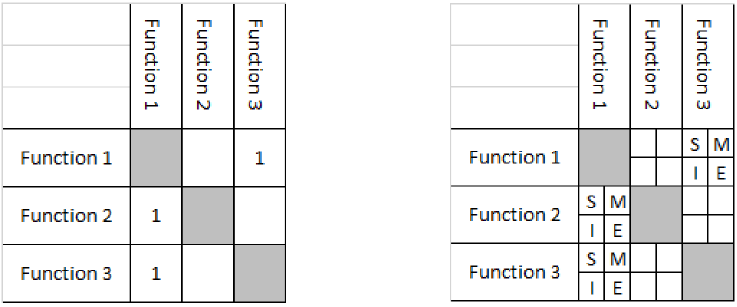


Fig. 31 – Single block function diagram with basic work flow types [144]

The design structure matrix (DSM) is another way to represent the architecture of a system [145]. The functions are presented as row and column headers of the matrix. The connection mark 1 in **Fig. 32** indicates that the function on the row depends on the function on the column. For instance, the function 2 and 3 depends on function 1 and function 1 depends on function 3. These marks can also be divided into spatial (S), Material (M), information (I) and Energy (E). The rows and columns can also be components, tasks, team members, constraints etc.



	Function 1	Function 2	Function 3
Function 1	▨		1
Function 2	1	▨	
Function 3	1		▨

	Function 1	Function 2	Function 3
Function 1	▨		S M I E
Function 2	S M I E	▨	
Function 3	S M I E		▨

Fig. 32 – Design Structure Matrix (DSM)

Another method was developed to include the functions or components of a product or system and their interconnections. The object-process methodology (OPM) was developed in order to include both aspects into the same model [146]. Objects represent sub-systems and processes represent system functions. In the graph (**Fig. 33**), objects are represented as rectangles and processes with ellipses. The links (or connector) between objects and processes use multiple symbols to indicate the action of an object. For instance, a connector with a black circle at the process end indicates that an object performs a process. However, a white circle indicates that the object is part of the process but not performing the action. In addition, other information can be implemented in such a representation, such as states (diamond shape), effect (arrows) and aggregations (•), as represented in the OPM flowchart.

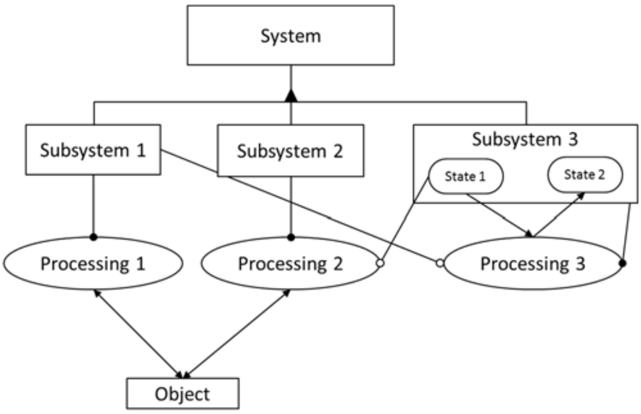


Fig. 33 – Object-process diagram

4.2 Pendulum system as an example

In this section we use a simple case study to illustrate the application of the method. The pendulum system is a simple mechanism that consists of mainly 4 parts: a support, an arm, a mass and an actuator (See **Fig. 34**). The mechanism's principles consist of 3 main simple functions: lifting the mass, lowering the mass and holding the mass.

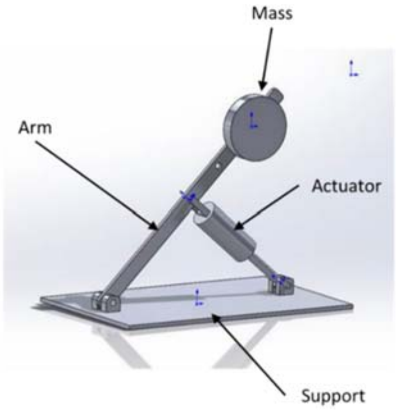


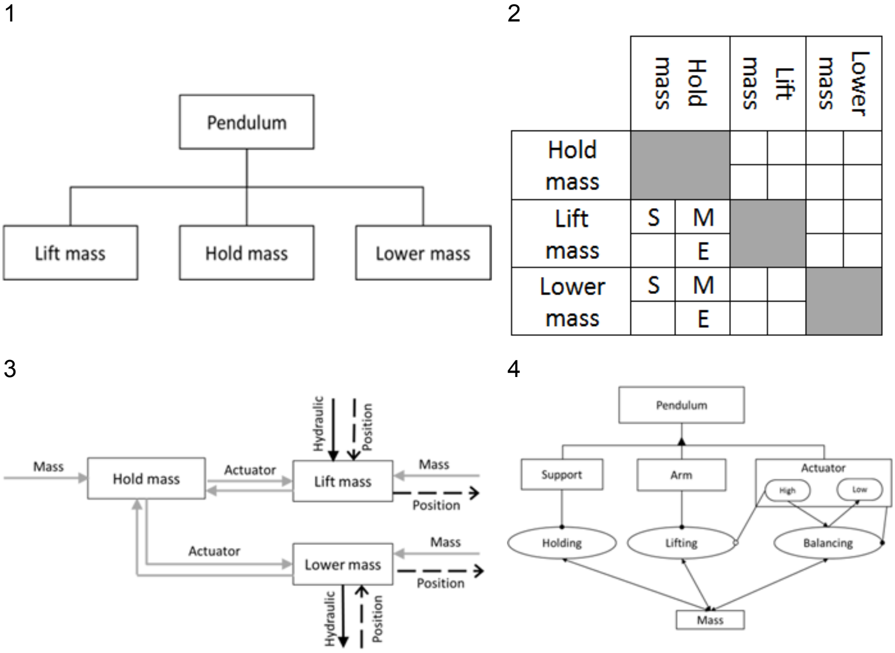
Fig. 34 – Virtual model of a simple Pendulum mechanism

The pendulum model can be represented by various function analysis charts. Four common functional diagrams can be used to represent the pendulum system:

- Hierarchical functional structure (1)
- Design structure matrix (2)
- Single block diagram (3)
- Object-process methodology (4)

Nevertheless, the purpose of this brief comparison is not to define the most suitable representation for a system, but rather to visualise the differences between the four common forms of structural functional representations. It will also later be useful for the different phases of the design process for verification and validation purposes.

Fig. 35 illustrates the pendulum system through its three main functions using the four functional representations introduced previously:



	Hold mass		Lift mass		Lower mass	
Hold mass						
Lift mass	S	M				
		E				
Lower mass	S	M				
		E				

Fig. 35 – Pendulum system represented through four common functional diagrams.

The hierarchical functional structure (1) is limited in the amount of information delivered by this kind of chart. To make it a bit more detailed, the system-level tree structure can be added to the functional diagram; however, it will remain very limited in the level of information.

The DSM representation (2) shows the function structure model and the interactions between the functions. For instance, the function ‘lift mass’ is dependent to the function ‘hold mass’ by spatial, material and energy parameters. This kind of representation gives information on the level of dependency and what type it is. One important aspect is that the inputs and outputs of the system are not shown in this kind of representation, however it is a very modular representation, rows and columns can be easily reorganised to create functional modules.

The block function diagram (3) includes the system's energy input and output (hydraulic), together with position information data. Moreover, it shows the relation between energy and object interactions with the function and gives the type of relation (one or two-way).

The Object Process Methodology (OPM) (4) enables simultaneous function representation and system components. In some cases, environmental constraints and system users can be added to the representation together with their related interaction with the object. The dynamic state of the system is also represented, such as the position of the actuator: high or low. So far, this kind of representation provides a more complete description than the three previous representations.

4.3 Functional and dysfunctional analysis applied to the pendulum

The functional analysis previously described for the pendulum model does not bring information on the potential failures in the developed system. A dysfunctional analysis aims to bring information that specifies the different states of the system and to determine the principle causes of failure as well as to understand the relation between components and failures. The state notion is fundamental in the verification and validation purpose, since a system or sub-system is validated regarding a particular state, although it can end up in a failure mode for a slightly different state. Among the methods of dysfunctional analysis, we refer to Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) described in Chapter 3. As a graphical representation tool of dysfunctional analysis, the Petri network is commonly used. They are powerful mathematical and graphical tools for performing discrete-event simulations (DES).

4.3.1 Failure Mode Effect Analysis (FMEA)

The FMEA is usually used to collect information on the developed system in order to improve the reliability, quality and safety of a system, and reduce the potential risks of the product. It is a well-defined process commonly used in the late phase of the design process, when the system is already in advanced development or even in the engineering phase. In this thesis, the FMEA is used to list and analyse failure modes in order to build the dysfunctional model of the system. Therefore, the aim of using FMEA in this study is not to compute the Risk Priority Number (RPN) of the system design, but simple to list and analyse system failures, causes and effects. However, in the later phase of the process, RPN can be included in the evaluation method as a decision-making criterion.

By using the block function diagram previously established for the pendulum system (**Fig. 36**), it is quite straight forward to determine the failure causes of the 3 main functions:

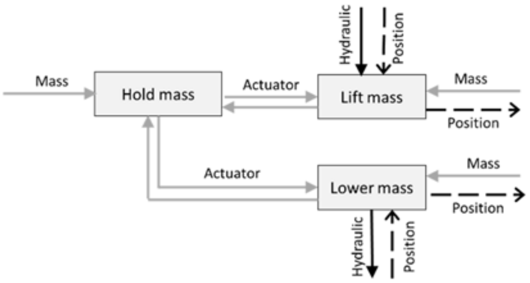


Fig. 36 – Block function diagram of the pendulum system

From this diagram, it is possible to list the FMEA of the pendulum. For instance, the *lift mass* function is connected with 4 arrows as inputs and 2 arrows as outputs. This means that the failure of the *lift mass* function is caused by the mass object, the position information, the hydraulic (as energy source) or the actuator object. The **Table 3** lists the function and related failure modes' causes and effects of the pendulum system, based on the block function diagram representation.

Table 3 – FMEA applied to the pendulum concept

Main functions	Failure modes	Causes	Effects
Lift the mass	The mass is not moving	The actuator is failing	The mass remains down
		The hydraulic source is failing	The mass remains down
		The mass is too heavy	The mass remains down
		Wrong position information	The mass remains down
Hold the mass	The mass is still moving	The actuator is failing	The mass is falling down
		No damping	The system is vibrating
		The mass is too heavy	The mass is falling down
Lower the mass	The mass is not moving	The actuator is failing	The mass is already down
		The hydraulic source if failing	The mass is already down
		The mass is too heavy The actuator is not enough powerful	The mass is already down
		Wrong position indication	The mass is already down

In **Fig. 36**, for the system function *Lift the mass*, one failure mode is considered 'the mass is not moving' and the cause of this failure can have 4 different causes. The failure can happen because of the actuator, because of the hydraulic power source, because of the mass or because of wrong sensor information. One of these failures will lead to the effect that the mass will remain down and thus the system is not working as planned.

The same approach is considered for the two other main functions of the pendulum: system *hold the mass* and *lower the mass*. Identifying most of the failure causes, from the early phase of the design, is of primary importance when designing a system.

4.3.2 Functional Petri Net representation of the Pendulum

The discrete aspect of the Petri-Net model allows for modelling the functional sequence of the system (**Fig. 37**). Each place, represented by a circle, indicates the state of the system. The token represents the current state of the system. In this example, the sequence consists of 4 phases: *P0: Initial position*, *P1: Lifting phase*, *P2: Holding phase* and *P3: Lowering phase*. Each state of the system is separated by a rectangle, called transition, which represents the action that needs to be performed to provoke the change of the system state. Rectangles are a timed transition, which means that a firing rate can be applied to each transition. In this example, the rate of the transition represents the time needed before performing the action (opening or closing the valve) that the transition represents, before reaching the next state. For instance, if Lifting the mass is considered twice as long as lowering the mass, then the rate of the transition '*T1: Close input valve*' will be two times the rate of the transition '*T3: Close all valves*'.

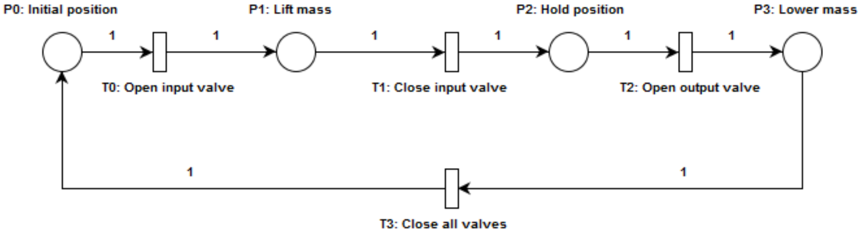


Fig. 37 – Functional Petri Net model of the Pendulum sequence

The transition delay for a system sequence level represents the solicitation time of the system (*working time*). This transition follows a functional distribution associated with the system.

For each transition of the system sequence, a uniform distribution is used, in this case (**Fig. 38**) to model the distribution of the different phases of the functional sequence. For instance, the transition between the initial position phase and the lifting phase is randomly fired between 1 and 2 hours, while the firing time between the Lifting phase and holding position is happening between 0 and 1 hour time.

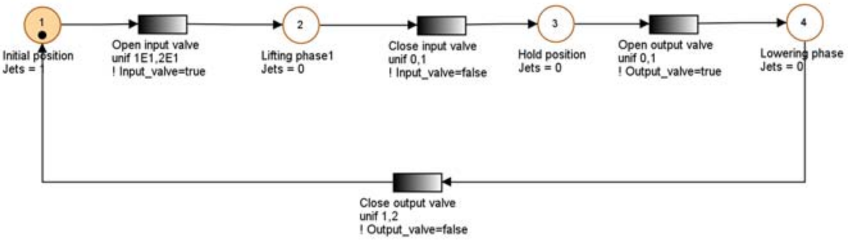


Fig. 38 – Functional Petri Net model of the system sequence level under GRIF Moca

The sequence level diagram drives the simulation, and 2 variables have been implemented into the transitions. *Input_valve* and *Output_valve* are two Booleans variables. They are initially defined as false, which means that before the system starts, the input and output valves are closed. When the *Open input valve* transition is fired, then the variable *Input_valve* is set as true, meaning that the valve is in an opened configuration, and thus the system goes to the *Lifting phase* state. When the transition *Close input valve* is fired, the *Input_valve* variable is set as false, meaning that the input valve is closed. The transitions *Open output valve* and *Close output valve* are in the same way linked to the variable *Output_valve*.

The sequence of the operation consists of working phases (*lifting* and *lowering* phases) and standby phases (*initial position* and *holding* phases). If we consider the failure rate of the valves (*input* and *output* valves) the failure distribution may be different in the case of the working phase or the standby phase. The same philosophy could be applied to the mechanical failure of the component. The distribution of the mechanical failure in a lifting phase can be different than in the lowering phase, and both obviously different than during a standby phase. Now let's concentrate on the component level of the system (*input* and *output* valves) modelled by the Petri-net shown in **Fig. 39**.

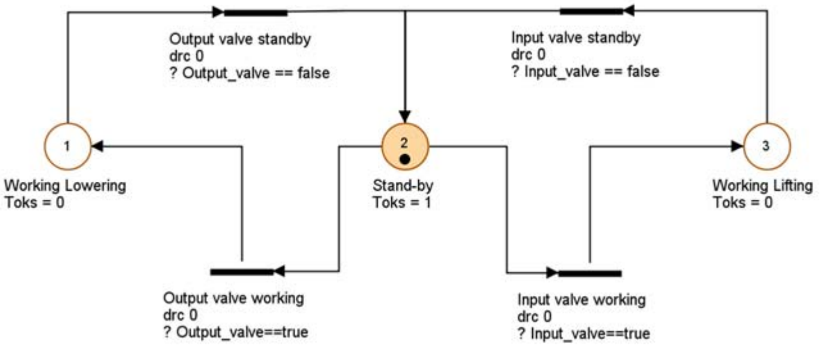


Fig. 39 – Functional Petri Net model of the component level

Each valve has only 2 modes: *opened* and *closed*. When the input valve is *opened*, the output valve has to be *closed* and vice versa. The component level model is driven by the enabling functions implemented in each component transitions. When one of the variables *Input_valve* or *Output_valve* is set as *true*, the transition is instantly fired following a Dirac distribution, basically a timeless transition.

4.3.3 Dysfunctional Petri Net representation

Each valve has 2 failure modes: *Seizing* or *Leaking*. When one of the failure modes happens, the whole system is considered to be not working. The Petri net model of the input and output valves presented in **Fig. 40**, shows the association of a Weibull distribution to the failure modes of the valves.

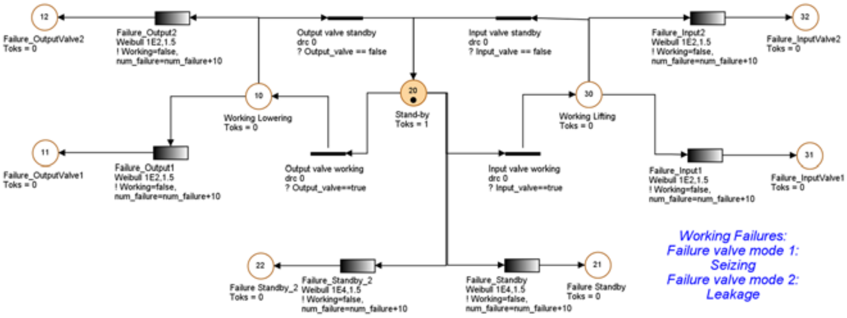


Fig. 40 – Dysfunctional Petri Net model of the component level

In this model the two valves are combined together in the *standby mode* (*place 20*) and their failure distribution have higher parameters, since it is considered that in a *standby mode* the failure probability of one of the valves is lower than in the *working mode*. Then the model consists of two working phases, the *working lifting* phase, represented by *place 30* that consists of actuating the input valve, and the *working lowering* phase, represented by *place 10*, which consists of actuating the output valve. Each valve has 2 failure modes:

- Valve Failure mode 1: Seizing
- Valve Failure mode 2: Leaking

Therefore, different parameters can be applied to each failure mode. However, in this study we do not focus on the type of failure distribution probability of the valves; therefore, in the model shown in **Fig. 40**, each failure mode has the same probability of failure that follows a Weibull distribution, with the following standard parameters: *η=100; β=1.5*.

Place 20 is the standby mode of the valves. The transitions between *place 20* and *places 10* and *30*, which correspond to actuating of the input or output valves, each transition follows a Dirac distribution with a delay null, since the sequence of the system (shown in **Fig. 38)** already takes into account the delay between each phase.

4.3.4 Fault Tree analysis

In order to ease the modelling process of the system towards a functional Petri Net model, the use of fault tree analysis may be useful for understanding the relation between components and failures. In this simple case study, it has been considered that each valve has two failure types as previously described, *seizing* and *leaking*. Therefore, the system enters into a failure mode when the valve is leaking OR seizing. In the case of a doubled valve system, *valve_1* AND *valve_2* need to be in failure mode to cause the failure of the entire system. The system behaviour can be represented first as a Fault Tree Analysis model before being transformed to a stochastic Petri Net model, especially in the case of complex systems.

4.3.5 Reliability of the pendulum using the Petri Net model

In order to visualise the result of the failure probability of the entire system, a Boolean variable *working* has been implemented. The initial value of the variable is set as *true* and in the event of any failure event, the variable *working* is changed to *false*. The value of the variable *working* over time is shown in **Fig. 41**.

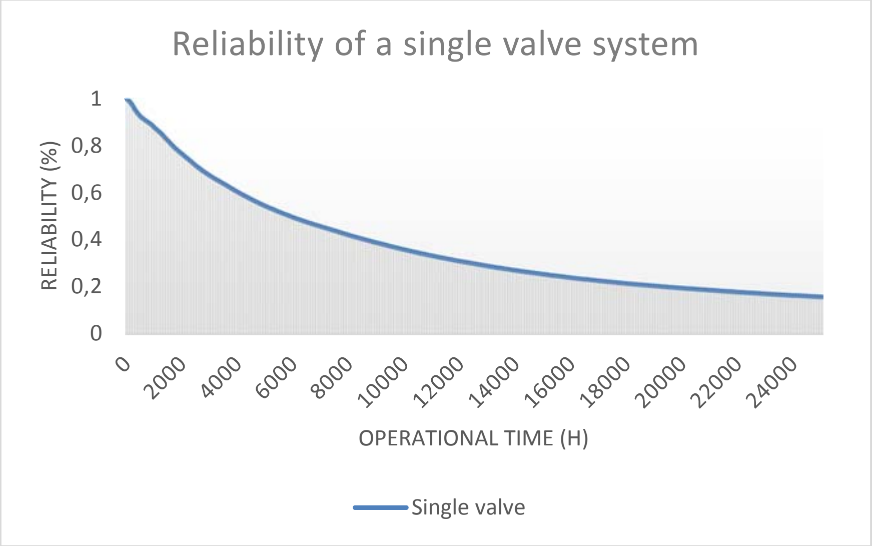


Fig. 41 – Reliability prediction of a single valve system

Now let's consider the same pendulum system but with a redundant configuration of valves. The output valve is doubled as well as the input valve. The Petri Net models of the set of output valves is presented in **Fig. 42** and the set of input valves is presented in **Fig. 43.** In this case, it is supposed that in order to have an overall failure of the system both of the input valves or both of the output valves have to fail at the same time. On the other hand, this means that if one input valve and/or one output valve fails, the system is still considered to be in a working mode.

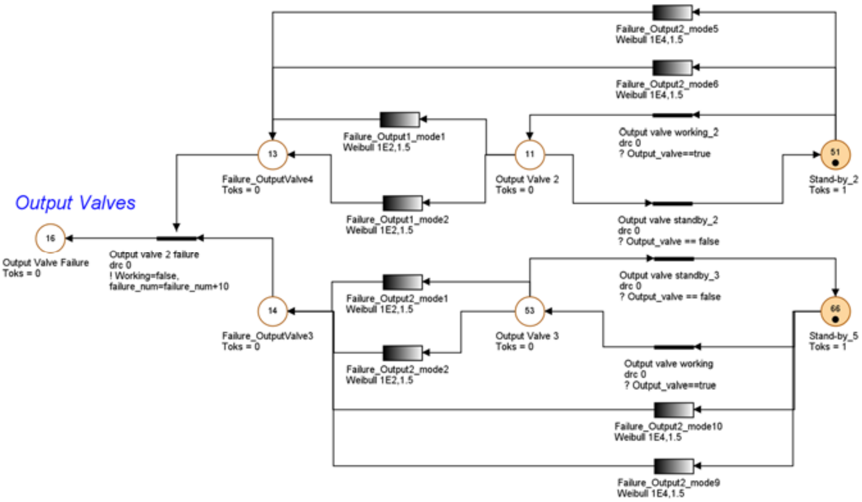


Fig. 42 – Dysfunctional Petri Net model of a doubled output valves system

The **Fig. 42** consists of two standby mode represented by *place 51* and *place 66* respectively connected to *place 11* and *place 53* that correspond to the working state of the valves. Each of the standby modes are connected to two failure modes as well as the two working mode places (seizing and leakage). Parameters have been kept similar to the single valve system. The output valve system enters in a failure mode only if both of the output valves fail simultaneously, which means that a token has to be present in *place 13* and in *place 14*.

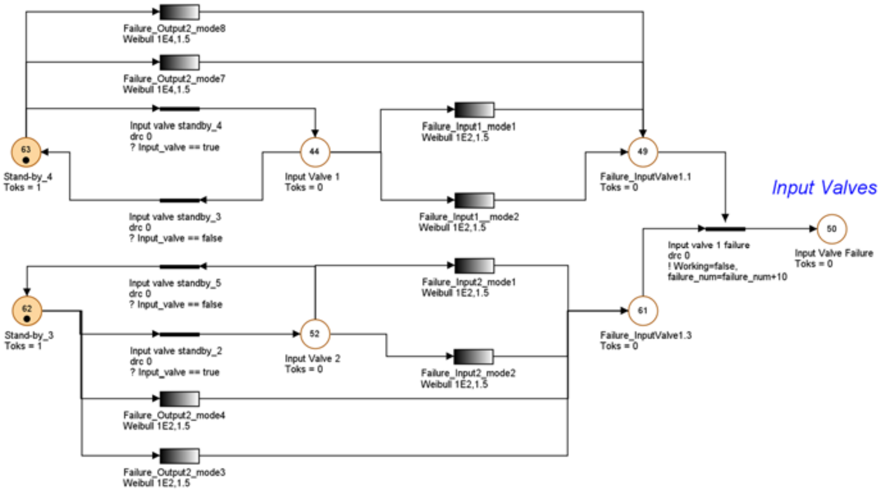


Fig. 43 – Dysfunctional Petri-net model of a doubled input valves system

The **Fig. 43** represents the same redundant valve Petri Net model but applied to the input valves. Transition parameters are similar to the single valve system as for the output valves model. To enter into a failure mode, both of the output valves have to fail simultaneously, which means that a token has to be located in each of the *places 41* and *61*.

Fig. 44 compare the previous reliability of a single valve system that was presented in **Fig. 41** with the reliability of the redundant valves system. The system enters into failure mode only when the two input or output valves fail simultaneously.

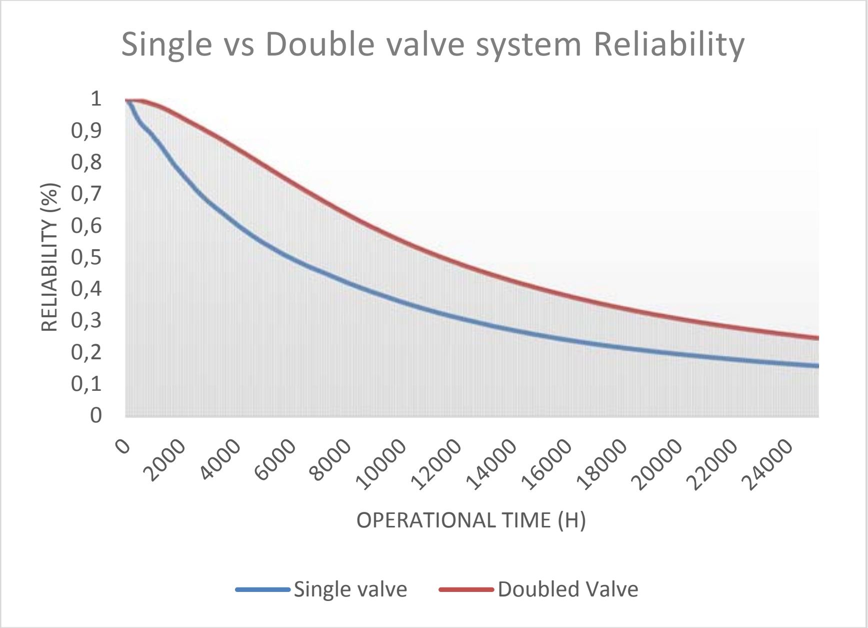


Fig. 44 – Reliability comparison between single and double set of valves

The graph shows that over the entire lifecycle, the redundant valves system provides a reliability up to +25% than the single valve system after 6 000 h of operations. The difference decreases to about +10% of extra reliability at the end of the lifetime. Preventive as well as corrective maintenance are not taken into account in these results.

4.3.6 Common failure modes and environmental factors

Most of the failure modes are similar from one system to another, and therefore the failure types can be categorised. In this case we consider only mechanical failures mode, therefore it applies basically to metallic components. For instance, composite materials or plastic components failures are not in the scope of this study.

Mechanical failure modes can be categorized by one of the following mechanical failure processes [147]:

- Distortion
- Fatigue and Fracture
- Wear
- Corrosion

Much research has been carried out in order to test the evolution of fatigue on mechanical components [148] and how to represent system fatigue behaviour [149, 150]. In this thesis, human errors are not taken into account, such as the three main human errors: errors of omission, errors of commission, and operational errors [151]

Several parameters can amplify the occurrence of the previously listed failure processes. For instance, environmental factors may affect mechanical component failure distributions:

- Temperature is a major factor affecting reliability. The effect of temperature combined with load and thus stress on components [152, 153]
- Dust also affects the lifetime of a mechanism, due to dust accumulation it may lead to blockage of mechanisms [154, 155]
- Radiation has an effect on component reliability, since it affects the material structure of the mechanical component [156], the tensile strength, ductility and fracture toughness. Proper materials have to be used in order to reduce the effect of radiation on mechanisms [157-159].

In the case of electronic components, the main environmental factor that affects reliability is the temperature. The reliability of the component depends either on temperature gradients, temperature cycle magnitude or the rate of change of temperature [160, 161]. Radiation also may affect the reliability of electronic components, such as connectors and terminals [162].

4.4 Verification-based design process framework

Fig. 45 represents the verification-based design framework of the method applied to any system. An estimation of the operation time of the operation is used as an input for the discrete event dynamic system in order to represent the operational time of the system. Environmental factors that may affect the system’s lifetime behaviour are also important inputs. The system functional stochastic Petri Net is then modelled for each of the concepts that are analysed as well as their respective dysfunctional Petri Net model. A failure mode and effect analysis (FMEA) has to be carried out and failure distribution data need to be collected for each failure mode. This approach is used as an iterative process all along the system design process and constantly evolves according to the system-level of design.

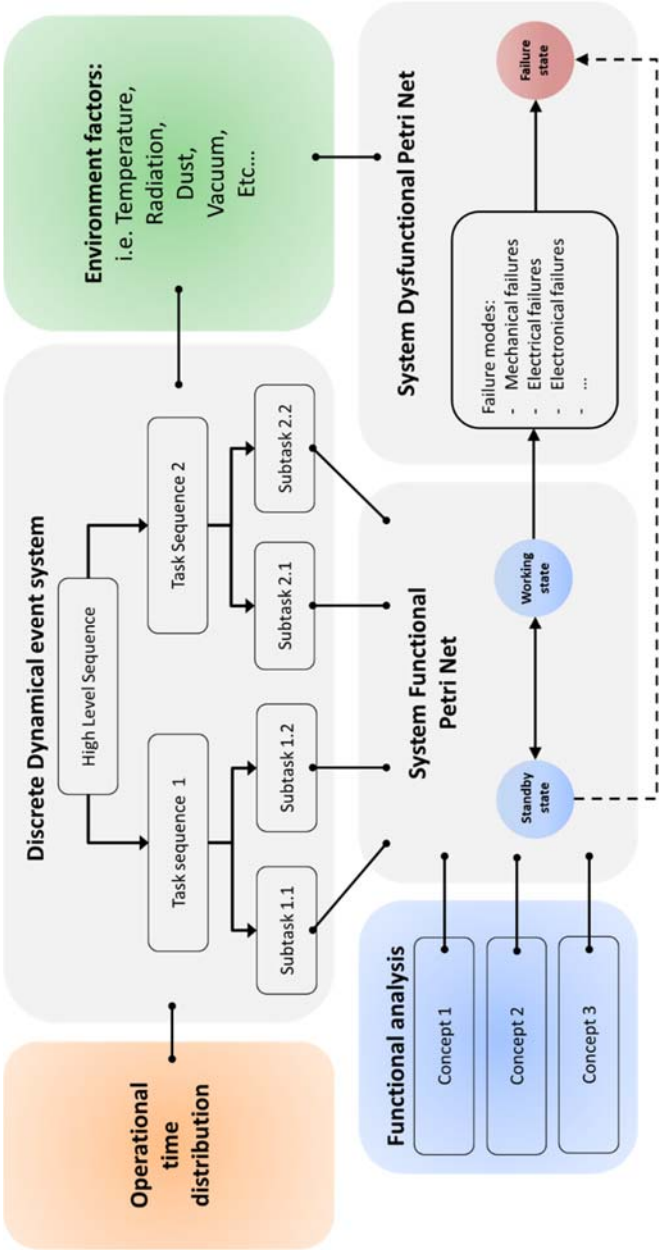


Fig. 45 – Verification-based design process framework

5 CASE STUDY 1: RELIABILITY-BASED METHOD IN THE DESIGN PROCESS

This chapter introduces the first case study that is used to validate the theoretical hypothesis described in the previous chapters and to demonstrate also the application of the method. In this chapter, the developed process is used to design an innovative remote handling system for the maintenance of the Divertor area of a new tokamak generation fusion reactor called DEMO. This chapter starts by describing the environment of the project, mainly with a focus on nuclear fusion activities. The second part of the chapter is dedicated to the project itself and the main specifications in terms of designing a complex system for the maintenance of the tokamak. Section 5.3 describes the case study on which the method developed in this thesis will be applied. The fourth part focuses on the initial requirements and system breakdown structure that are used as inputs in the developed method. The fifth part is focused on the modularity and iterative aspect of the method. The sixth and seventh sections cover the discrete dynamical system representation and the respective functional analysis of the developed system and the development of the respective discrete event dynamic system. The functional stochastic Petri Net model of the different design concepts are presented as well as their respective dysfunctional models and the evaluation of the different concept designs are described in Sections 5.8. In Section 5.9, environment factors are implemented for the case study, while the results of this chapter are discussed in the last part.

The main objective of this chapter is to clearly define the requirements of the system to be developed as well as the constraints that are imposed by the environment, and then to build the functional and dysfunctional models of the systems using a Petri-net approach in order to be able to perform the comparison of the different design options. This case study mainly focuses on mechanical/mechatronic system-development-oriented remote handling for a fusion reactor, however it can be considered as a general mechatronic system if we omit to take into account certain constraints, such as high temperature and radiation.

The objectives of using these case studies are first to apply the suggested method on the development of a real and fairly complex system that is part of a large scale project. Experience gained throughout the development of this system can be reused to improve the design processes of such kinds of complex systems for future fusion project as well as other systems in the industry.

5.1 Description of the case study environment

Nuclear fusion is a promising source of massive and clean energy for humanity [163, 164]. ITER is an international project and is a part of a series of experimental reactors which are meant to investigate and demonstrate the feasibility of using fusion as a practical source of energy. In ITER, construction of physical test mock-ups can be very expensive due to the large-scale and complexity of the facilities. Digital mock-ups and virtual tests have been extensively used especially throughout the design and operations planning process of ITER [165]. The digital mock-ups are further utilized to design and test the maintenance procedures of the reactor via remote-handling equipment. Extending the use of virtual prototypes to all phases of the lifecycle, from the concept design to the manufacturing and maintenance phase will lead to an increase in confidence in the systems, while decreasing the need for some aspects of costly physical prototypes. Therefore, this thesis has been motivated by the clear research trend towards reducing the need for physical prototypes in the development of fusion reactors through the use of digital tools.

The purpose of the ITER reactor (**Fig. 46**) is to demonstrate nuclear fusion as a feasible energy source. The technological goal of ITER is to deliver ten times the fusion power compared to the input. This means that with 50 MW of input power the ITER machine is designed to produce 500 MW of fusion power.

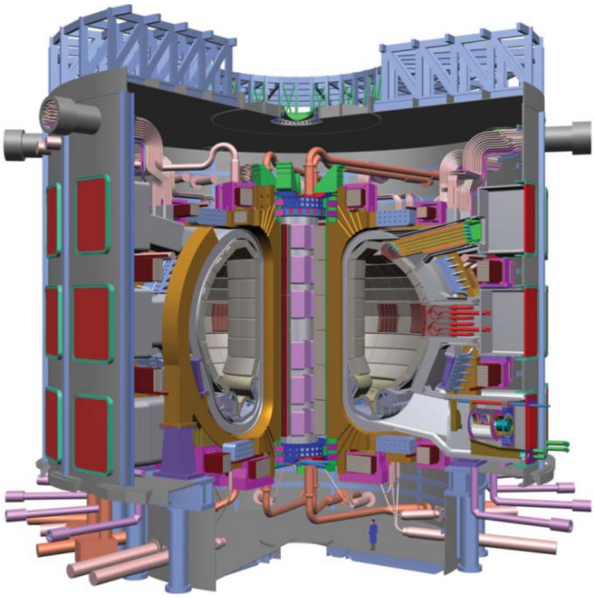


Fig. 46 – Model of the ITER reactor

This 500 megawatt test fusion power plant is already under construction in Cadarache in the south of France. The global cost of ITER construction is estimated at over EUR 6.5 billion over the next ten years, of which the EU will contribute 45 per cent. Another EUR 5 billion of funding is anticipated for the 20-year operation period.

Such powerful machines will deal with huge amounts of energy, in the form of heat as well as in the form of neutrons that are liberated during the fusion reaction. This results in a situation where machine components become activated and thus direct human intervention in the machine is no longer possible due to a hazardous radioactive environment. For the next generation of fusion experimental power plants at ITER level and above, the radiation level for manned access will be exceeded. Thereby the developed technology uses Remote Handling (RH) systems to be able to perform all operations in hostile areas of the machine.

An important aspect of the reactor that needs to be taken into account during the design phase of the machine is the maintenance operations that will occur under hostile conditions. Fusion reactors require maintenance in three situations:

- Unscheduled system failure preventing the normal operation of the machine
- Periodic preventive replacements of components
- Machine system upgrades for experimental purposes

Due to the radiation level, together with heavy and consequent components to be manipulated, the developed approach is to perform the maintenance operations remotely with the help of remote handling devices. Remote handling is the technology that enables the synergistic combination of technology and engineering management systems in order to safely, reliably and repeatedly perform manipulation without being humanly in contact with the hostile environment.

Remote handling will have an important role to play in the ITER Tokamak. Once the operation begins, inspections, repair and changes in the reactor can only be performed via specialized remote handling equipment. Very reliable and robust remote handling techniques will be necessary to manipulate and exchange components (**Fig. 47**) weighing up to 10 tons.

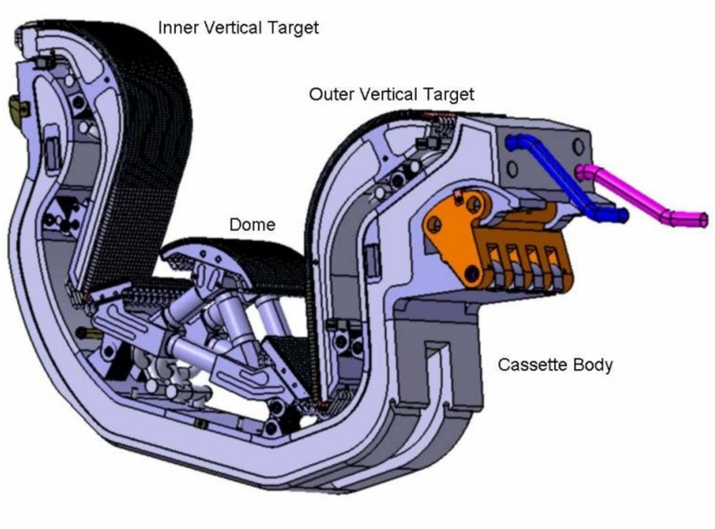


Fig. 47 – ITER Divertor Cassette 3D model [166]

The Divertor Test Platform 2 (DTP2) laboratory, located at the VTT Technical Research Centre of Finland in Tampere, is used for developing equipment, methods, software and all parts of the machine through the use of virtual technologies.

The aims of this platform are to test and demonstrate all the remote handling operations of the ITER divertor, providing the necessary input for the final installation. The purpose of the DTP2 is to plan a full maintenance cycle, develop tools and methods necessary for this, while defining risks and articulating hazard scenarios. The facility provides full functional tests of specially designed water hydraulic robots to carry heavy components during maintenance operation [167-171]. ITER is not an end in itself: it is the bridge towards a first plant that will demonstrate the large-scale production of electrical power and Tritium fuel self-sufficiency. This is the next step after ITER: the Demonstration Power Plant, or DEMO for short. A conceptual design for such a machine could be complete by early 2020. If all goes well, DEMO will lead fusion into its industrial era, beginning operations in the early 2030s, and putting fusion power into the grid as early as 2040.

Therefore, the goal of this thesis aims at focusing on the design process of mechatronic systems that are heavily used in remote handling in fusion reactors for carrying heavy components, but which can be extended and applied to other engineering applications, such as in airplane, ship, automobile and other industrial forms of manufacture.

5.2 Description of the project: DEMO

DEMO is the successor of ITER and the next step to demonstrate the feasibility of producing fusion energy using a more industrial approach. Its purpose is to develop and test technologies for operating a reactor not as a scientific experiment, but as a power plant. DEMO must demonstrate the necessary technologies not only for controlling more powerful plasmas than previously but also for safely generating electricity consistently, as well as technologies for regular, rapid, and reliable maintenance of the plant. As in ITER, DEMO will need to be fully maintained remotely by means of remote handling equipment. However, one of the main requirements is the plant availability. Therefore, maintenance operations must be as fast as possible to decrease the shut down time of the power plant.

This high-level requirement drives the design process by orienting design choices towards a high plant availability rate by increasing the reliability of the remote handling equipment. The early phases of the design process are focusing on developing a solution that verifies the high-level requirements. By definition, in the early design phase, the developed system is very weak in detail; however, a strong confidence in the concept design is required before going deeper in the design. Collecting confidence in the developed system as early as possible decreases the risk of design errors and thus reduces also the development time of the system.

In this particular case study of developing new remote handling solutions for DEMO, based on the plant’s high-level requirements, it requires a novel approach for establishing confidence in the design from the very early phases of the development process. The remote handling operation of the Divertor area is of primary importance for the availability of the plant, and complex systems need to be developed, verified and validated. Therefore, this case study has been chosen to support the validation of this thesis work.

The method developed in this thesis will aim at improving the design process of complex systems in the very early phase with the aim of establishing confidence in the concept design for later verification and validation. This method helps to drive the design of the system based on the high-level requirements, which is primarily controlling the reliability of the developed systems to ensure higher plant availability.

5.3 Description of the case study: Divertor Cassette RH system

As in ITER, the in-vessel area where the plasma is located during the operation of the plant consists of a torus vessel. This torus is composed of a wall and a floor. The wall consists of blankets that are actively cooled to control the plasma operation as well as extracting out of the reactor the energy produced in terms of heat. The floor consists of a Divertor, quite similar to ITER, and its aim is to extract the heat, collect dust and control the plasma.

The wall and floor of the vessel of the reactor will be subjected to high constraints in terms of temperature and temperature changes, as well as neutronics, a vacuum environment and very high stress. Therefore, those components that face the plasma during operation will require regular replacement during the life-time of the power plant. Remote handling devices are therefore required to perform the extraction as well as the installation of these facing components inside the reactor. The Divertor area consists of 54 Cassettes, is designed with 18 maintenance ports through which the 54 Divertor Cassettes will be installed and removed. This equates to 3 Divertor Cassettes per ports. In comparison, ITER had only 3 maintenance ports that were used to install and remove the 54 Cassettes that composed the ITER Divertor area. In ITER, the entire replacement of the Divertor area, which entails removal of old cassettes and installation of the new set of cassettes, was estimated to take around 3 months. During this time, the power plant would be shut down and is therefore non-operational. In DEMO, plant availability is a high level requirement, and the maintenance time needs to be shortened. Therefore, each maintenance port will be used to replace 3 Cassettes only, which allows for performing more Divertor maintenance operations in parallel, which will lead to shorter Divertor maintenance time. The specificity of the Divertor remote handling operations in DEMO is of course increasing the availability of the plant by decreasing the maintenance time of the plant, by means of remote handling due to the high radiation environment. The Divertor maintenance operation consists in carrying remote handling equipment from the hot-cell, which is the place where the refurbishment and replacement operations are performed and where equipment are stored, to the in-vessel area. This operation consists of using a mean of transport, called a cask, between the hot-cell and the maintenance port of the vessel.

In the very early design phase, only a small amount of information is available about the required system itself. However, environment information according to where the system will aim to operate is defined. In this case, the information available used to start the design process of the Divertor remote handing system consists of the type of environment (nuclear, dust and temperature controlled), the type of components to handle (Divertor Cassettes), the number of ports through which to perform the operation, and the number of cassettes per ports. However, the configuration of the port (such as the size of the cross section, the length or the inclination) is not defined, or highly subject to changes during the design of the DC remote handling system.

5.4 System requirements analysis

In the very early phases of the design, different options for the general configuration of the tokamak were proposed, and a comparison of each option needs to be performed in order to decide which option is more relevant from a remote handling point of view. Since one of the main requirements in DEMO is the availability of the plant, the failure of the remote maintenance systems should be minimized and in the event that there is a failure it should be recoverable.

When designing a complex system, a breakdown structure of the existing requirements should be defined in order to categorise requirements and allocate them properly during the design process. The initial requirements are defined by translating customer needs (CN) into requirements. The first step of the design process consists of collecting and listing requirements. Then requirements can be categorised and used as input for the design process. From a design point of view, for some cases when the list of requirements is consequent, all the requirements cannot be relevant in the design process from the beginning. Yet in accordance with the evolution of the design, requirements are iteratively inputted. In this particular case study, many requirements are derived from the previous project ITER. It is obviously necessary to use the ITER experience and the knowledge gained from previous studies performed over many years of designing the Divertor Cassette Remote Handling system in ITER. However, special attention is needed when reusing previous experiences and requirements since the purpose of the entire project was different than in DEMO.

5.4.1 Customer needs

The very first step in the design process is to establish the customer needs (CNs). The CNs are obtained from the previous experience as well as from discussions with the various stakeholders. In this case study, the high-level requirements consist of the customer needs that include information on the general plant design and procedures. The list of customer needs is provided in **Appendix A - Table 16.**

According to those high-level requirements, it has been defined that the Divertor remote handling system will perform the installation and removal of 3 Divertor Cassette per maintenance ports. Therefore, the main design of the vacuum vessel consists of 16 maintenance ports. The availability of the plant is one of the main requirements, which makes a big difference in the design compared to ITER.

Some concept designs of the vacuum vessel have already been performed and 2 options for the configuration of the maintenance ports have been suggested. The first option is to consider the port being inclined at 45 degrees from the ground of reference. The second option is to have a horizontal port. Those two options involve important differences in the design of the remote handling system, in terms of operations, kinematics and available space.

5.4.2 Customer constraints

The customer constraints are the constraints provided by the customer that limit and therefore guide the design of the developed system. Constraints can be related to the environment, time, costs, reliability and availability.

The list of the main customer constraints is provided in **Appendix A - Table 17**.

5.4.3 From customer needs to functional requirements

Functional requirements are built from the CNs, and each system function is then mapped to the related CNs. The Design Structure Matrix (DSM) [145] method is used to perform the mapping. In this case study, 13 functional requirements are mapped with the 22 CNs (Cf. **Appendix B - Table 18**). For instance, if parameter A affects the choice of parameter B, then we will put a mark ‘X’ in the cell where the column of A and the row of B intersect. We repeat this process until we have recorded all parameter interactions. The result is a map of the dependencies that affect the detailed structure of the artefact.

The same approach is used to create design Input Constraints (ICs). Input Constraints are created and mapped against Customer Constraints (See Section 5.4.4). Once the functions and their interaction with customer needs are placed in the DSM, a clustering approach [172] can be applied in order to group the functions into sub-systems that are complementary so as to regroup related functional requirements. Therefore, in this case study, 5 remote handling sub-systems have been defined as well as their respective functional requirements (Cf. **Appendix B** - **Table 19**).

- Transfer cask
    - Shall provide features for transporting hardware from the power plant to the maintenance facility
- Mover
    - Shall provide brakes to enter into a safe mode
    - Shall provide radial motion
    - Shall provide interfaces to support a manipulator and tooling
    - Shall provide interfaces to support various end-effectors
    - Shall provide rescue features compatible with RM rescue equipment (together with the rescue sub-system)
- Manipulator and tooling
    - Shall provide tooling for cutting, welding and pipes inspection as well as for connecting and disconnecting the divertor cassettes to the vessel
    - Shall provide interfaces for handling pipes
    - Shall provide interfaces for handling the port inner closure plate (together with the End-effectors sub-systems)
- End-effectors
    - Shall provide lifting motion
    - Shall provide toroidal motion
    - Shall provide an interface with the Divertor Cassettes
    - Shall provide an interface for handling the port inner closure plate (together with the manipulator sub-system)
- Rescue system
    - Shall provide rescue features compatible with RM rescue equipment (together with mover sub-systems)
    - Shall provide rescue systems for RH equipment

The main interfaces of the Divertor Cassette Remote Handling system are presented in **Fig. 48**.

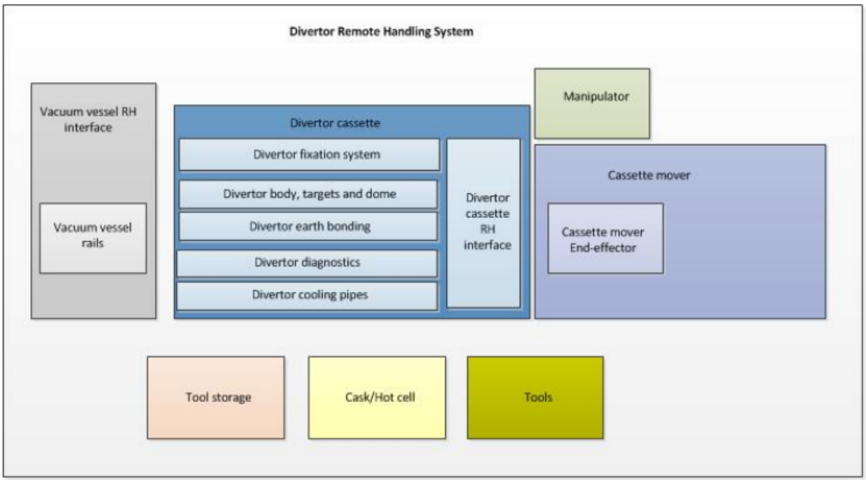


Fig. 48 – DEMO Divertor Remote Handling system interfaces [173]

To be able to perform the removal and installation of the Divertor Cassettes, the system has been divided into systems and sub-systems, and the interfaces have been listed. The system itself is composed of a main mover, its end-effector and a manipulator. The system will interact with different interfaces such as the Divertor Cassette, Vacuum Vessel, transport cask, tool storage and hot-cell.

5.4.4 From customer constraints to design input constraints

The input constraints are defined from the customer constraints (Cf. **Appendix B - Table 20**), and are then mapped with each other using the DSM approach as previously.

The clustering approach of the Input Constraint DSM (Cf. **Appendix B - Table 21**) enables the definition of the main criteria that need to be taken into account during the design and iterative assessment of each RH system and sub-system. In this case study 6, the design parameters have been listed.

The Divertor RH systems shall:

- Maximize plant availability
- Maximize recoverability
- Respect the design constraints
- Maximize the reliability
- Respect procedure constraints
- Minimize failures (occurrence, risk, severity)

From those 6 parameters, four parameters can be assessed quantitatively and are not related to the formalized design procedures. The plant availability, the RH system recoverability and reliability have to be maximized when the failure criteria that encompass the occurrence, risk and severity of the failures have to be minimized. Therefore, using those defined parameters will enable the engineer to assess different RM systems and procedures. Various remote handling procedures can be assessed as well as the use of various RM systems, equipment and technology. Using these parameters will also enable an assessment of the influence of any plant design changes on the remote handling procedures.

5.5 Modular and iterative design process

The developed process offers the possibility to be iterative and modular. From a very high-level system functional definition, this approach can lead the design throughout each phase of the design process. The high-level sequence can be used to derive more detailed tasks and operations without modifying the main sequence. As well as systems and sub-systems, it is possible to derive various design options from a functional level up to the component level. Various design configurations can be tested in order to quantify the most appropriate concept against customer needs.

In the case of DEMO, environmental factors may influence the reliability of the system and its components, such as temperature or radiation level. Using the stochastic Petri Net approach enables the application of different criteria to each phase of the maintenance operation according to the position of the system inside the vessel. For instance, when the system is in the transfer cask, the radiation level will be much lower than when the mover will be in the vessel area. Reliability will thereby be affected. This same approach applies to the temperature and dust criteria. Since the influence of the radiation on the reliability of the components is not yet a well-known factor, it is not taken into account in this study. **Fig. 49** shows an overview of the iterative approach using DEMO remote maintenance as a case study.

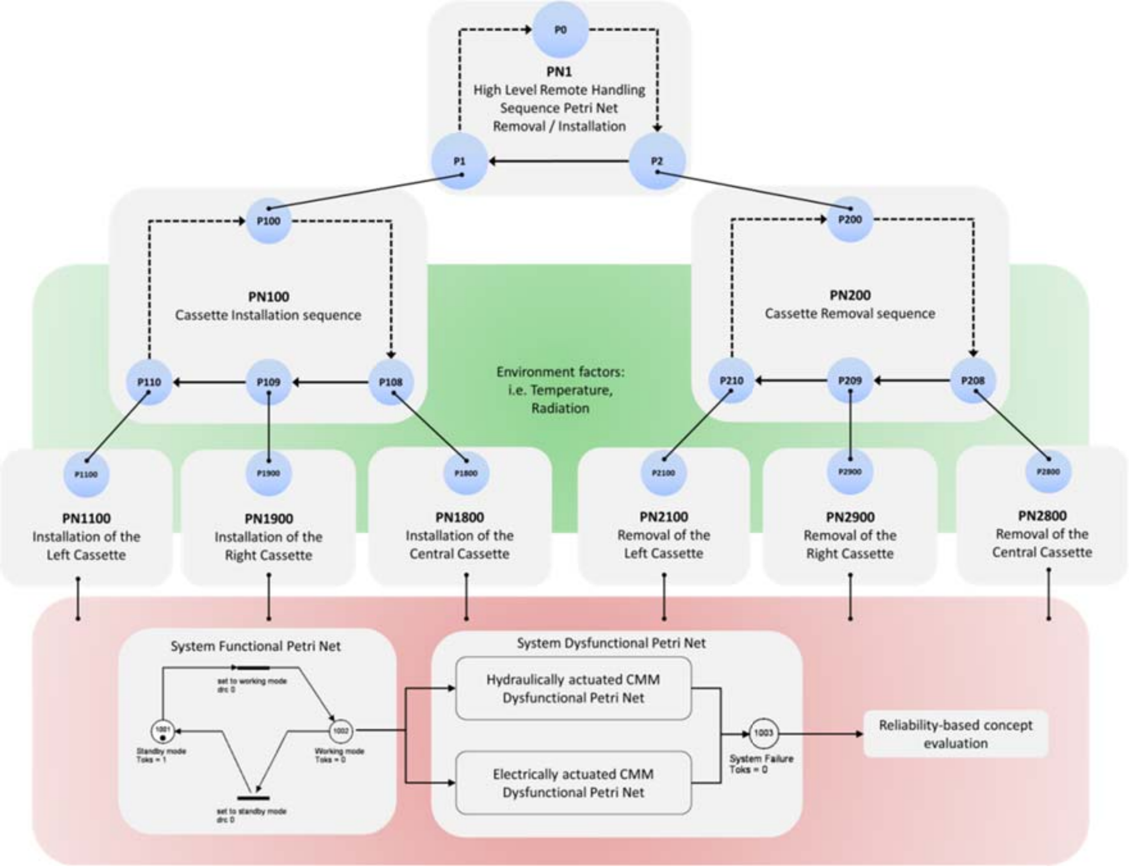

P0
PN1
High Level Remote Handling Sequence Petri Net
Removal / Installation
P1
P2
P100
PN100
Cassette Installation sequence
P108
P109
P110
P200
PN200
Cassette Removal sequence
P208
P209
P210
Environment factors:
i.e. Temperature, Radiation
P1100
PN1100
Installation of the Left Cassette
P1900
PN1900
Installation of the Right Cassette
P1800
PN1800
Installation of the Central Cassette
P2100
PN2100
Removal of the Left Cassette
P2900
PN2900
Removal of the Right Cassette
P2800
PN2800
Removal of the Central Cassette
System Functional Petri Net
set to working mode
drc 0
1001
Standby mode
Toks = 1
1002
Working mode
Toks = 0
set to standby mode
drc 0
System Dysfunctional Petri Net
Hydraulically actuated CMM Dysfunctional Petri Net
Electrically actuated CMM Dysfunctional Petri Net
1003
System Failure
Toks = 0
Reliability-based concept evaluation

Fig. 49 – Design concept evaluation framework applied to DEMO maintenance strategy

5.6 Discrete event dynamic system

The requirements analysis has been performed and CNs and CCs have been defined as well as system and sub-system functional requirements. Therefore, it is possible to define the discrete sequence of the system, which is basically the operational sequence that the system is expected to perform. In this case study the operational sequence is the maintenance strategy of the Divertor. The dynamic discrete sequence is the basis of the Functional Stochastic Petri Net approach.

Table 5 collects the high-level operational sequence of the removal of the Divertor remote handling system. The column *operation ID* orders the operations and the column *Place ID* links the Petri Net discrete event to the respective operation. The column *Time estimation* provides a normal distribution of the operational time of each operation on a scale from 1 to 5, as presented in **Table 4**. The engineer estimates the time of each operation according to the scale and the table gives the lognormal parameters for defining transitions in the discrete Petri Net operational sequence.

During the preliminary design phases, operational time is unlikely to be known. Therefore, the time estimation enables us to give some approximations, while the randomisation or fuzzification (**Fig. 50**) gives more objectivity to the estimation.

Table 4 – Time distribution scale

		lognormal distribution (h)	
Scale	**Time Distribution**	**μ**	**σ**
1	from 0 to 2h	1	0,5
2	from 2h to 10h	4	2
3	from 10h to 1day	14	5
4	from 1day to 4days	84	15
5	from 4days to 10days	168	25
D	Timeless transition	Dirac distribution	

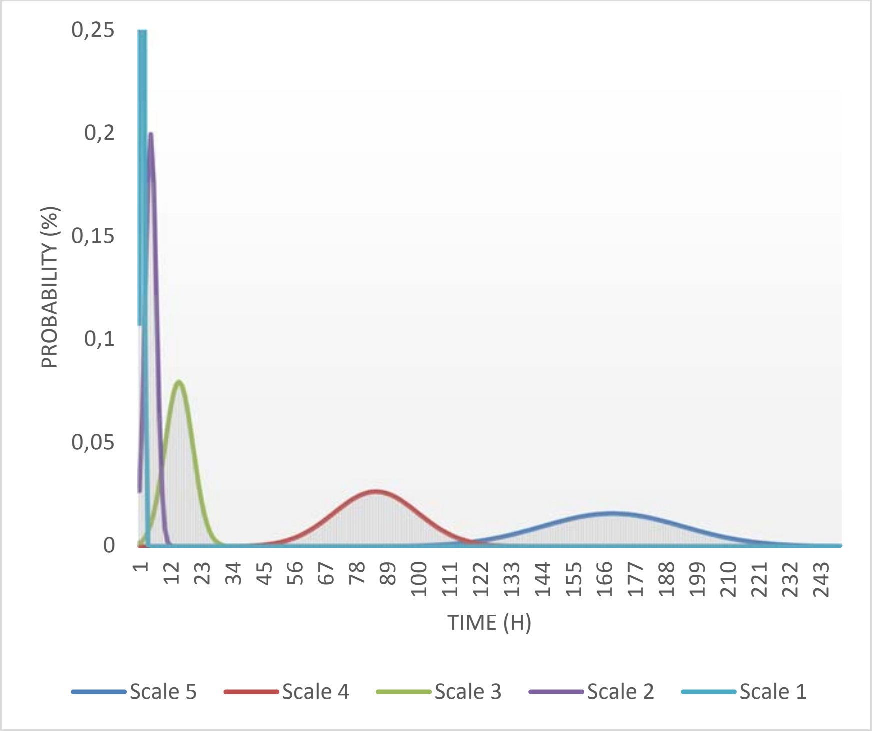


Fig. 50 – Time randomisation/fuzzification following a lognormal distribution

Operations 1, 8, 9 and 10 are timeless transitions, since they indicate a phase, such as *Central Cassette Removal*. Therefore, a Dirac time distribution is used with a parameter of 0s.

For each operation a set of systems or sub-systems are used. Therefore, the *utilisation* column is used to list devices and is mapped with each operation. Four sub-systems are listed: *transfer cask*, *Cassette Mover*, *Cassette End-Effector* and *Manipulator*. For instance, in this case study, the transfer cask is used in the following operations: 2, 7, 8.11, 9.7, 10.8 and 12 of **Table 5**.

Table 5 - DEMO Divertor Removal Sequence

Petri Net	Operation	Cassette Removal	Transfer Cask	Cassette Mover	Cass End-Effector	Manipulator+tools	Time estimation
ID		**Divertor RH operation Sequence**					
P1	1	Starting point for Divertor Removal					dirac
P2	2	Docking the transfer cask	X				1
P3	3	Removal of the PCP				X	2
P4	4	Removal of the ex-vessel cooling pipes		X		X	4
P5	5	Removal of the inner flange		X		X	2
P6	6	Removal of in-vessel Divertor pipes		X		X	4
P7	7	Preparing entering into the tunnel	X	X		X	2
P8=P80	8	Removal of the Central Cassette					dirac
P81	*8.1*	Drive the Cassette Mover (CM) from the transfer cask up to the Divertor Central Cassette		X			1
P82	*8.2*	Align the CM to the Central Cassette		X	X		1
P83	*8.3*	Hold CM in fixed position		X	X		1
P84	*8.4*	Release the Earth Bonds				X	2
P85	*8.5*	Connect CM end-effector to Cassette interface			X		1
P86	*8.6*	Release the cassette Preloading System using manipulator and tools				X	2
P87	*8.7*	Release the Cassette Locking using manipulator and tools				X	2
P88	*8.8*	Take hold of the cassette outer rail bridge		X	X		1
P89	*8.9*	Release the outer rail bridge using manipulator and tools				X	2
P90	*8.10*	Lift the Central cassette together with the outer rail bridge		X	X		1
P91	*8.11*	Carry the cassette and outer rail bridge back to the cask	X	X	X		2
P9=P900	9	Removal of the Right Cassette					dirac
P910	*9.0*	Drive the CM from the cask to the Right Cassette		X			1

P911	*9.1*	Align the CM to the Right Cassette		X	X		1
P912	*9.2*	Release the Earth Bonds				X	2
P913	*9.3*	Take hold of the cassette		X	X		1
P914	*9.4*	Release the cassette Preloading System				X	2
P915	*9.5*	Release the Cassette Locking				X	2
P916	*9.6*	Lift the Right Cassette		X	X		1
P917	*9.7*	Carry the Right Cassette to the cask	X	X	X		2
P10=P 150	10	Removal of the Left Cassette					dirac
P101	*10.1*	Drive the CM from the cask to the Left Cassette		X			1
P102	*10.2*	Align the CM to the Left Cassette		X	X		1
P103	*10.3*	Release the Earth Bonds				X	2
P104	*10.4*	Take hold of the cassette		X	X		1
P105	*10.5*	Release the cassette Preloading System				X	2
P106	*10.6*	Release the Cassette Locking				X	2
P107	*10.7*	Lift the Left Cassette		X	X		1
P108	*10.8*	Carry the Left Cassette to the cask	X	X	X		2
P11	11	Installation of PCP				X	2
P12	12	Removal of the cask	X				1

Table 6 describes the installation sequence of the Divertor maintenance operation and respective time estimation of each operation.

Table 6 – DEMO Divertor Installation Sequence

Petri Net	Operation	**Cassette Installation**	Transfer Cask	Cassette Mover	Cass End-Effector	Manipulator+tools	Time estimation
ID		**Divertor RH operation Sequence**					
P260	1	Starting point for Divertor Installation					D
P261	2	Docking the transfer cask	X				1
P262	3	Removal of the PCP				X	2
P263= P272	4	Installation of the Left Cassette					D
P273	*4.1*	Drive the Cassette Mover (CM) and the Left Cassette from the transfer cask up to the Divertor area		X			1
P274	*4.2*	Align the CM to the Vessel		X	X		1
P275	*4.3*	Carry toroidally the Left Cassette to its final position in the Vessel		X	X		1
P276	*4.4*	Preload and lock the Left Cassette to its final position			X	X	2
P277	*4.5*	Disconnect the End-Effector from the Cassette Interface			X	X	1
P278	*4.6*	Connect the Earth Bonds				X	2
P279	*4.7*	Carry the CM and end-effector back to the cask	X	X	X		2
P264= P321	5	Installation of the Right Cassette					D
P322	*5*	Drive the Cassette Mover (CM) and the Right Cassette from the transfer cask up to the Divertor area		X			1
P323	*5.1*	Align the CM to the Vessel		X	X		1
P324	*5.2*	Carry toroidally the Right Cassette to its final position in the Vessel		X	X		1
P325	*5.3*	Preload and lock the Right Cassette to its final position			X	X	2

P326	*5.4*	Disconnect the End-Effector from the Cassette Interface			X	X	1
P327	*5.5*	Connect the Earth Bonds				X	2
P328	*5.6*	Carry the CM and end-effector back to the cask	X	X	X		2
P265= P371	6	Installation of the Central Cassette					D
P372	*6.1*	Drive the Cassette Mover (CM), the outer rail bridge and the Central Cassette from the transfer cask up to the Divertor area		X			1
P373	*6.2*	Align the CM to the Vessel		X	X		1
P374	*6.3*	Lock the Outer rail bridge to the Vessel			X	X	2
P375	*6.4*	Preload and lock the Central Cassette to its final position			X	X	2
P376	*6.5*	Disconnect the End-Effector from the Cassette Interface			X	X	1
P377	*6.6*	Connect the Earth Bonds				X	2
P378	*6.7*	Carry the CM and end-effector back to the cask	X	X	X		1
P266	7	Preparing to close the maintenance port (pipes installation)	X	X		X	2
P267	8	Installation of in-vessel pipes		X		X	4
P268	9	Installation of the inner flange		X		X	2
P269	10	Installation of the ex-vessel cooling pipes		X		X	4
P270	11	Installation of PCP				X	2
P271	12	Removal of the cask	X				1

Table 7 indicates the different Petri Net levels. The high level operational sequence consists of the RH Removal and Installation Sequence (P1 to P12 and P3002 to P3013). Each high-level sequence is the parent of 3 sub-sequences (Central, Right and Left Cassette).

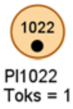
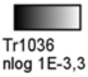
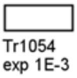
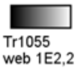
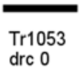
Table 7 – Places ID and respective Petri Nets

ID	Petri Nets
P1 to P12	RH Removal Sequence
P81 to P91	Central Cassette Removal
P910 to P917	Right Cassette Removal
P101 to P108	Left Cassette Removal
P260 to P271	RH Installation Sequence
P272 to P279	Central Cassette Installation
P321 to P328	Right Cassette Installation
P371 to P378	Left Cassette Installation

The Petri nets mentionned in the above table are described later in this section (**Fig. 52**, **Fig. 53**, **Fig. 54** and **Fig. 55**). The software used to model the behavior of complex dynamic systems is: GRIF - GRaphical Interface for reliability Forecasting and the module is: Stochastic Petri Nets with Predicates and Assertions.

Table 8 is giving the legend of the pictogram used to represent the Petri Net.

Table 8 – Petri Net representation legend

	Place number, ID name and number of tokens.
	Transition set with normal logarithmic distribution - Average $m=1*10^{-3}h$ - Error factor $e=3$
	Transition set with exponential distribution - Rate: $\lambda=3*10^{-4}$
	Transition set with Weibull distribution. - Mean MTTF: $m=100\ h$ - Shape parameter: $\beta=2$
	Transition set with Dirac distribution. - Delay: $\delta=0h$

Transitions can be set with an iput variable (represented with ‘?’) or an output variable (represented with ‘!’) to define when the transition can be fired.

The first discrete event dynamic level is the High-level maintenance strategy (**Fig. 51**). Starting from *RH_operation_OFF* to *RH_operation_START* and then set the maintenance operation to *Cassette_removal* and finally to *Cassette_Installation*.

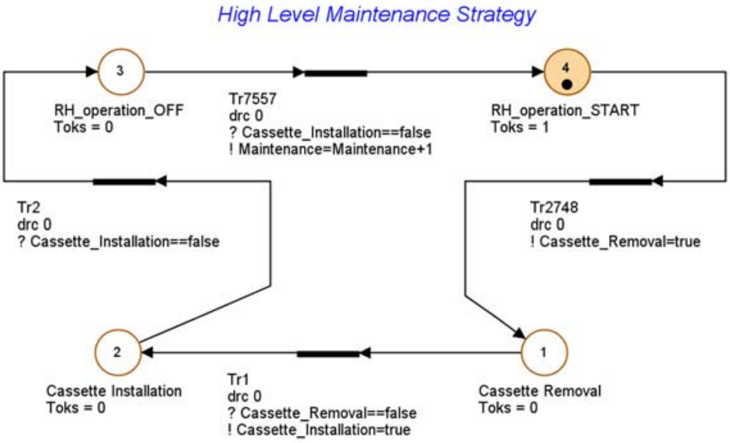

High Level Maintenance Strategy
3
RH_operation_OFF
Toks = 0
Tr7557
drc 0
? Cassette_Installation==false
! Maintenance=Maintenance+1
4
RH_operation_START
Toks = 1
Tr2
drc 0
? Cassette_Installation==false
Tr2748
drc 0
! Cassette_Removal=true
2
Cassette Installation
Toks = 0
Tr1
drc 0
? Cassette_Removal==false
! Cassette_Installation=true
1
Cassette Removal
Toks = 0

Fig. 51 – High-level discrete event dynamic system of DEMO RH maintenance

The **Fig. 52** represents the Petri Net of the high level sequence that consists of the main phases of the RH Divertor Removal operation. *Place 1* represents the first operation named: ‘*Starting point of the divertor removal*’ and is represented with a transition set as Dirac distribution since it is only an indicative step. The token represents the state of the task. **Fig. 52** is the initial state of the sequence of the Divertor Cassettes removal operation. Then each transition of *places 2* to *8* are setted with LogNormal distribution to represent the time estimation of each place.

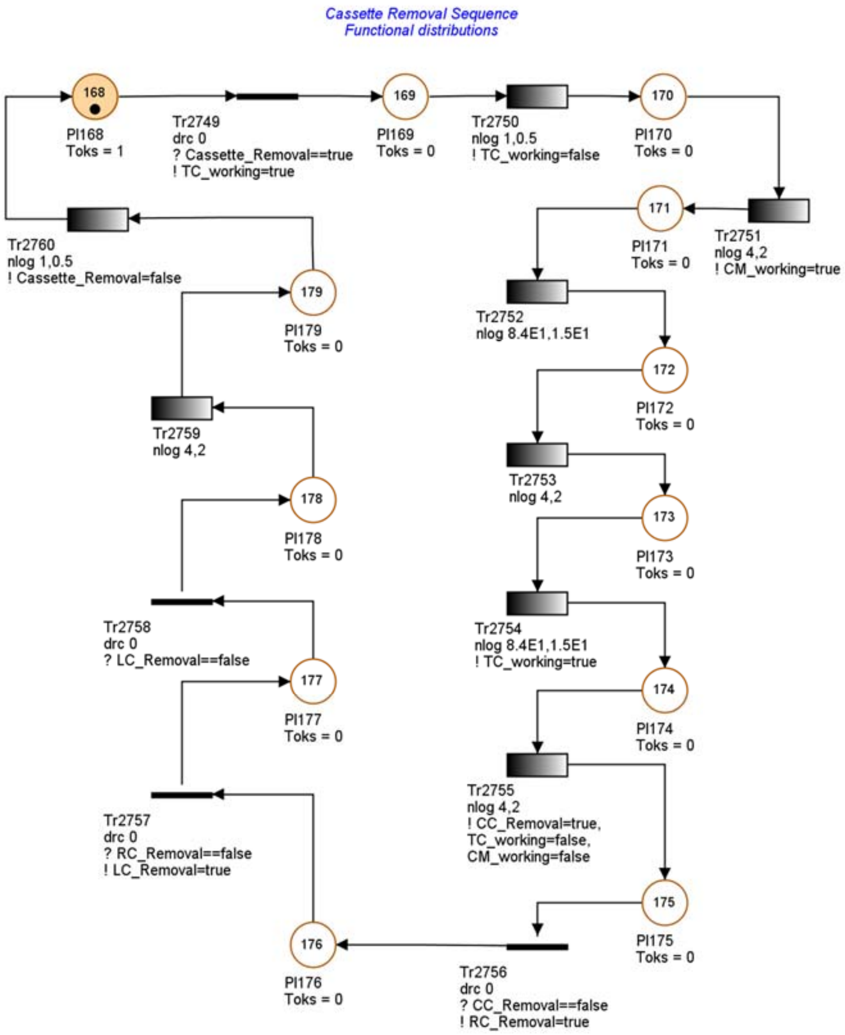


Fig. 52 – High-level Stochastic Petri Net for representing the RH sequence

When the token reaches place 8, the variable *CC_Removal* is set to *true* in order to enable the start of the Central Cassette Removal sub-Petri net shown in **Fig. 53.** On the place *P2*, the transfer cask is used to perform the operation, therefore the transition between *P1* and *P2* sets the variable *TC_working* as *true* and sets back to *false* when the transfer cask is no longer in working mode. The working and failure mode of the sub-system is described below in Section 5.7.

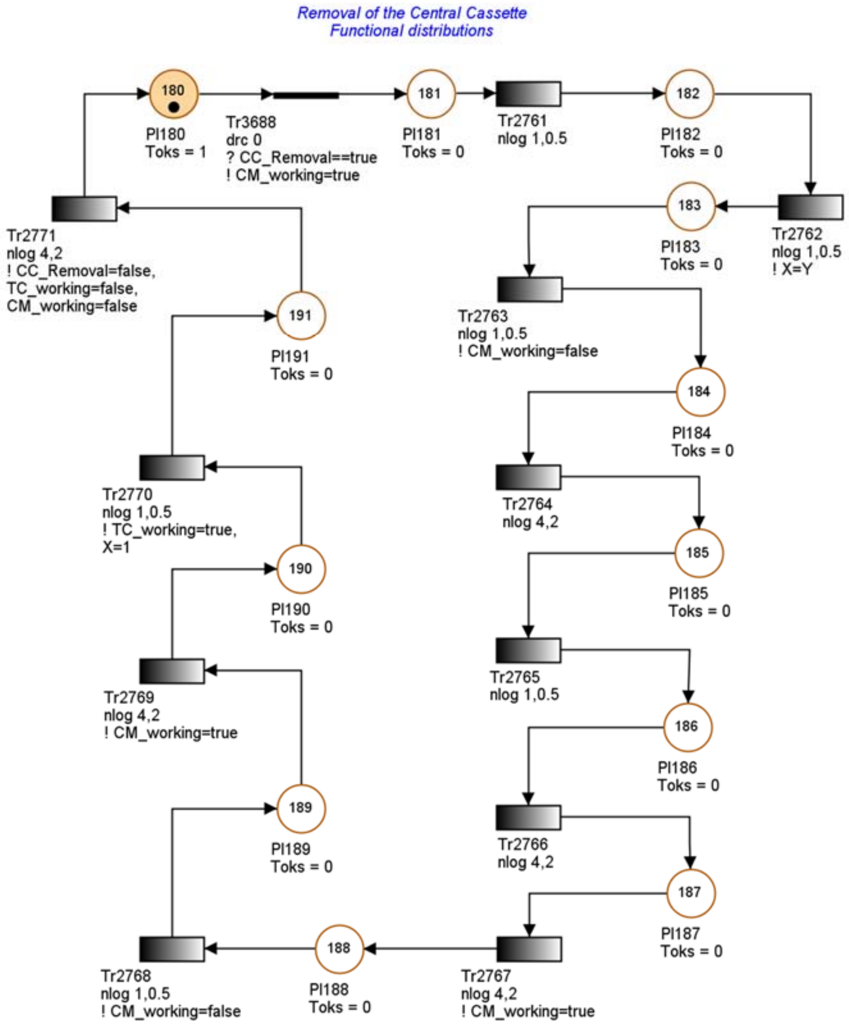


Fig. 53 – Central Cassette Removal Petri Net sequence

After removing the central cassette, then the variable *CC_Removal* will set to *false* and the high level Removal sequence will continue to *place 9* and set the *RC_Removal* to *true* to enable the Petri net for the right cassette removal shown in **Fig. 54**. At the end of the Right Cassette removal, the *RC_Removal* variable is set to *false*, and the token in the high level Petri net will go to *Place 10* and set *LC_Removal* to *true* for starting the removal sequence of the Left Cassette shown in **Fig. 55**.

The Stochastic Petri net of the Central Cassette removal sequence starts at place *ID 80*, which is set with a Dirac transition. It also has a pre-requisite called *guard* for *CC_Removal* set as *true*. When the high-level sequence set the *CC_Removal* as *true*, then the Central Cassette removal Petri net sequence starts. The transition towards P81 sets *CM_working* as *true* since the cassette mover is used to perform the tasks from *P81* to *P83*; the same applies for *P88*, *P90* and *P91*.

Fig. 54 consists of the stochastic Petri net of the Right Cassette removal sequence. The pre-requisite to enable the start of this Petri net is to set the *RC_Removal* to *true*, which happens when the token reaches place *ID10* on the high level Petri net sequence.

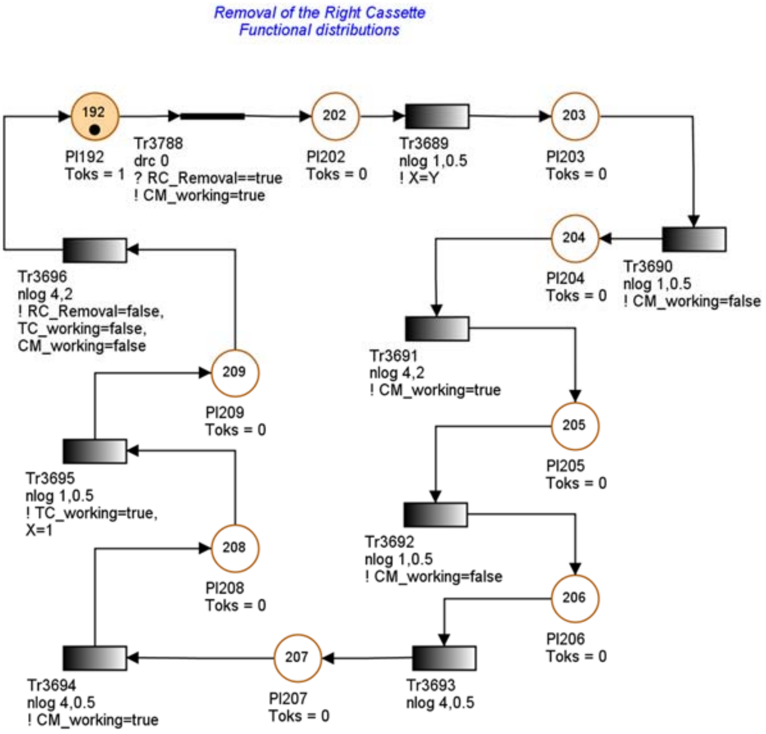


Fig. 54 – Right Cassette Removal Petri Net sequence

Fig. 55 consists of the stochastic Petri net of the Left Cassette removal sequence. The pre-requisite to enable the start of this Petri net is to set the *LC_Removal* to *true*, which happens when the token reaches *place ID10* on the high level Petri net sequence.

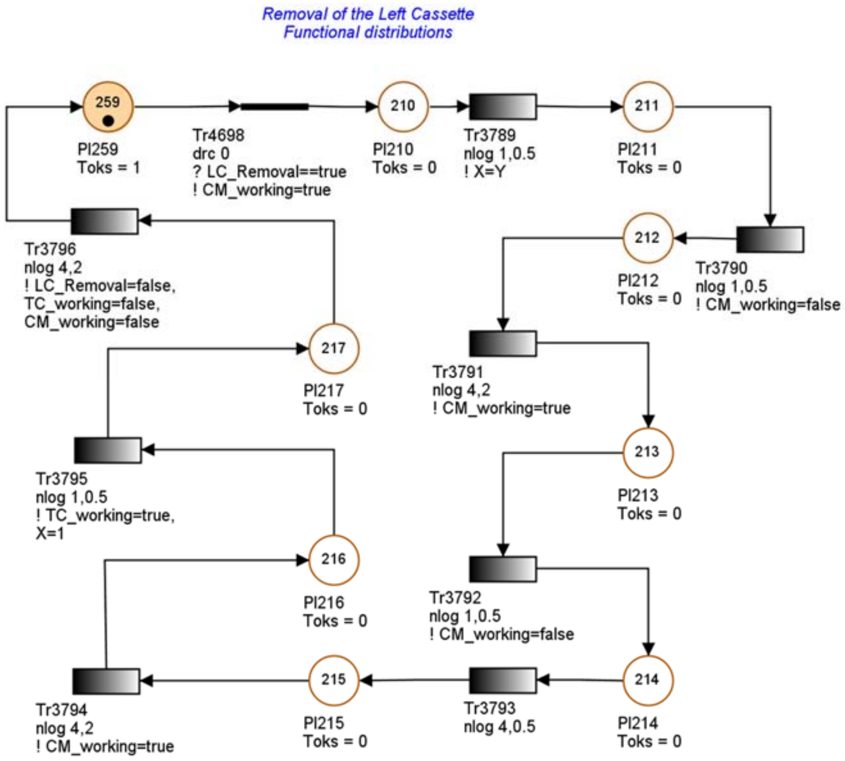


Fig. 55 – Left Cassette Removal Petri Net sequence

The previous set of Petri nets constitutes the two highest levels of the operational sequence representation. The highest level is the operation sequence of the developed system followed by the task sequence level, which in this case consists of the removal of the central, right and left Divertor cassette for DEMO.

In this case study, operations are performed in series. The central cassette has to be removed before the right cassette removal operation for instance. However, it is possible to have operations performed in parallel by two different devices for instance.

The following **Fig. 56**, **Fig. 57**, **Fig. 58** and **Fig. 59** represent the discrete event dynamic system of the installation sequence of the DEMO Divertor Cassette.

Fig. 56 represents the discrete event dynamic system of the high-level cassette installation sequence. Starting from *Place 260*, the Cassette installation begins and in *place 263*, the Left cassette is installed followed by the Right Cassette and finally the Central Cassette in *place 265*.

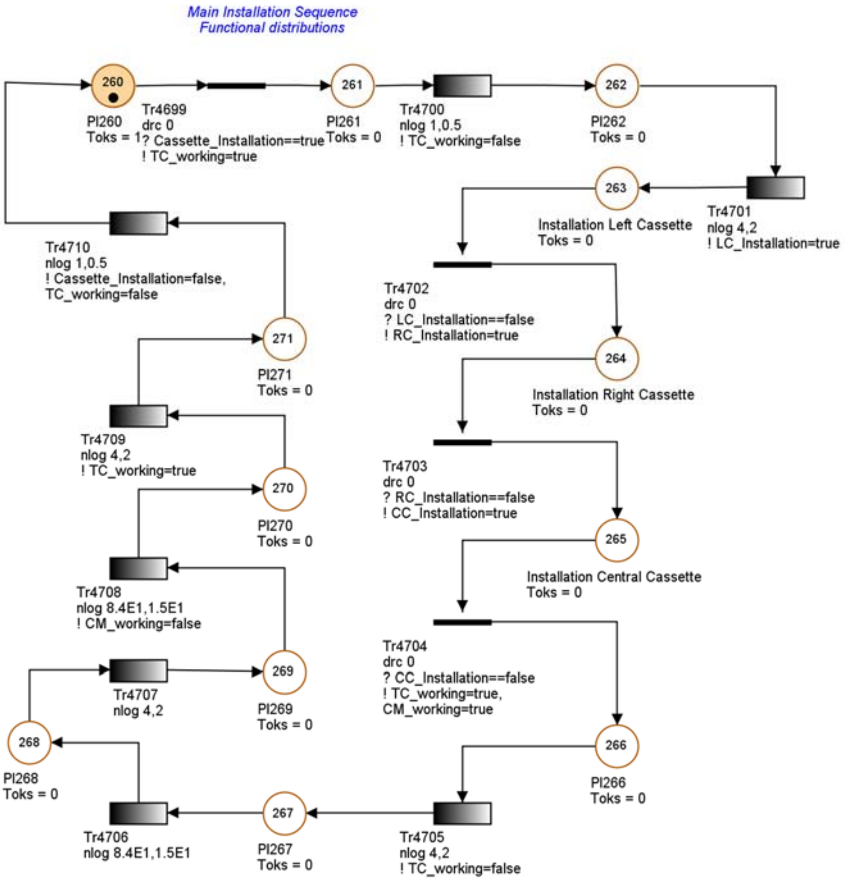


Fig. 56 – High-level Divertor Cassettes installation Petri Net sequence

Fig. 57 represents the discrete event dynamic system of the left cassette installation. Starting from *Place 272*, the left divertor cassette is installed through seven steps from *place 273* to *279*.

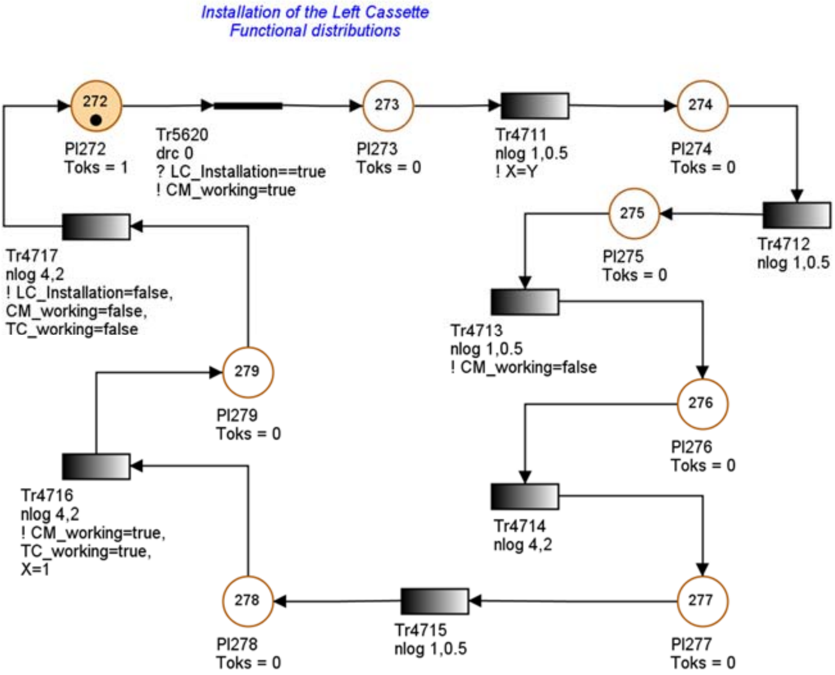


Fig. 57 – Left Cassette installation Petri Net sequence

Fig. 58 represents the discrete event dynamic system of the right cassette installation sequence. After installing the left cassette, the maintenance operation consists in installing the right cassette. This operation consists in seven steps, similar to the left cassette installation, represented from *places 322* to *328*.

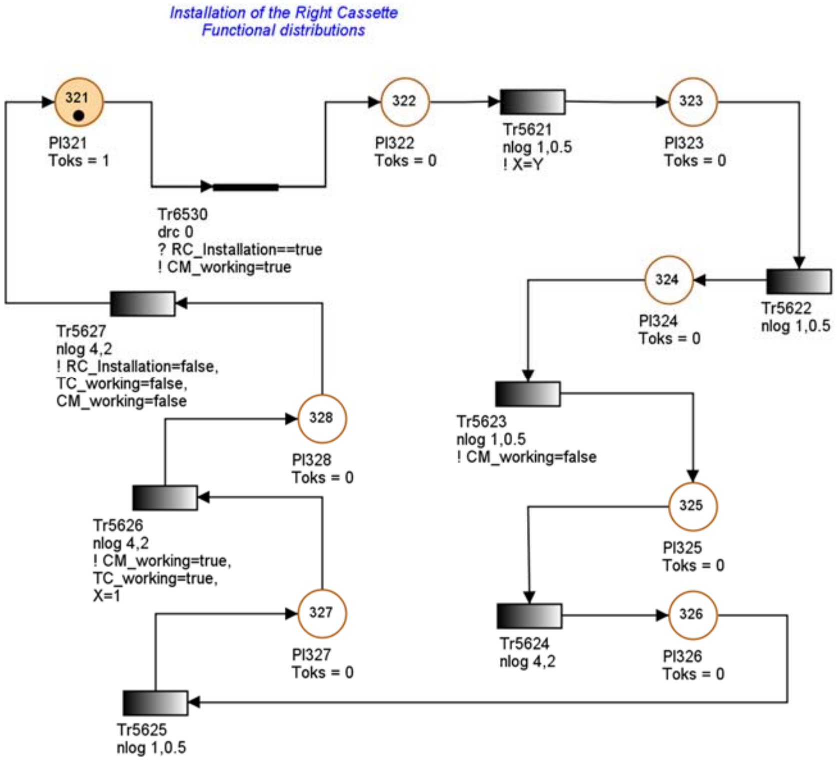


Fig. 58 – Right Cassette installation Petri Net sequence

Finally, the discrete event dynamic system of the central cassette installation sequence is represented in **Fig. 59**. After installing the left and right cassette, the maintenance operation consists in installing the central cassette to close the final gap of the divertor area. The central cassette installation consists in seven steps from *place 372* to *378*.

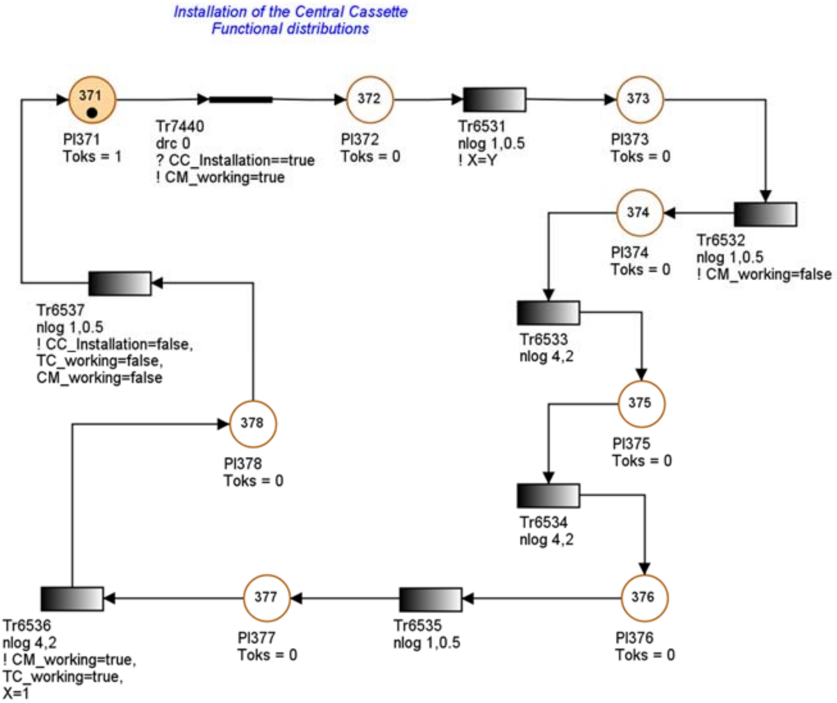


Fig. 59 – Central Cassette installation Petri Net sequence

As with the Cassette removal discrete event dynamic system, the discrete event dynamic system of the cassette installation is modelled as a series of events, however, when implementing the system functional Petri Net, it is operating in a parallel manner, which means that the top-level stochastic Petri Net is actually a set of parallel stochastic Petri Net models.

5.7 Functional Petri Net representation

In this section, the functional representation of two options of a particular system, the Divertor maintenance transfer cask, are presented using the block diagram approach presented in Section 4.1.3. Concerning the transfer cask system, in Section 5.4.3, we defined that the function of the transfer cask is to '*provide features for transporting hardware from the power plant to the maintenance facility*'. At this level of design, the general plant design is always evolving and various configurations are suggested. For instance, the inclination of the lower maintenance port can be horizontal or inclined at a 45° angle from the horizontal axis. It is then obvious that according to design changes, technical solutions will also evolve. While one transfer cask solution might be relevant for one port inclination, it may be not relevant for a different inclination. This method aims at defining and comparing different solutions in the early design phase in order to assess which solution is more relevant before going deeper in the detail design.

Now let's consider the two following port options for the case study:

- 45° inclined port (**Fig. 60**)
- Horizontal port (**Fig. 61**)

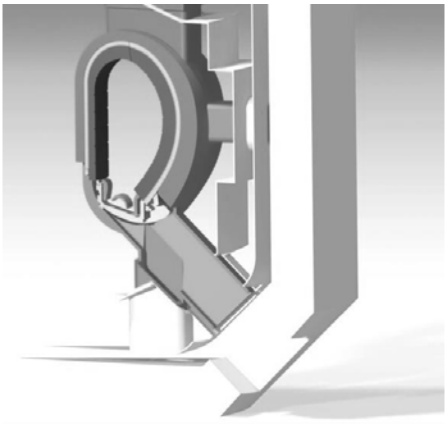


Fig. 60 – DEMO cross section of the 45° lower port configuration

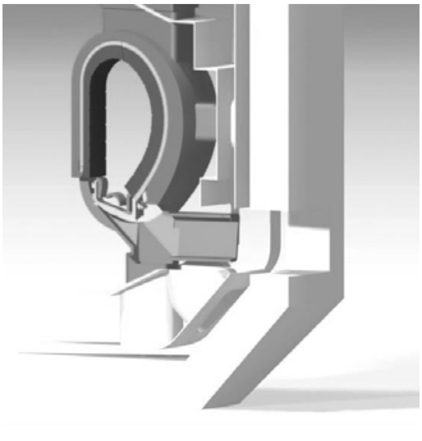


Fig. 61 - DEMO cross section of the Horizontal lower port configuration

In some cases of the early design phase, it is always challenging to assess if a certain configuration is more reliable than a second one. In this example of DEMO RH system development, we have been provided with two tokamak configurations. In the first configuration, the port has a purely 45° angle from the outside of the vessel up to the Divertor area. On the other hand, the so-called horizontal option is actually a partly horizontal section and a 45° section when entering the Divertor area.

In comparison with the complexity of the entire plant design, this port option difference may seem negligible; however, it has an important influence on the design approach of the RH operation and equipment in terms of reliability and costs. Therefore, using the method presented in Chapter 1 offers a way to assess quantitatively if one or another configuration is more relevant to develop further.

The 45° and horizontal configuration of the maintenance port of DEMO plant leads the design to different transfer cask options. For a 45° port, the area where the cask is supposed to be plugged is inclined, whereas in the horizontal configuration, the transfer cask can be plugged horizontally. Now let's consider two cask options for the respective port configuration. A single radial motion transfer cask for the horizontal port configuration, and a 2-function system with a radial and tilting motion for the 45° port transfer cask.

Fig. 62 represents the block diagram option of the Radial motion. This function is needed in both of the options. To perform a radial motion function, the system requires for instance 4 inputs: mechanical features such as rack and pinion mechanism, an electrical engine which also requires an electrical source, and finally some electronic devices for providing position information. This function will have an effect on the transfer cask itself, seen as the mechanical interfaces and its position.

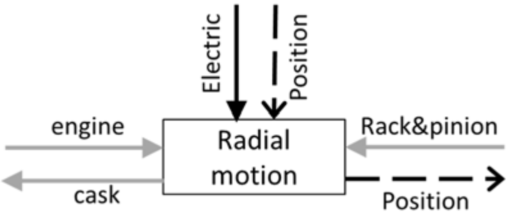


Fig. 62 – Block function diagram of the Radial motion

The second configuration with the 45° port option requires two functions: the radial motion as previously presented and the tilting motion. **Fig. 63** represents the block function diagram of the tilting motion. To be performed, it requires for instance a hydraulic source, and an actuator as the mechanical interface, a valve, as a mechatronic interface in the case of a servo valve for instance, and an electronic interface for the position sensor. This function has an effect on the cask and its position.

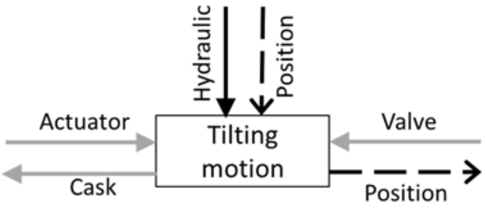


Fig. 63 – Block function diagram of the Tilting motion

The system is considered to have 3 potential functional modes. When the system is in use to perform some operations, it is considered to be in the working mode. When the system is not used during the operation, it is considered to be in a standby mode. And finally, when the system faces some failure in one of its components, it is considered to be in the failure mode. **Table 9** lists the three modes of the transfer cask, and their respective places in the Functional Petri Net representation of the transfer cask (**Fig. 64**).

Table 9 – Functional modes of the transfer cask

Place ID		
Horizontal Port	*45° Port*	*Mode*
P1001	P1004	Standby
P1002	P1005	Working
P1003	P1006	Failure

Fig. 64 gives a functional representation of the transfer cask using a Petri Net model. The initial state of the transfer cask is considered to be in standby mode. When the transfer cask is in use to perform some operations, the variable *TC_working* is set to *true* and the thus the token is transferred to the place *Working*. When *TC_working* is set to *false*, the token is transferred back to the *Standby* place.

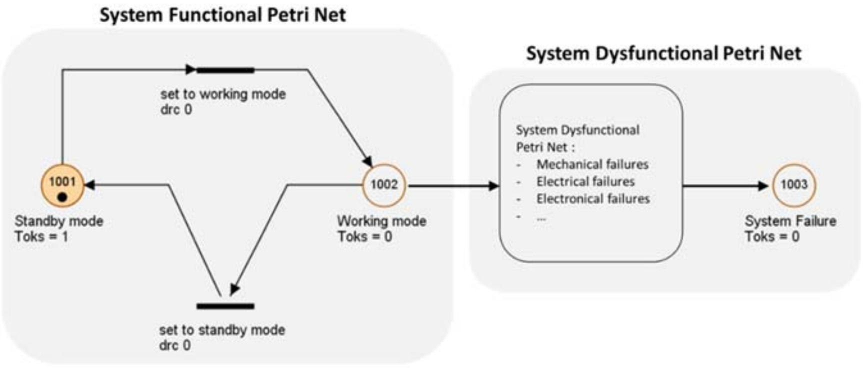


Fig. 64 – Functional and dysfunctional Petri Net representation of a system

The third place is the failure mode, when one or more components face a failure, the system is considered as not operational. The transition between the working mode and the failure mode is described in the next section.

5.8 Dysfunctional analysis

5.8.1 Dysfunctional analysis of two transfer cask options

The dysfunctional analysis aims to evaluate the possible failure modes of the system functions. In this case study, the failure analysis of the radial and tilting motion are listed in **Table 10**. The values and respective distributions are taken from the reliability data base for electronic, electrical and mechanical devices [129, 174-176]. In **Table 10** the mechanical failure mode is associated with Weibull distributions. Electrical and electronic failure types are associated with exponential distributions.

Table 10 – Failure mode of the Radial and Tilting motion function

Function	Component	Failure mode	Reliability distribution	Parameters
Radial motion	Engine	Mechanical	Weibull	β=1,5 η=5000 h
	Rack & pinion	Mechanical	Weibull	β=1,5 η=5000 h
	Electricity	Electrical	Exponential	λ=3x10^{-4} h^{-1}
	Sensor	Electronic	Exponential	λ=3x10^{-4} h^{-1}
Tilting motion	Hydraulic	Mechanical	Weibull	β=1,5 η=5000 h
	Actuator	Mechanical	Weibull	β=1,5 η=5000 h
	Valve	Mechanical	Weibull	β=1,5 η=5000 h
	Sensor	Electronic	Exponential	λ=3x10^{-4} h^{-1}

Fig. 65 represents the functional and dysfunctional Petri net model of the transfer cask in the horizontal port configuration. Only the radial motion function is required to perform the task; therefore, only the four failure modes listed in **Table 9** for the radial motion are represented in the Petri net. The two white transitions represent the exponential distribution of the electrical or electronic failures type. The two black transitions represent the Weibull distribution for the mechanical failure types.

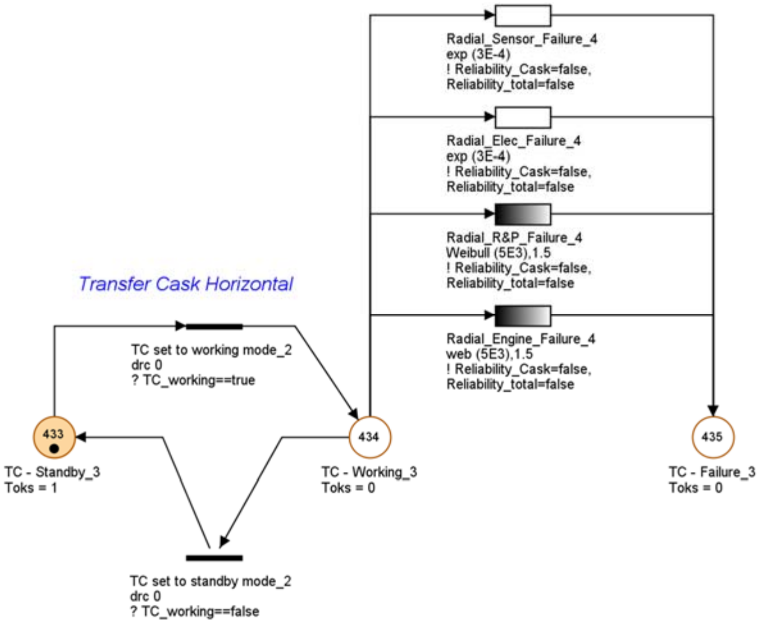


Fig. 65 – Functional and dysfunctional Petri Net of the Horizontal port transfer cask

Each firing of a failure mode transition has an assignment that sets the variable *Cask_failure* to *true*. In this example, only failures that are taken into account are failures happening when the system is in a working mode. Failures that happen during the standby state of the system are not taken into account.

Fig. 66 represents the functional and dysfunctional Petri model of the transfer cask for the 45° port configuration. The failure modes of the two functions (radial and tilting motions) are represented.

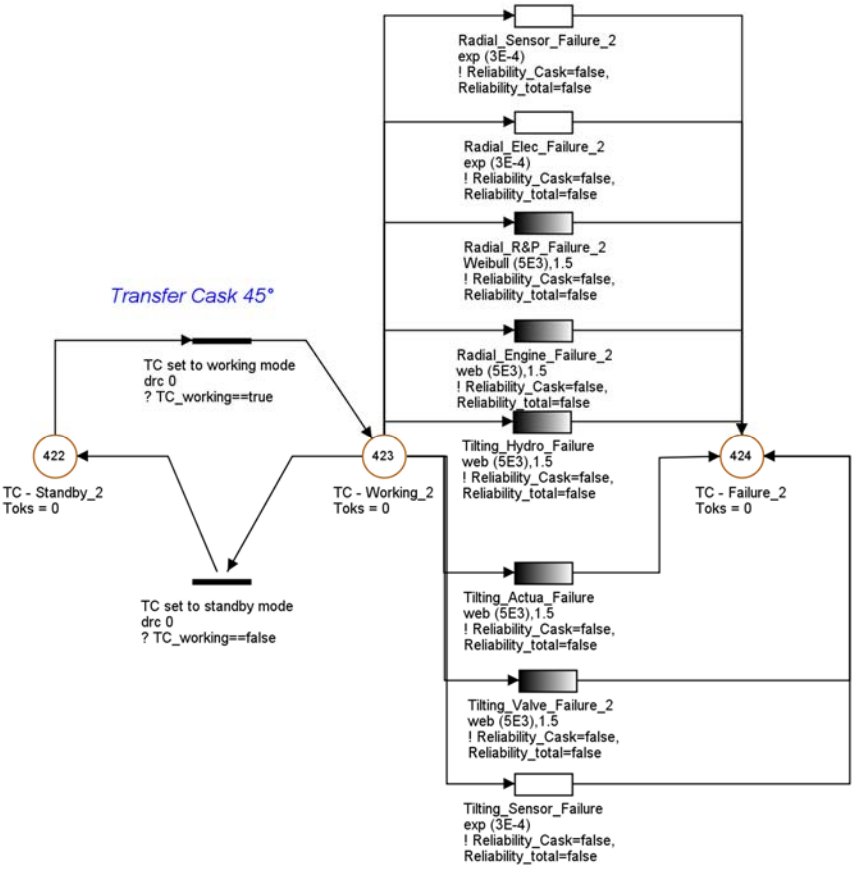


Fig. 66 – Functional and dysfunctional Petri Net of the 45° port transfer cask

Fig. 67 is the comparison of the reliability of the two-cask concept. This graph shows that the reliability of the cask concept for the horizontal port configuration is slightly higher than the cask concept for the 45° port option. For the same operational time, 3600 hours, the average reliability is higher by about 10% in the case of the Horizontal transfer cask concept.

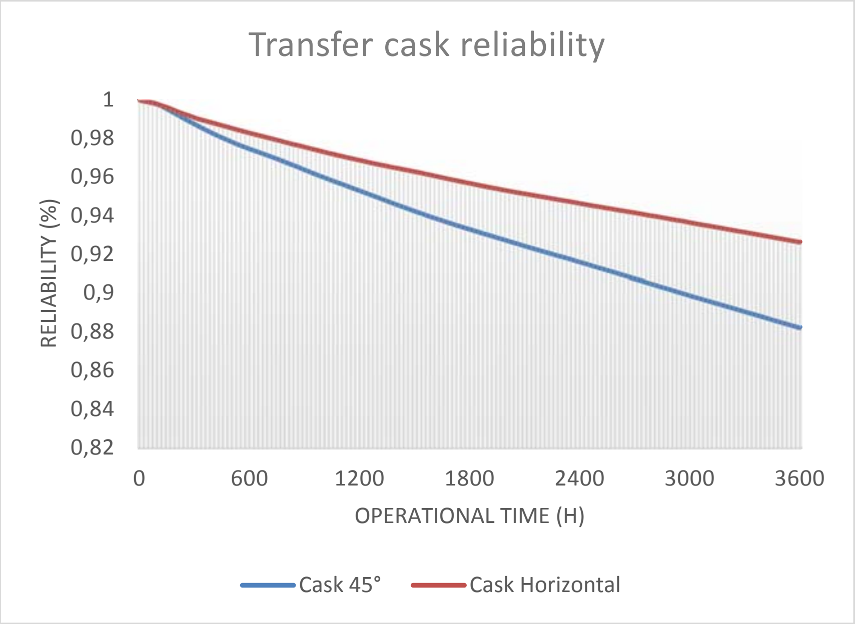


Fig. 67 – Reliability comparison between 45° port and horizontal transfer cask option.

The operational time of the transfer cask is much less than the operational time of the movers, therefore, as expected, cask reliability will have only a slight influence on the overall RH system reliability. **Fig. 68** shows the utilisation rate for each transfer cask in the two different port configurations. The utilisation rate is similar in the two cases and uses about 15% of the maintenance time for removing the 3 Divertor Cassettes.

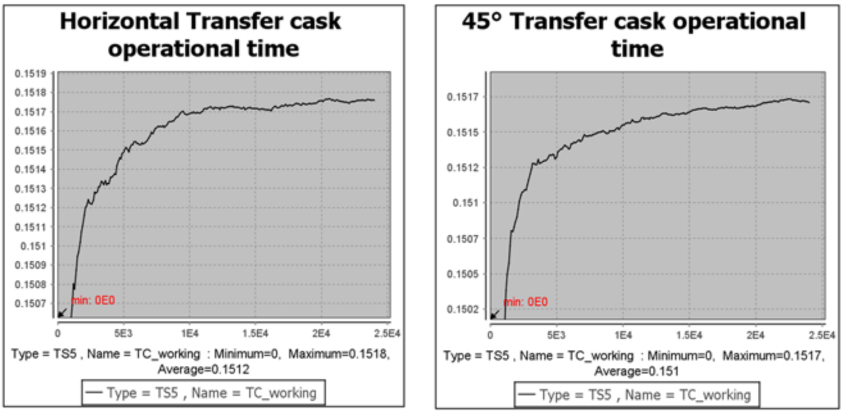


Fig. 68 – Operational time of the transfer cask

5.8.2 Dysfunctional analysis of two mover concepts

In the case of complex systems such as in DEMO, where various systems and sub-systems are needed to perform a task, the full operation strategy has to be simulated in order to compare the reliability of the two port options. Therefore the same approach is performed on the functional level of the two different Cassette movers that will be designed for each port option. As presented earlier in this chapter, the 45° port is a straight port up to the vessel area. However, the horizontal port is a hybrid configuration since it is horizontal in the tunnel area and has a 45° slope before entering the vessel. Therefore, the transfer cask in the horizontal configuration has one less function than the 45° transfer cask, as shown in **Table 11**.

Table 11 – Functional Failure mode of the Mover concept for the 45° port configuration

Functions	Sub-systems	Components	Failure types	Parameters	
Provide radial motion	Radial motion	Engine	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h
		Rack&pinion	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h
		Electricity	Electrical (Exp)	$\lambda=3\text{x}10^{-4}\ \text{h}^{-1}$	
		Sensor	Electronic (Exp)	$\lambda=3\text{x}10^{-4}\ \text{h}^{-1}$	
Provide brakes to enter into a safe state	Brakes	Hydraulic	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h
		Actuator	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h
		Valve	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h
		Sensor	Electronic (Exp)	$\lambda=3\text{x}10^{-4}\ \text{h}^{-1}$	
Provide interfaces to support manipulator and tooling	Linear motion	Engine	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h
		Rack&pinion	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h
		Electricity	Electrical (Exp)	$\lambda=3\text{x}10^{-4}\ \text{h}^{-1}$	
		Sensor	Electronic (Exp)	$\lambda=3\text{x}10^{-4}\ \text{h}^{-1}$	
Provide interfaces to support various end-effectors	End-Eff interface	Mechanical	Mechanical (Weibull)	$\beta=1,5$	$\eta=5000$ h

The petri net models for the two mover concepts (respectively 45° and Horizontal port options) are represented in **Fig. 69** and **Fig. 70**.

Fig. 69 represents the Petri Net model of the failure modes presented in **Table 11** for the 45° port mover configuration. The functional loop happens between place *1007* 'standby mode' and *1008* together with place *1013* set as '*working mode*', while the dysfunctional model corresponds to place *1009-1012.* Respectively *1009* corresponds to the radial motion failure, *1010* relates to the brakes failure, *1011* to linear motion and finally *1012* to the failure of the mechanical interface.

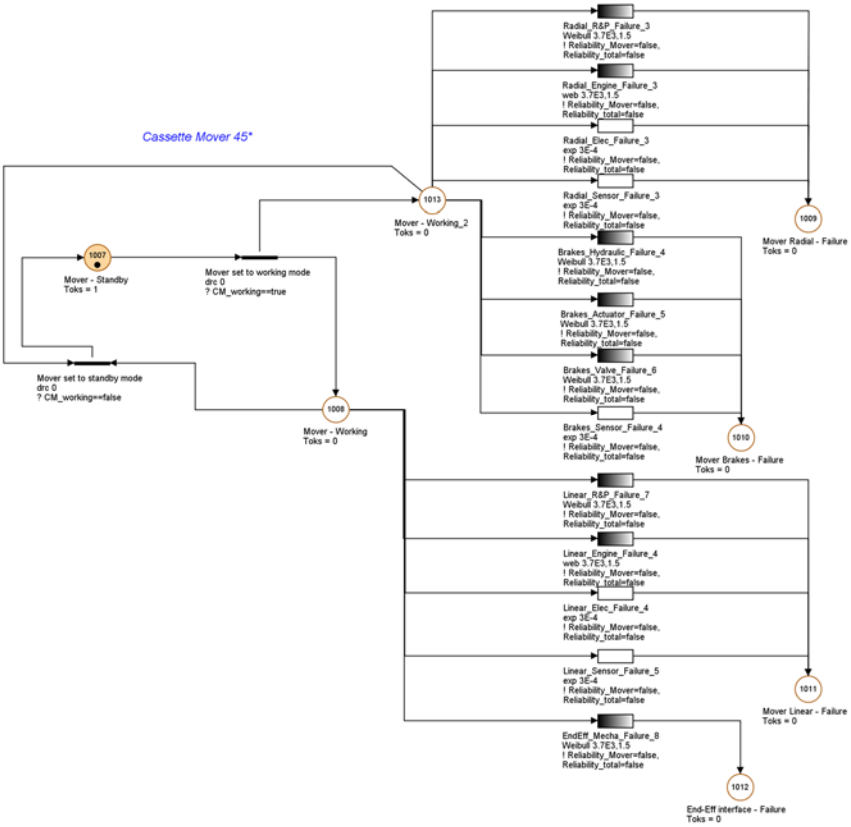


Fig. 69 – Functional and Dysfunctional Petri Net model of the Mover concept for the 45° Port configuration

The mover for the horizontal port needs an additional tilting motion, as shown in **Table 12,** to be able to enter the vessel area compared to the 45° port that is purely straight.

Table 12 – Functional Failure mode of the Mover concept for the Horizontal port configuration

Functions	Sub-systems	Components	Failure types	Parameters
Provide radial motion	Radial motion	Engine	Mechanical (Weibull)	β=1,5 η=5000 h
		Rack&pinion	Mechanical (Weibull)	β=1,5 η=5000 h
		Electricity	Electrical (Exp)	$\lambda=3x10^{-4}$ h^{-1}
		Sensor	Electronic (Exp)	$\lambda=3x10^{-4}$ h^{-1}
Provide brakes to enter into a safe state	Brakes	Hydraulic	Mechanical (Weibull)	β=1,5 η=5000 h
		Actuator	Mechanical (Weibull)	β=1,5 η=5000 h
		Valve	Mechanical (Weibull)	β=1,5 η=5000 h
		Sensor	Electronic (Exp)	$\lambda=3x10^{-4}$ h^{-1}
Provide interfaces to support manipulator and tooling	Linear motion	Engine	Mechanical (Weibull)	β=1,5 η=5000 h
		Rack&pinion	Mechanical (Weibull)	β=1,5 η=5000 h
		Electricity	Electrical (Exp)	$\lambda=3x10^{-4}$ h^{-1}
		Sensor	Electronic (Exp)	$\lambda=3x10^{-4}$ h^{-1}
Provide interfaces to support various end-effectors	End-Eff interface	Mechanical	Mechanical (Weibull)	β=1,5 η=5000 h
Provide tilting motion	Tilting motion	Hydraulic	Mechanical (Weibull)	β=1,5 η=5000 h
		Actuator	Mechanical (Weibull)	β=1,5 η=5000 h
		Valve	Mechanical (Weibull)	β=1,5 η=5000 h
		Sensor	Electronic (Exp)	$\lambda=3*10^{-4}$ h^{-1}

Fig. 70 represents the Petri Net model of the failure mode of the Horizontal port mover configuration presented in **Table 12**. Similar as previously, the functional loop happens between place *1007, 1008* and place *1013*, while the dysfunctional model corresponds to place *1009-1012.* Respectively *1009* corresponds to the radial motion failure, *1010* relates to the brakes failure, *1011* to linear motion and finally *1012* to the failure of the mechanical interface. However, place *1014* corresponds to the failure mode of the tilting motion which is not present in the 45° port mover configuration.

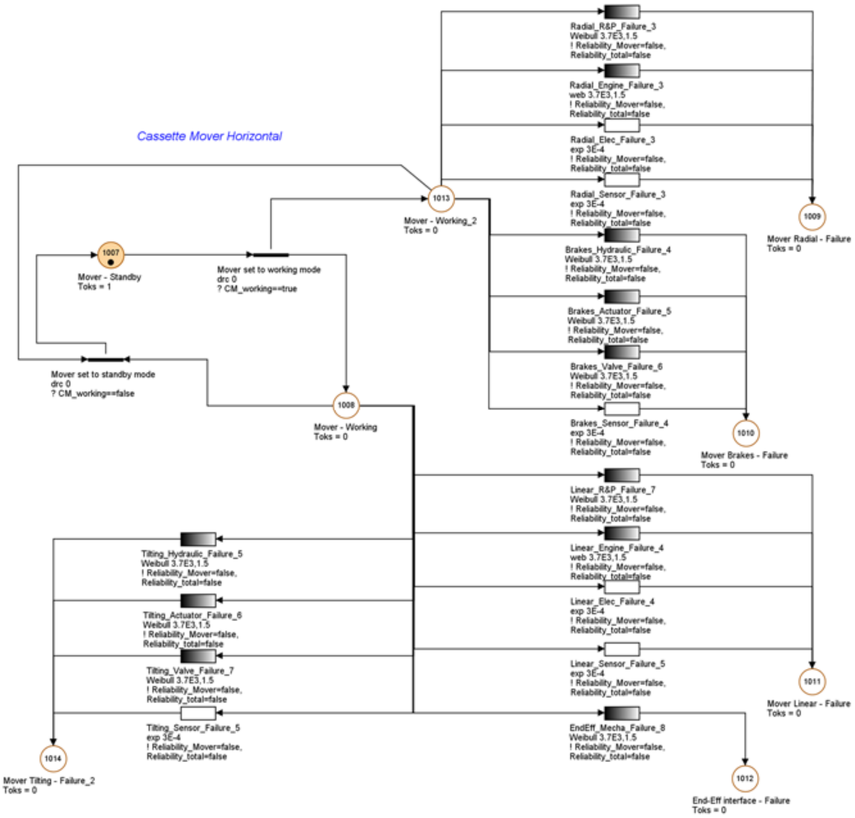


Fig. 70 – Functional and dysfunctional Petri Net model of the Mover concept for the Horizontal Port configuration

The predictive reliability for the two different movers is shown in **Fig. 71**. The mover concept for the horizontal port option has a slightly lower reliability than the 45° port mover concept, which is due to its extra tilting function, which obviously increases it failure probability.

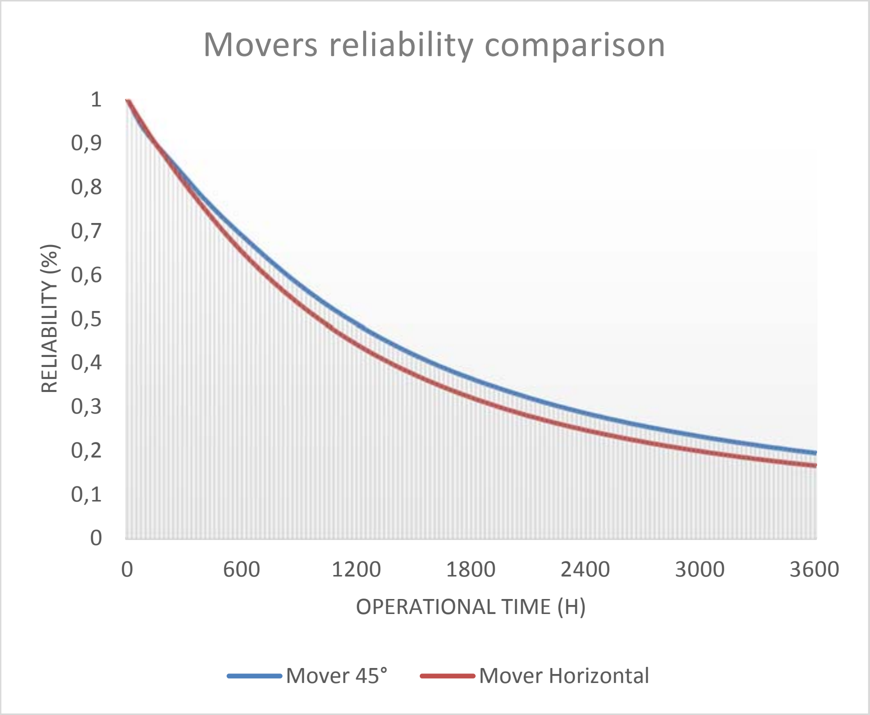


Fig. 71 – Predictive reliability for the two mover concepts

The reliability of the 45° port mover concept has up to 5% greater reliability than the horizontal port mover concept after 1 800 hours of operating time. After 3 600 hours, the difference is about +3% greater. As expected the 45° port mover is slightly more reliable than the horizontal mover concept. However, the difference is not very significant and other systems reliability have to be combined together in order to evaluate the overall RH concepts reliability.

5.8.3 System reliability comparison

Taking into account the respective transfer cask and mover reliability for each port configuration, **Fig. 72** shows the reliability comparison between the remote maintenance concepts for the 45° and the Horizontal ports. The 45° Port concept offers a slightly higher reliability than the Horizontal port options.

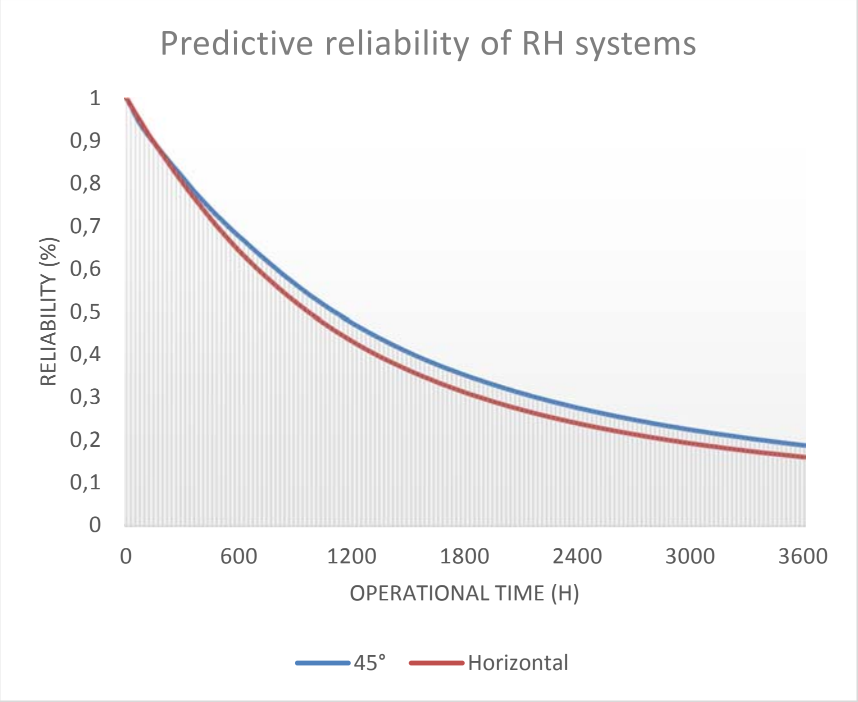


Fig. 72 – Comparison of the reliability of the RH systems (mover and cask) concept for the two port configurations

5.9 Environmental factors

Environmental factors can have an influence on the reliability of components and thus of the parent systems and sub-systems. However, in many cases, environmental factors are not constant over the operating time and fluctuate according to the phase of the operation. For instance, in the maintenance operation of the Divertor in DEMO, the radiation level is different in the hot-cell area than in-vessel. Therefore, the remote handling devices are subjected to different levels of radiation regarding the phase of the operation. It is similar for the temperature factor. The temperature of the environment is different depending on whether the system is located in the hot-cell or in-vessel. Those criteria may have considerable effects on the system reliability [177]. Moreover, each component may exhibit different behaviour when subject to radiation (**Fig. 73**) or temperature. In the case of a complex system, it is hardly possible to evaluate the influence of the radiation on the reliability of the parent system.

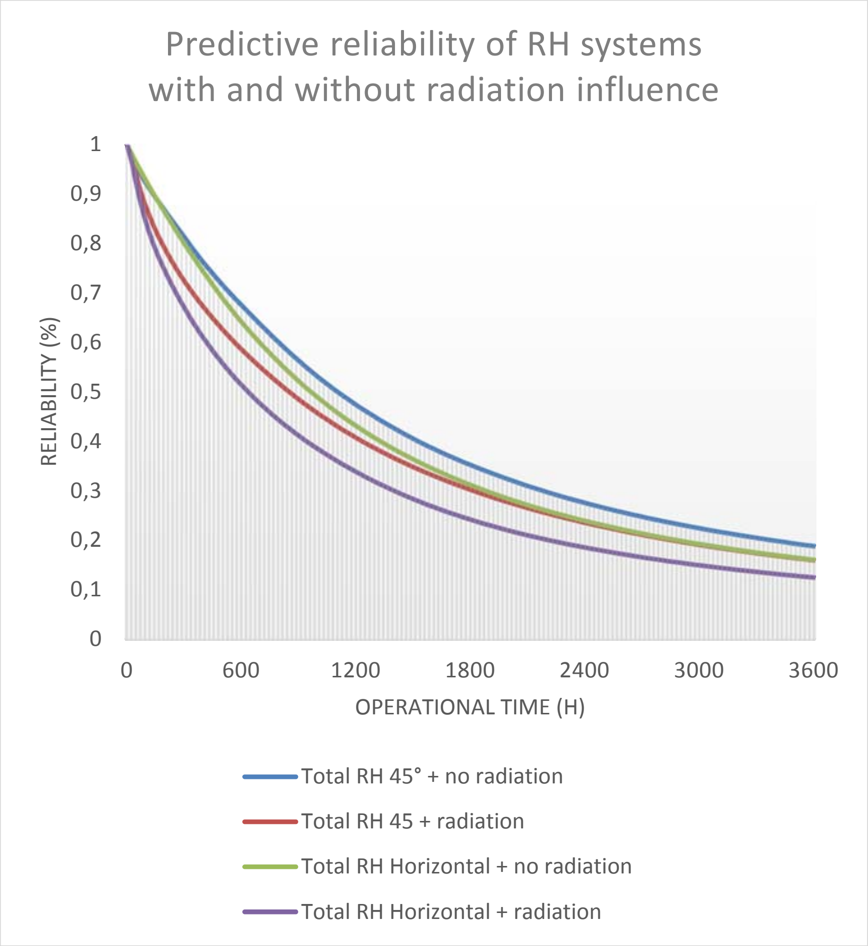


Fig. 73 – Influence of radiation factor on overall RH systems reliability

Therefore, the developed Petri Net based approach enables us to take into consideration the effects of the environmental factors on the reliability of components and thus on the reliability of the parent system. Different concepts may be evaluated against each other based on their reliability as influenced by environmental criteria, such as temperature or radiation.

As an example, in the following case study (**Fig. 73**), the radiation criteria has been taken into account in order to evaluate the influence of the radiation, where the effect of radiation leads to a decrease by a factor of two in the reliability of each component. In the Petri Net dysfunctional model of the CMM, a radiation variable has been implemented and divides by 2 the reliability of each component of the mover when entering the vessel area. However, when the mover is in the transfer cask, the radiation level is set to 1 and thus does not affect the reliability of the components.

5.10 Result analysis

This chapter has shown the application of the developed method on an actual complex case study. The DEMO maintenance operation has been used as the discrete event dynamic system and the functional and dysfunctional model of two RH system configurations have been modelled. The comparison of the two configurations has shown that even if the 45° transfer cask was less reliable than the Horizontal cask, the total reliability of the combination of cask and mover demonstrated a higher reliability for the 45° configuration. Therefore, this analysis has shown that the method is suitable for simulating a single system as well as a combination of complex systems.

The next phase for this case study is to model the full maintenance sequence together with the full set of systems required to perform these operations. In such a case, the evaluation of the maintenance strategy would be highly relevant for the decision-making process to decide whether the 45° port configuration tends to be more reliable strategy than the horizontal port configuration.

Finally, the implementation of arbitrary environment factors such as the radiation has been simulated. It was considered that the radiation decrease by a factor of two in the reliability of the component of the mover when it reached the in-vessel area. However, it is important to notice that this value does not represent the reality, but aims only to show that environmental factors can be implemented in this method. Results have shown that such environmental factors may influence the decision-making process, since different system combinations or maintenance strategies can be considered.

6 CASE STUDY 2: RELIABILITY-BASED METHOD FOR SYSTEM EVALUATION

This chapter describes the application of the method of a more advanced system in terms of detail level. The case study used in this chapter is the Cassette Multifunctional Mover (CMM) for the ITER Divertor remote maintenance. This system is already built as a prototype and currently in the physical testing phase. The first part of this chapter introduces the environment of the case study, the ITER project. The second part introduces the CMM itself and its different sub-systems and components. The third section of this chapter focuses on the dysfunctional analysis of the CMM. Finally, Section 6.4 summarizes the results obtained from the comparison of two potential CMM concepts applied in DEMO maintenance environment.

6.1 Description of the case study: ITER RH system for the Divertor maintenance

Due to the erosion of plasma facing components the replacement of the Divertor and its refurbishment in the hot-cell is foreseen 4 times during the ITER lifetime. The Divertor handling concept is based on various elements: the Divertor segmentation into 54 cassettes, three dedicated access vacuum-vessel ports at Divertor level located at 120° apart from each other, the cassette multifunction-mover (CMM) system, the cassette toroidal mover (CTM), the pipe tools, the transport casks and double-door and the control system [178].

The radial transport of the cassettes through the 3 Divertor RH ports is carried out by the Cassette Multifunctional Mover (CMM) (See **Fig. 74**), which is a multi-degree-of-freedom hydraulic robot used for the remote handling maintenance of the fusion reactor ITER. It includes different domains of technology such as mechanical, hydraulics and automation, control system, electrical and electronic domains. This system has been developed over many years, and various international institutes have taken part in the design of the system. A physical prototype (**Fig**. **75**) has been build and is currently being tested in VTT Technical Research Centre of Finland Ltd [35].

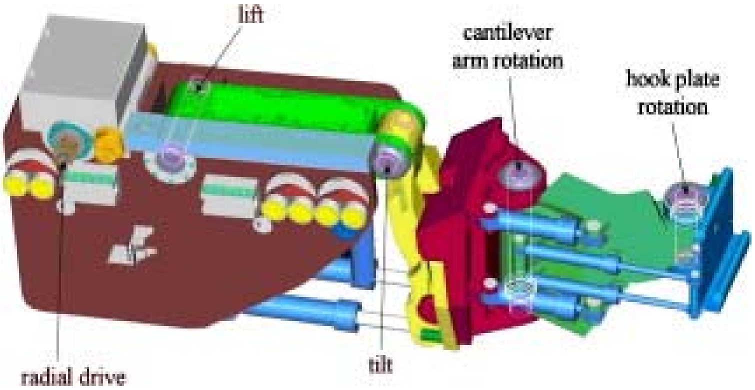


Fig. 74 – Cassette Multifunctional Mover in the ITER Virtual Mock-up [179, 180]

The purpose of this system if to carry a heavy component located inside the ITER fusion reactor. The ITER machine is made up of 54 Divertor cassettes way 9 tons each that cover 360° of the in-vessel fusion reactor floor. There are three maintenance access ports at the bottom of the reactor vessel. For each maintenance port, 18 cassettes are planned to be removed. To transport the cassettes out of the vessel, there are two different types of remote control devices called cassette movers. One is acting in a radial way fashion the maintenance tunnel access and the second one is acting in the toroidal way inside the vessel. The device that is used in this study is the Cassette Multifunctional Mover (CMM) that operates along the radial axis, used to extract the cassettes through the 3 maintenance tunnels. For the cassette removal operation, the CMM grabs the central cassette located in the axis of the maintenance tunnel access. The CMM together with its integrated manipulator release the preloading and locking system of the cassette in order to extract the Divertor cassette through the maintenance tunnel. When the central cassette is removed, the CMM is equipped with an end-effector, the so-called Second Cassette End-Effector (SCEE) (**Fig. 75**), which is used to grab the second cassette located on the side of the maintenance access port. It grabs the second cassette and moves it toroidally to orientate it toward the tunnel maintenance port in order to be removed.

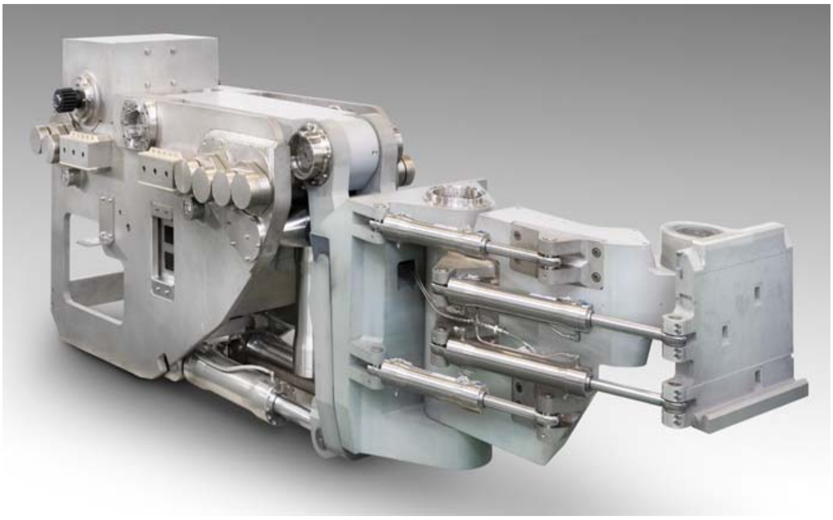


Fig. 75 – Cassette Multifunction Mover and Second Cassette End-Effector physical prototypes [179, 180]

The design challenges related to this mover are extremely high due to the minimal clearances between the cassette and vacuum vessel port. The most important factor for ITER RH systems is reliability [181]. The Divertor maintenance operation should be fully reliable. It is considered as a remote handling Class 1 operation, which means that the design of the Divertor RH system must be verified and validated by proof-of-principles and full-scale mock-ups/prototypes. Therefore the DTP2 platform aims at answering this ITER requirement [182]. Beside testing the Divertor maintenance operations and developing operational tasks, the DTP2 facility is used to verify and improve the design of the Divertor components.

The CMM is a fairly complex mechatronic system that has been developed over many years among research centres and is now in the physical testing phase. During its design phase, starting with a list of high level requirements, the design has evolved throughout different phases which represented different levels of design (concept, detailed, engineering and final); many evolutions of its design have been proposed. The purpose of using this case study in this thesis is to use this 10 years of experience required to develop the latest version of the Divertor Maintenance system. This experience is particularly helpful in order to improve the current design process in use, in the first instance in the fusion engineering field, but also in industries such as airplane, automobile and other complex engineering and manufacturing sectors.

For more than 20 years now, different concepts have been developed, virtual concepts as well as physical concepts. **Fig. 76** shows the evolution of the radial mover concepts between ITER 1998 and ITER FEAT, which were two different ITER fusion reactor concepts [183].

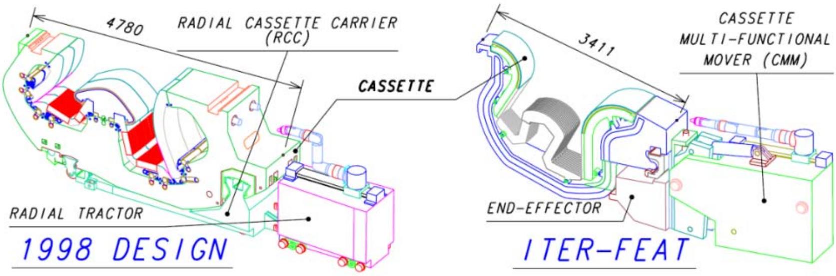

4780
RADIAL CASSETTE CARRIER (RCC)
CASSETTE
RADIAL TRACTOR
1998 DESIGN
3411
CASSETTE MULTI-FUNCTIONAL MOVER (CMM)
END-EFFECTOR
ITER-FEAT

Fig. 76 - Radial mover concepts, evolution between the 1998 design and ITER FEAT [184]

Fig. 77 shows the ITER CMM concept in the early 2000s equipped with a second cassette end-effector and a manipulator arm.

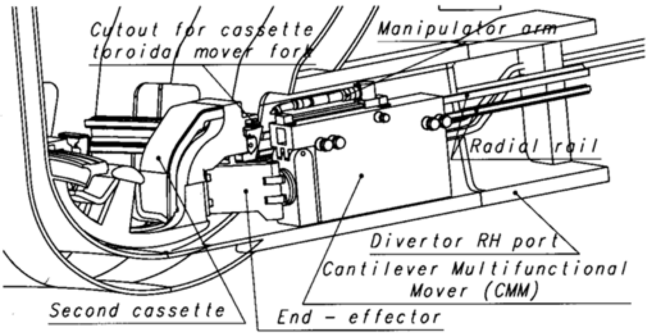

Cutout for cassette toroidal mover fork
Manipulator arm
Radial rail
Divertor RH port
Cantilever Multifunctional Mover (CMM)
Second cassette
End - effector

Fig. 77 – Cassettes are installed on the in-vessel toroidal support rails using the cantilever multifunctional mover (CMM) [185]

The design of the CMM has been radically changed over the years. Requirements have been changed throughout the evolution of the research in all related fields, which led to constantly updated designs to meet to requirements changes.

The CMM is used for the insertion and extraction of the Divertor cassettes from the vacuum vessel along the maintenance tunnel to the transfer cask docked at the maintenance port. The following paragraph lists two levels of requirements: high level requirements for the Divertor remote handling system and the system level requirements oriented towards the CMM itself. The Divertor Remote Handling (RH) System should provide the means for remote replacement of the ITER Divertor System [186-188].

6.2 ITER Cassette Multifunctional Mover applied to DEMO maintenance

In this section, we consider the latest ITER CMM design applied to the DEMO maintenance operational sequence. Let's consider that the level of design of the DEMO cassette mover has evolved towards a more detailed concept, such as the existing CMM device for ITER (**Fig. 78)**. Obviously, the actual CMM design cannot fully satisfy the full set of DEMO requirements, however, it is interesting to know how the developed method can be applied to a detailed system that is already at the physical prototyping and testing phase.

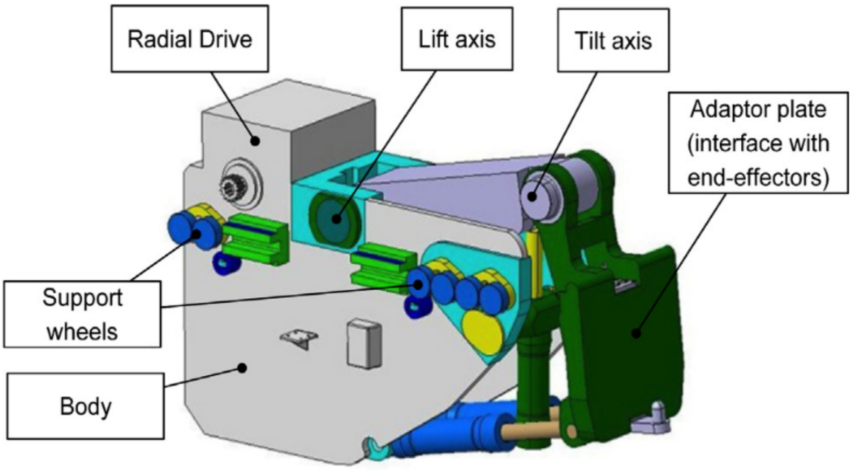


Fig. 78 – Sub-systems of the Cassette Multifunctional Mover for ITER Divertor Maintenance

The discrete event dynamic system of the DEMO maintenance operational sequence is used together with the discrete functional model of the CMM at a component level. The system and sub-system of CMM are modelled as a functional and dysfunctional stochastic Petri Net, and implemented into the DEMO maintenance operational sequence PN.

The CMM system consists of five main sub-systems: Body, Radial Drive Unit, Wheel assembly, Lifting system, and Tilting system. Below is a description of each sub-system.

- *Body*

The CMM body is the structural connection point for all the major load-bearing sub-systems.

- *Radial Drive Unit*

The radial drive (RDR) provides the radial motion of the CMM along the radial rails from cask to reactor (**Fig. 79**). The radial drive is based on a rack and pinion system driven by two servomotors running two pinions, one each side of the CMM. Two racks are installed on rails along the sides of the radial tunnel. The RDR contains two similar servomotor/gearbox sub-systems. During normal operation both servomotors are used to drive the CMM in parallel. However, if one motor fails the other is sufficiently powerful to drive the system as normal. Brushed DC servomotors have been chosen to allow for simple open loop control during system recovery. The motors include a tachometer and a holding brake.

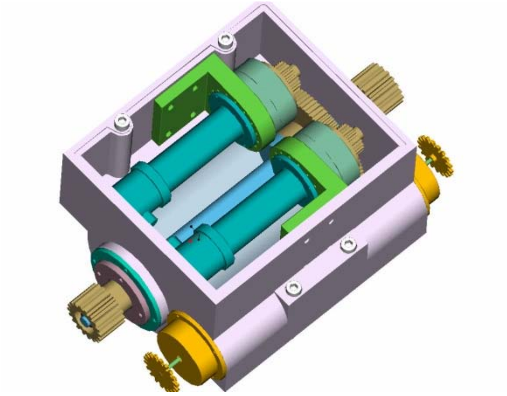


Fig. 79 – CMM Radial Drive Unit

- *Wheel assembly*

The CMM moves from the cask to the reactor along radial rails. The weights of the CMM and its components as well the Divertor Cassette are carried entirely on the CMM wheels. The CMM wheels are arranged in units comprising a 2-wheeled bogie as shown in **Fig. 80**. A minimum of four wheels on each side is required at the front of the CMM and two on each side.

Therefore, there are 3 wheel-subassemblies that contain 2 wheels each, so 6 wheels on each side of the CMM. Each wheel has a roller bearing, while each wheel-subassembly is connected to the main body with a roller bearing. A total of 18 bearings are used for the CMM wheel system.

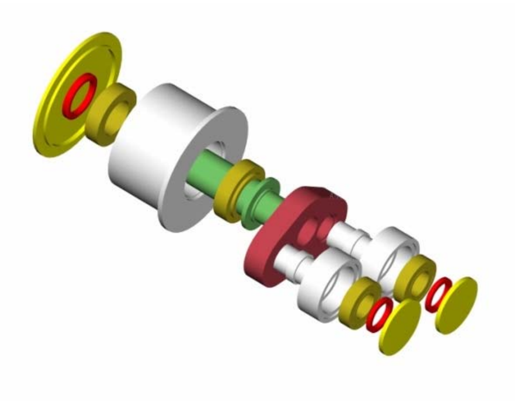


Fig. 80 – The two-wheel bogie design

- *Lifting system*

The lift arm is a beam connected to the CMM body at its rear end. The lift cylinder is connected in the middle of the lift arm. The tilt arm is connected to the front end of the lift arm. The lift arm is connected to the CMM body with two highly preloaded tapered roller bearings. The bearings are mounted in housings that are inserted into the CMM body. The Lift cylinder is connected to both sides of the CMM body via a yoke mounted on spherical slide bearings. The cylinder rod is connected to the lift arm with a slide bearing which forms part of the cylinder rod end. A dual speed resolver is used between the lift arm and CMM body. The hydraulic actuators require very precise positioning and therefore need to be position controlled with servo valves.

- *Tilting system*

The tilt arm is a metallic structure integrating the adapter plate for the end-effectors, connection to tilting system and interfaces for two tilting cylinders. The tilt arm is connected to the lift arm at its top end. Two tilting cylinders support the lower end of the tilt arm. The cylinders producing the tilt motion are connected in parallel and driven with one servo valve. The rear ends of the tilt cylinders are connected to a block which is bolted to the CMM body. Tilt cylinder rods are connected to the lower end of the tilt arm. The joints at the end of both tilt cylinders have spherical slide bearings. The position of the tilt axis is measured by a resolver mounted coaxially with the link joints, i.e. the joint between the lift arm and the tilt arm. Similar to the Lifting system, the hydraulic actuators are controlled with servo valves.

6.3 Dysfunctional analysis of ITER CMM

In this case study, the original configuration of the CMM is used and compared with a modified CMM configuration using electrical motors instead of hydraulic cylinders for the actuation of the lifting and tilting system.

In the event the failure distribution for a particular component is unknown, such as for structural mechanical parts or software and electronic components, some standard distribution parameters can be used. **Table 13** gives the standard distribution parameters for electronic, mechanical and software components, based on [176, 189].

Table 13 –Standard distribution parameters

K	Component	Distribution	Parameters
1	Electronic	Exponential	λ=3x10^{-4} h^{-1}
2	Mechanical	Weibull	β = 1,5 and η=5000 h
3	Software	Exponential and Jelinski-Moranda	N$_0$=70; φ=3x10^{-6} h^{-1}

This means that the assumed underlying time-to-failure distribution for all failure rates presented in NPRD-91 is the exponential distribution. Unfortunately, many part types for which data are presented typically do not follow the exponential failure law, but rather exhibit wear out characteristics, or an increasing failure rate over time.

The common parts of the CMM configuration, whether it is actuated hydraulically or electrically are listed in **Table 14**. In this case, when one component is entering into a failure mode, the whole system is considered as failed. However, in a real situation the number of wheels and their respective bearings for instance are many times redundant, thus the failure of one component usually does not lead to the failure of the entire system. Nonetheless, for a notion of simplicity, in the following simulation, the failure of one component will lead to the failure of the whole system.

Table 14 - CMM components and failure distribution parameters based on [174]

Sub-systems	Components	number	Failure distribution	Parameters
CMM Body	Body	1	Mechanical (Weibull)	β = 1,5 and η=5000 h
Wheel assembly	Support	6	Mechanical (Weibull)	β = 1,5 and η=5000 h
	Wheel	12	Mechanical (Weibull)	β = 1,5 and η=5000 h
	Bearing	18	Mechanical (Exponential)	λ=1,37x10^{-6} h^{-1}
Radial Drive Unit	Rack	2	Mechanical (Exponential)	λ=1,76x10^{-6} h^{-1}
	Gear	3	Mechanical (Exponential)	λ=14,3x10^{-6} h^{-1}
	Brush servomotors	2	Electrical (Exponential)	λ=18,13x10^{-6} h^{-1}
	Gearbox	3	Mechanical (Exponential)	λ=7,12x10^{-6} h^{-1}
	Sensor (tachometer)	2	Electrical (Exponential)	λ=2,1x10^{-6} h^{-1}
	Brakes	2	Mechanical (Exponential)	λ=100,4x10^{-6} h^{-1}
	Bearing	2	Mechanical (Exponential)	λ=1,37x10^{-6} h^{-1}

On the other hand, the two sub-assemblies that are different from one configuration to the other are the Lifting system and the Tilting system. In **Table 15**, lines highlighted in red are the original hydraulic cylinder components and the blue lines are its equivalent for electrical actuators. Component failure distributions and their respective parameters have been taken from the data source NPRD-91 [174]. It is important to notice that if a shape parameter, β, of the Weibull distribution is known for a particular component or assembly, the exponential parameter provided by NPRD-91 can be used to extrapolate the average failure rate to a Weibull characteristic life (x). However, if the percentage failure rate is relatively low, the methodology is of limited value.

Table 15 - CMM components (*suite*)
(*red*: hydraulic configuration; *dark blue*: electrical CMM)

Sub-systems	Components	number	Failure distribution	Parameters
Lifting system	Lift arm	1	Mechanical (Weibull)	β = 1,5 and η=5000 h
	Taper roller bearing	7	Mechanical (Exponential)	λ=1,37x10^{-6} h^{-1}
	Cylinder (Servo-valve)	1	Mechanical (Exponential)	λ=130,4x10^{-6} h^{-1}
	Sensor (Resolver)	1	Electrical (Exponential)	λ=1,3x10^{-6} h^{-1}
	Electrical Motor	1	Mechanical (Exponential)	λ=0.047x10^{-6} h^{-1}
	Sensor (Tachometer)	1	Electrical (Exponential)	λ=2,1x10^{-6} h^{-1}
	Tilting arm	1	Mechanical (Weibull)	β = 1,5 and η=5000 h
Tilting system	Cylinder (Servo-valve)	2	Mechanical (Exponential)	λ=130.4x10^{-6} h^{-1}
	Sensor (Resolver)	1	Electrical (Exponential)	λ=1.3x10^{-6} h^{-1}
	Electrical Motor	2	Electrical (Exponential)	λ=0.047x10^{-6} h^{-1}
	Sensor (Tachometer)	1	Electrical (Exponential)	λ=2,1x10^{-6} h^{-1}
	Bearing	2	Mechanical (Exponential)	λ=1.37x10^{-6} h^{-1}

Basically, the number of components for one CMM configuration to another is similar. However, reliability parameters associated with these components are consequently different.

6.4 Results of the case study

The comparison of two CMM configurations in the case of DEMO Divertor maintenance scenario has been performed based on the developed reliability Petri-Net approach presented earlier in this thesis.

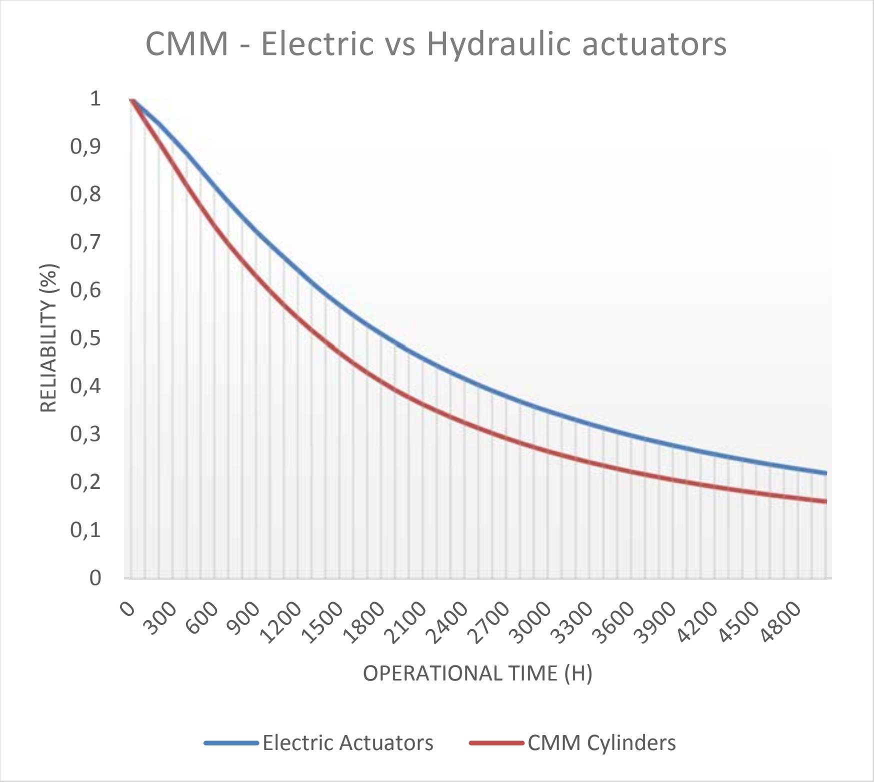


Fig. 81 – Reliability comparison between electrically or hydraulically actuated CMM

Fig. 81 shows the evolution over time of the reliability of the two CMM configurations performing the DEMO Divertor maintenance operation. In this case study, results show that the CMM actuated with electric motors and their respective sensors are more likely to be about 10% more reliable than the initial CMM configuration after 2 000 hours of operational time and about +6% more reliable after 5 000 hours of operational time.

However, in this case study, environmental factors have not been taken into account, such as the effects of radiation or temperature on the reliability behaviour of the systems and their components. Radiation will have a different influence on electrical components than hydraulic components.

7 DISCUSSION

This chapter discusses the theoretical implications of the method and its implementation within the systems engineering approach using two main case studies. As well, this chapter discusses the practical applications of the method together with its limitations and perspectives.

True to the form of an exploratory study, the state of the art in the field of complex systems design showed the need to develop advanced methods for the design verification based on system reliability. Reliability is one of the most important requirements in many industrial activities and become a central part of the decision-making process.

In addition, to support the decision-making process, a quantitative reliability-based evaluation method has been implemented to provide more objectivity to the decision-makers. The development of the method has been based on the best practices from research and industries and has been modelled using a simple example, the pendulum system, as well as two fairly more complex case studies, related to fusion activities and in particular DEMO remote handling systems, in two different phases of the design process. These case studies have been chosen because they are well representative of two main phases of the design process, the conceptual design and the engineering design phases.

The discrete dynamic event system that basically aims to represent the operational strategy of the system has been presented and modelled as a high level stochastic Petri Net. It was chosen to set the transitions with logarithmic distributions to represent the duration of each operation on a scale from 1 to 5 for more objectivity when actuall durations are not available at this stage of the design. Indeed, scale one considers a one-hour (±1h) operation duration while scale 5 considers a 6.5 days (±3 days) operation duration. In this case, the fuzzy logic used to represent the operational time helps to homogenize expert's opinions according to the estimated operation's durations. Especially in the concept design phase, it is usual that operational time remains an abstract data. The scale range can be adjusted regarding level of operational sequences and the degree of knowledge on these operations. In the case that operational durations are well known, the fuzzification is therefore not needed and transitions can be set with fixed time delays.

Two case studies have been used to demonstrate that the method is applicable in different phases of the design process, namely the concept design and engineering design phases. The functional models of both case studies have been presented and implemented in the discrete dynamic event system of the maintenance procedure. In the first case study, the failure distributions of sub-assemblies have been collected and implemented in the functional Petri net models of the two concepts. The comparison was then possible since both concepts were on the same design level. As expected, results showed that the overall reliability of the 45° inclination option was likely to be higher than the horizontal concept option.

DEMO remote maintenance operational sequence has been used for performing the simulations in this study. The requirements analysis phase and the development of the concept design used in the thesis have been adapted for this research work. Therefore, it does not represent exactly the reality of the DEMO RH project. However, the method demonstrated in this thesis aims to be used as part of the DEMO RH system development in the coming years if the benefits are significant enough. In DEMO, as with any other complex systems, many criteria have to be taken into account in the decision-making process during the design process. In this thesis, only reliability has been evaluated as the main criteria. But for instance, it is possible to implement many other criteria such as system availability, severity of the failures, operational time, recoverability and operational cost of the system. This applies as well to the environmental parameters that may influence the behaviour of the developed system. In this thesis only radiation effect as an arbitrary criterion has been taken into account. Additionally, if more knowledge is available on the effect of the radiation on components or sub-systems, the method can be refined according to the level of radiation encountered at each step of the operational sequence. For instance, temperature, dust or stress in the components can be also implemented as environmental parameter that would have an effect on the behaviour and reliability of the system. With this method, it is also possible to have an overview of critical components of a complex assembly, in order to decide whether redundant components are needed or even a re-design. The most critical operational phases can be highlighted using this method and appropriate measures can be considered.

Stochastic Petri Net method has been chosen because of its ability to connect various aspects of a system, such as its overall operational strategy as an event driven sequence, as well as the functional and dysfunctional behaviour of the system. The implementation of continuous Petri Net may offer significant benefits for modelling continuous environmental parameters such as the influence of radiation or temperature when these variables are not event-state limited. However, in the presented research work, the implementation of continuous variables has not been tested but seems to be a promising improvement of the method towards more efficiency. Additionally, the type of distribution to represent the probability of failures of a component can behave drastically different regarding the type of operating environment. The effect of radiation on the overall system is usually very challenging and further studies are needed to determine the influence of environmental parameters and their combinations (radiation combined with temperature for instance) on component reliability distributions.

A second theoretical implication of the method consists in the functional and dysfunctional representations of the system. The functional side of a system is represented as an event-state model, and only three states of the system were considered, namely stand-by state, working state and failure state. Likewise, the failure state could be only reached if the system was in a working mode. Accordingly, failures that could possibly happen during standby modes of the system were not taken into account because it has been considered that based on the case studies, standby mode failures were not sufficiently significant for influencing the overall results of the study.

Overall system reliability is mainly driven by the probability of failures of its subsystems and components. However, the reliability relationships between components is a relevant query. Using the functional block diagram approach helps to identify the degree of relationship between components, but the explicit effect of the failure of one component to other components and thus to the overall system remains challenging. The method presented in this dissertation considers that when a component fails, the overall system enters into a failure mode. However, in real situation, the overall system may still be functional even if a non-critical component has entered in a dysfunctional state. More development is obviously needed in order to take the reliability relationship between components into account and thus improving the method for more accuracy.

The results presented in the thesis regarding reliability have been kept general without reference to any particular field and are equally applicable to any range of industrial applications. Furthermore, it has been kept in mind during the elaboration of this thesis to retain the findings useful for other developments in order to continue the research and discussion on a wider scale. However, due to the ongoing project at the time of the elaboration of this thesis and the material available, fusion related remote handling systems have been used as the main case studies.

This research work has shown that stochastic Petri Net is an adequate modelling tool to be used for verification-based design process which can result in improving the decision making process and thus the efficiency of the entire design process for complex systems development. The iterative aspect of the method as well as the results obtained by the analysis of the two case studies showed that the method is relevant on every phase of the design process for system design, verification and optimization

Other perspectives for further research, especially regarding fusion power plants, would be to investigate the implementation of RAMI analysis parameters (Reliability, Availability, Maintainability and Inspectability). For instance, the overall availability of a power plant is essential to insure the competitive cost of electricity. Therefore, the optimum duration of the planned maintenance is determined by balancing the cost of a faster remote handling system with the cost of reduced power plant availability for generating revenue. The method presented in this dissertation could be an efficient tool to lead the design of maintenance systems towards an optimum balance between system reliability, maintainability and overall plant availability. Towards a wider scope, availability is also an essential criterion for an extensive range of industrial applications.

One additional criteria that disserves to be further investigated in this approach is the degree of recoverability of a system. Since system recoverability directly influences the overall system availability, the degree of recoverability is essential to assess whether one concept enables a higher overall system availability than another.

In order to answer the research question of the thesis, based on the results that have been established during this research work, it can be concluded that product confidence can be improved by using a reliability-based design process from the very early phases. Stochastic Petri Net approach offers a powerful solution for modelling various system behaviours that interact which each other. The iterative and quantitative nature of the method leads the design towards the most reliable solution and reduce the risk of design errors (based on customer needs) from the very early phase. Product development time is therefore shortened and design costs are also reduced by avoiding multiple product or prototype iterations.

It has been clearly shown that this method takes into account many system-relevant parameters, such as operational time according to level of design and environmental factors that demonstrates the quantitative aspect of the evaluation method when comparing various system designs in similar environment. The method has proven that the product confidence can be increased by collecting system information from the very early phases and therefore constantly evaluating the system behaviour against system requirements. As stated, the decision-making process is enhanced due to the objectivity of the method for concept design comparison at any phases of the design process.

The discrete event dynamic system remains the same when comparing different design and whenever modifications are applied in it; it applies automatically to every previously evaluated concept, there is no need to remodel it, it can simply be connected to another case study. Therefore, it makes the simulation a powerful tool for driving the design using reliability as the main criteria.

Based on the research reported in this thesis and the above discussions, suggestions for future research are summarized below:

- Method implementation is of primary importance since no software is currently available for applying such a method. It is important to notice that the more the system evolves towards a complex assembly, the more laborious the modelling work becomes. Therefore, by creating a toolbox and library of components to reuse pre-made component functional Petri net models would lead to an avoidance of cumulative errors and modelling inconsistencies.

- Implementing various kind of parameters that would influence the behaviour of the developed system, with a more user-friendly interface, would ease the modelling process and therefore decrease the evaluation time.

- In this thesis it has been stated that the current trend is to combine various simulations and base the design process on a set of multidiscipline simulations. One perspective would be to combine the discrete event dynamic simulation with the digital mock-up of the system and implement also the functional and dysfunctional behaviour of the system in the digital mock-up. This approach would lead to testing and verifying the system at different stages of the design, starting from the very early phases, and would enable the designer to anticipate design errors and future design optimizations. It would allow for the planning of rescue operations from the early design phase in the event of severe failures, which is currently assessed in the later phase of the design.

- The Hybrid Petri Net approach should also be implemented to model the discrete event dynamic in order to take into account more accurately the effect of continuous environmental parameters on the system reliability according to the operating phase. For instance, in the case of the fusion reactor, the RH devices are subjected to high levels of radiation only when they are located in the reactor. Otherwise, outside the vessel area, in the hot-cell for instance, the level of radiation is much lower and therefore affects the reliability to a lesser extent. This perspective can be translated for the temperature parameters for any other industrial application. For instance, the aircraft industry has to consider the temperature gradient during the airplane operating time. A similar approach can be developed for humidity and dust concentrations.

- Further study may be required to reduce the data uncertainties concerning the failure distribution of components, as well as software failures, which have not been taken into account in this work. Also failures between two components may lead to a new type of failure that may be challenging to model. More study and testing are needed to provide more realistic and robust results.

8 CONCLUSION

A verification-driven process for designing a complex system based on reliability requirements has been presented in this thesis. The thesis started with an extensive state of the art in verification and validation processes in various engineering fields, from an industrial and research point of view, as well as different practices in terms of design processes. The state of the art has shown that the current trend in both industry and research is towards a simulation-based design process that aims to provide a continuous verification of the developed concept over its design process. It has been shown that reducing design errors from the very early phase of the design leads to substantially decreased product design costs. However, this is not without challenges and modelling as well as evaluating concepts against each other using quantitative evaluation methods is one major issue.

The method suggested in this thesis has shown the possibility of assessing a design in a quantitative way all along the design process. This method is an innovative means of evaluating a concept design, since it is not influenced by the experience level or personal opinions of the analyst. The method is designed to be used as an iterative manner during the design process, from the very early phases up to the manufacturing phase. The method has been first developed using a simple case study, the pendulum system, and the functional and dysfunctional stochastic Petri net model of the system has been built using GRIF software. Reliability has been used as the main evaluation criteria in this case study; however, it is possible to implement other criteria such as availability, severity, operational time or any combination of criteria according to the requirements of the decision-making process. The model of a single valve actuator has been compared to a double valve model to assess the accuracy of the method. As forecasted, the double valve model has shown to be a more reliable solution than the single valve model. Results showed that the double valve model is about 30% more reliable than the single valve model after 4 000 h of operating time. However, this difference decreased to 10% after 20 000 h of operating time.

The method has then been applied to a real case study, the DEMO Divertor Remote Handling system. After analysing the extensive set of requirements, it was clearly demonstrated that the reliability of the system was one of the main design-driving requirements for the DEMO RH project. The discrete event dynamic system of the DEMO maintenance procedure for the removal and installation of the Divertor Cassettes has been modelled, and the operational time of each phase has been quantified in a fuzzy way, using a scale from 0 to 5, for more subjectivity.

The functional stochastic Petri nets of the two concept designs have been modelled: the transfer cask and the cassette mover.

During the project, two Divertor maintenance port options have been evaluated using the developed method, a 45° inclined port and a horizontal port. For each port option, two systems where compared at a functional level (the transfer cask and the main mover). Results showed that the transfer cask of the horizontal port option is slightly more reliable (≈5%) than the transfer cask for the 45° port configuration. However, the reliability of the Mover for the 45° port option is slightly higher than the horizontal mover (≈5%) after 3 000 h of operating time. The combination of the transfer cask and radial mover for each configuration were then evaluated, and the results showed that the 45° RH systems is more reliable by about 3% than the Horizontal port RH system. Indeed, the mover reliability has more influence on the total RH reliability, since the operational time of the mover is greater than the transfer cask operational time.

Moreover, it has been shown that the method can take into account environmental criteria that may affect component reliability and therefore the entire system reliability. In this case study it has been considered that radiation arbitrarily decreases the reliability of the mover by a factor of two, since only the mover is going into the vacuum vessel, where the radiation level is the highest, unlike the transfer cask that stays outside the vessel. Results showed that taking into account such important criteria is of primary importance, since it may affect the decision-making process. The radiation criterion accentuates the difference between the two RH concepts. The 45° concept is 5% more reliable than the Horizontal concept after 3 000 h. Without a consideration of radiation, it was only a 3% difference between the two concepts.

Finally, the method has been applied on a more detailed system design, and the ITER Divertor Cassette Multifunctional Mover has been used on the discrete event dynamic system of DEMO maintenance. The detail of ITER CMM has been broken down to the component level, and two configurations of the CMM have been evaluated. The first model consisted in the real CMM as it has been designed using water hydraulic actuators. The second model consisted in an electrical actuated CMM using torque motors. Results showed that the difference in reliability between the electric actuator CMM version versus the hydraulic actuator CMM varies from +10% more reliable after 2 000 h of operating time to +7% more reliable after 4 000 h of operating time for the electrically actuated CMM version. However, in this final case study, no environmental criteria were taken into account; those results therefore aim at comparing two solutions under same conditions. The mean of this study is obviously not to reconsider the design of the CMM, solely used for comparison basis.

On the basis of the presented theory, simulations and experiments, it can be concluded that the reliability-based Petri net method can improve confidence in the development of complex systems from the early design phases. The iterative and quantitative nature of the method supports the decision-making process and drives the design towards the most reliable solution and therefore decrease the number of design iterations which results in the end in decreasing product development time [174].

9 REFERENCES

[1] W. Welsch, "Virtual to begin with?," *Sandbothe/Winfried Marotzki (Eds.),* vol. Subjektivität und Öffentlichkeit, pp. 20-60, 2000.

[2] "Oxford English Dictionary," *Online edition,* 2014.

[3] P. G. Maropoulos and D. Ceglarek, "Design Verification and validation in product lifecycle," *CIRP Annals - Manufacturing Technology 59,* pp. 740-759, 2010.

[4] W. L. Oberkampft and T. G. Trucano, "Verification and validation benchmarks," *Nuclear Engineering and Design,* vol. 238, pp. 716-743, 2008.

[5] R. Scigliano, M. Scionti, and P. Lardeur, "Verification, validation and variability for the vibration study of a car windscreen modeled by finite elements," *Finite Elements in Analysis and Design,* vol. 47, pp. 17-29, 2011.

[6] B. H. Thacker, S. W. Doebling, F. M. Hemez, M. C. Anderson, J. E. Pepin, and E. A. Rodriguez, "Concepts of Model Verification and Validation," National Nuclear Security Agency (NNSA)2004.

[7] W. L. Oberkampft and T. G. Trucano, "Verification and Validation in Computational Fluid Dynamics," Sandia National Laboratories, California2002.

[8] K. H. Chang, "Product Design Modeling using CAD/CAE," *Elsevier,* vol. The Computer aided Engineering Design Series, 2014.

[9] E. Commission, "Factories of the Future - Multi-annual roadmap for the contractual PPP under Horizon 2020," EFFRA European Factories of the Future Research Association, Luxembourg 978-92-79-31238-0, 2013.

[10] M. Bordegoni and C. Rizzi, "Innovation in Product Design - From CAD to Virtual Prototyping," *Springer,* 2011.

[11] P. Brandon and T. Kocatürk, *Virtual Futures for Design, Construction and procurement*, 2009.

[12] J. Heilala, J. Montonen, P. Järvinen, S. Kivikunnas, M. Maantila, J. Sillanpää, and T. Jokinen, "Developing Simulation-based decision support systems for customer-driven manufacturing operation planning," in *2010 Winter Simulation Conference*, Cranfield University, UK, 2010.

[13] M. Wetter, "A View on Future Building System Modeling and Simulation," in *Building Performance Simulation for Design and Operation*, H. a. R. Lamberts, Ed., ed Routledge, UK, 2011.

[14] P. G. Maropoulos, P. Vichare, O. Martin, J. Muelaner, M. D. Summers, and A. Kayani, "Early design verification of complex assembly variability using a Hybrid - Model Based and Physical Testing - Methodology," *CIRP Annals – Manufacturing Technology,* vol. 60, pp. 207-210, 2011.

[15] W. Schamai, P. Helle, P. Fritzson, and C. J. J. Paredis, "Virtual Verification of System Designs against System Requirements," in *ACES-MB Workshop Proceedings*, 2010.

[16] NASA, "Systems Engineering Handbook," National Aeronautics and Space Administration2007.

[17] INCOSE, "Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities," *International Council on Systems Engineering,* 2012.

[18] "Systems Engineering for Intelligent Transportation Systems," in *An introduction for Transportation Professionals*, ed: National ITS Architecture Team, 2007.

[19] R. Guillerm, H. Demmou, and N. Sadou, "Safety evaluation and management of complex systems: A system engineering approach," *Concurrent Engineering: Research and Application,* vol. 20, pp. 149-159, 2012.

[20] G. Wang, "Definition and Review of Virtual Prototyping," 2002.

[21] S. Aromaa, S. P. Leino, and J. Viitaniemi, "Virtual prototyping in human-machine interaction design," *VTT Technology 185,* 2014.

[22] J. Kortelainen, *Semantic Data Model for Multibody system Modelling*. Kuopio: VTT Publications 766, 2011.

[23] G. N. Suther, "Evaluating the perception of design errors in the construction industry," 1998.

[24] J. M. Stecklein, J. Dabney, B. Dick, B. Haskins, R. Lovell, and G. Moroney, "Error Cost Escalation Through the Project Life Cycle," presented at the 14th Annual International Symposium - International Council on Systems Engineering (INCOSE) Foundation, Toulouse - France 2004.

[25] B. Blanchard, "System Engineering Management, 4th edition," *John Wiley & Sons,* 2004.

[26] B. Gumus, A. Ertas, D. Tate, and I. Cicek, "The transdisciplinary Product Development Lifecycle model," *Journal of Engineering Design,* vol. 19, pp. 185-200, 2008.

[27] B. Rooks, "A shorter product development time with digital mock-up," *Assembly Automation,* vol. 18, 1998.

[28] A. G. Stephenson, L. D. LaPiana, D. R. Mulville, P. J. TRutledge, F. H. Bauer, D. Folta, G. A. Dukeman, R. Sackheim, and P. Norvig, "Mars Climate Orbiter Mishap Investigation Board Phase I Report," NASA1999.

[29] S. H. Choi and A. M. M. Chan, "A Virtual Prototyping system for Rapid Product development," *Computer-Aided Design,* vol. 36, pp. 401-412, 2004.

[30] R. Sinha, V.-C. Liang, C. J. J. Paredis, and P. K. Khosla, "Modeling and simulation methods for design of engineering systems," *Journal of Computing and Information Science in Engineering,* vol. 1, pp. 84-91, 2001.

[31] A. Abbas-Bayoumi and K. Becker, "An industrial view on numerical simulation for aircraft aerodynamic design," *Journal of Mathematics in Industry,* vol. 1, 2011.

[32] R. J. Oden, T. Belytschko, J. Fish, T. J. R. Hughes, C. Johnson, D. Keyes, A. Laub, L. Petzold, D. Srolovitz, and S. Yip, "Simulation-Based Engineering Science - Revolutionizing Engineering Science through Simulation," 2006.

[33] R. A. Dougal, B. Langland, and A. Monti, "Virtual prototyping as a mechanism for simulation-based design," presented at the Proceedings of the 2007 Summer Computer Simulation Conference, San Diego, California, 2007.

[34] M. Soltaniehha, J. A. Gardzelewski, G. Tan, and A. Denzer, "Passivhaus and net zero energy residential designs in a cold climate: a simulation based design process for the next generation of green homes," in *Fifth National Conference of IBPSA*, Wisconsin, USA, 2012.

[35] J. Palmer, M. Irving, J. Järvenpää, H. Mäkinen, H. Saarinen, and M. Siuko, "The design and development of divertor remote handling equipment for ITER," *Fusion Engineering and Design,* vol. 82, pp. 1977-1982, October 2007.

[36] M. Lehtonen, "Simulation-based design process of smart machines," VTT Technical Research Centre of Finland 951-38-6809-5, 2006.

[37] IEEE, "IEEE Standard for System and Software Verification and Validation," in *IEEE Std 1012TM-2012*, ed: Computer Society, 2012, pp. 1-223.

[38] J. F. Koning, M. R. de Baar, B. S. Q. Elzendoorn, C. J. M. Heemskerk, D. M. S. Ronden, and W. J. Schuth, "Analysis of ITER upper port plug remote handling maintenance scenarios," *Elsevier, Fusion Engineering and Design,* vol. 87, pp. 515-519, 2012.

[39] S. Kiviranta, H. Saarinen, H. Makinen, and B. Krassi, "A method for enabling real-time structural deformation in remote handling control system by utilizing offline simulation results and 3D model morphing," *Fusion Engineering and Design,* vol. 86, pp. 1958-1962, Oct 2011.

[40] A. Tesini, B. Otto, J. Blight, C.-H. Choi, J.-P. Friconneau, K. K. Gotewal, D. Hamilton, F. Heckendorn, J.-P. Martins, T. Marty, M. Nakahira, J. Palmer, and R. Subramanian, "ITER Remote Maintenance System (IRMS) lifecycle management," *Elsevier - Fusion Engineering and Design,* vol. 86, pp. 2113-2116, 2011.

[41] AIAA, "Guide for the Verification and Validation of Computational Fluid Dynamics Simulations," 978-1563472855, 1998.

[42] Department of Defense, "Documentation of Verification, Validation & Accreditation (VV&A) for Models and Simulations," *MIL-STD-3022,* 2008.

[43] ASME, "Guide for Verification and Validation in Computational Solid Mechanics," *American Society of Mechanical Engineers,* vol. ASME V&V 10 – 2006, 2006.

[44] S. Reiter, A. Burger, A. Viehl, O. Bringmann, and W. Rosenstiel, "Virtual Prototyping Evaluation Framework for Automotive Embedded Systems Engineering," *Simutools,* 2014.

[45] P. Parviainen, H. Hulkko, J. Kääriänen, J. Takalo, and M. Tihinen, "Requirements engineering - Inventory of technologies," *VTT Publication,* 2003.

[46] H. Erdelyi, D. Talaba, and F. Girbacia, "Virtual Prototyping of an Automobile Steering System using Haptic Feedback," in *MACMESE'09 - WSEAS International Conference*, Baltimore, 2009.

[47] J. I. Bier and P. J. Tjelle, "The importance of interoperability in a simulation prototype for spares inventory planning," presented at the Proceedings of the 26th conference on Winter simulation, Orlando, Florida, USA, 1994.

[48] A. H. Scott, "Modeling aircraft assembly operations," presented at the Proceedings of the 26th conference on Winter simulation, Orlando, Florida, USA, 1994.

[49] J. D. Claxton, *Test and Evaluation Management Guide*: The Defense Acquisition University Press, 2005.

[50] T. Olofsson, R. Jongeling, B. Toolanen, and S. Woksepp, "Project environment and process design of building projects supported by virtual design and construction methods," in *W78 Conference* Slovenia, 2007.

[51] T. Wang and P. Ji, "Understanding customer needs through quantitative analysis of Kano's model," *International Journal of Quality & Reliability Management,* vol. 27, pp. 173-184, 2010.

[52] R. Ramanathan and J. Yunfeng, "Incorporating cost and environmental factors in quality function deployment using data envelopment analysis," *Elsevier - Omega,* vol. 37, pp. 711-723, 2009.

[53] T. Buchert, A. Kaluza, A. F. Halstenberg, K. Lindow, H. Haygazun Hayka, and R. Stark, "Enabling Product Development Engineers to Select and Combine Methods for Sustainable Design," *21st CIRP Conference on Life Cycle Engineering,* vol. 15, pp. 413-418, 2014.

[54] F. Z. Bai and Y. Zhao, "Dynamics modeling and quantitative analysis of multibody systems including revolute clearance joint," *Elsevier - Precision Engineering,* vol. 36, pp. 554-567, 2012.

[55] R. Lubas, M. Mycek, J. Porzycki, and J. Was, "Verification and validation of evacuation models - methodology expansion proposition," *Transportation Research Procedia,* vol. 2, pp. 715-723, 2014.

[56] G. Di Gironimo, "Innovative assembly process for modular train and feasibility analysis in virtual environment," *International Journal on Interactive Design and Manufacturing,* vol. 3, pp. 93-101, 2009.

[57] S. H. Choi and H. H. Cheung, "A versatile virtual prototyping system for rapid product development," *Computers in Industry,* vol. 59, pp. 477-488, 2008.

[58] P. Fritzson, *Principles of Object-Oriented Modeling and Simulation with Modelica 2.1*, 2003.

[59] A. Thanachareonkit and J. L. Scartezzini, "Modelling Complex Fenestration Systems using physical and virtual models," *Solar Energy,* vol. 84, pp. 563-586, 2010.

[60] M. Bozzano, A. Cimatti, J. P. Katoen, P. Katsaros, K. Mokos, V. Y. Nguyen, T. Noll, B. Postma, and M. Roveri, "Spacecraft early design validation using formal methods," *Reliability Engineering and System Safety,* vol. 132, pp. 20-35, 2014.

[61] F. Demoly, L. Toussaint, B. Eynard, D. Kiritsis, and S. Gomes, "Geometric skeleton computation enabling concurrent production engineering and assembly sequence planning," *Elsevier - Computer-Aided Design,* vol. 43, pp. 1654-1673, 2011.

[62] M. Debbabi, F. Hassane, Y. Jarraya, A. Soeanu, and L. Alawneh, *Verification and Validation in Systems Engineering: Assessing UML/SysML Design Models*: Springer-Verlag New York, Inc., 2010.

[63] D. Mourtzis, M. Doukas, and D. Bernidaki, "Simulation in Manufacturing: Review and Challenges," *CIRP Annals – Manufacturing Technology,* vol. 25, pp. 213 - 229, 2014.

[64] CIMdata, "Simulation Lifecycle Management," Michigan, CIMdata report, 2011.

[65] W. Cheung and D. Shaefer, "Product Lifecycle Management: State-of-the-Art and Future Perspectives," *Business science reference,* 2009.

[66] A. P. Hameri and J. Nihtilä, "Product data management - exploratory study on state-of-the-art in one-of-a-kind industry," *Computers in Industry 35,* pp. 195-206, 1998.

[67] D. Systèmes. (2013). *Reqtify - Dassault Systèmes*. Available: http://www.3ds.com/products-services/catia/capabilities/systems-engineering/requirements-engineering/reqtify/

[68] F. Ameri and D. Dutta, "Product Lifecycle Management: Closing the Knowledge Loops," *Computer-Aided Design & Applications, Vol.2, No.5,* pp. 577-590, 2005.

[69] E. S. Zitney, "Process/equipment co-simulation for design and analysis of advanced energy systems," *Computers and Chemical Engineering,* vol. 34, pp. 1532-1542, February 2010.

[70] F. Zorriassatine, C. Wykes, R. Parkin, and N. Gindy, "A survey of Virtual Prototyping techniques for mechanical product development," *Proceedings of the Institution of Mechanical Engineers,* vol. 217, pp. 513-530, 2003.

[71] A. Moser and R. Schweiger, "Prospects and barriers for up-front CAE-simulation in the automotive development," in *NAFEMS*, 2007.

[72] H. Park and M. R. Cutkosky, "Framework for Modeling Dependencies in Collaborative Engineering Processes," *Research in Engineering Design,* vol. 11, pp. 84-102, 1999.

[73] T. Määttä, "Virtual environments in machinery safety analysis," PhD, VTT Publications, 2003.

[74] E. Shehab, M. Bouin-Portet, R. Hole, and C. Fowler, "Enhancing digital design data availability in the aerospace industry," *CIRP*

Journal of Manufacturing Science and Technology, vol. 2, pp. 240-246, 2010.

[75] L. Hu, T. Yongliang, Z. Chaoying, Y. Jiao, and S. Yijie, "Evaluation Model of Design for Operation and Architecture of Hierarchical Virtual Simulation for Flight Vehicle Design," *Chinese Journal of Aeronautics,* vol. 25, pp. 216-226, 2012.

[76] S. Sanders, A. Rolfe, S. F. Mills, and A. Tesini, "Application of Remote Handling compatibility on ITER plant," *Elsevier, Fusion Engineering and Design,* vol. 86, pp. 1989-1992, 2011.

[77] G. Di Gironimo, "A RE-CAE methodology for re-designing free shape objects interactively," *International Journal on Interactive Design and Manufacturing,* vol. 3, pp. 273-283, 2009.

[78] A. Tesini and J. Palmer, "The ITER remote maintenance system," *Elsevier - Fusion Engineering and Design,* vol. 83, pp. 810-816, 2008.

[79] ITER, "Remote Handling Code of Practice," ITER_D_2E7BC5

[80] A. Tesini and A. C. Rolfe, "The ITER Remote Maintenance Management System," *Elsevier - Fusion Engineering and Design,* vol. 84, pp. 136-241, 2009.

[81] L. P. M. Duisings, S. van Til, A. J. Magielsen, D. M. S. Ronden, B. S. Q. Elzendoorn, and C. J. M. Heemskerk, "Applying HAZOP analysis in assessing remote handling compatibility of ITER port plugs," *Elsevier, Fusion Engineering and Design,* 2013.

[82] G. Grossetti, G. Aiello, C. Heemskerk, B. Elzendoorn, R. Gessner, J. Koning, A. Meier, D. Ronden, P. Späh, T. Scherer, S. Schreck, D. Strauss, and A. Vaccaro, "The ITER EC H&CD Upper Launcher: Analysis of vertical Remote Handling applied to the BSM maintenance," *Elsevier, Fusion Engineering and Design,* 2013.

[83] A. Encheva, H. Omran, M. Pérez-Lasala, A. Alekseev, S. Arshad, O. Bede, S. Bender, L. Bertalot, M.-F. Direz, J.-M. Drevon, S. Jakhar, Y. Kaschuk, V. Komarov, R. Lebarbier, F. Lucca, B. Macklin, P. Maquet, A. Marin, A. Martin, S. Mills, D. Netoiu, K. M. Patel, C. S. Pitcher, J. Reich, R. Reichle, G. Sandford, T. Sarot, G. Vayakis, C. Walker, and M. Walsh, "Challenges of ITER diagnostic electrical services," *Elsevier - Fusion Engineering and Design,* vol. 88, pp. 1423-1427, 2013.

[84] E. Laniado-Jacome, "Numerical Model to Study of Contact Force in a Cylindrical Roller Bearing with Technical Mechanical Event Simulation," *Journal of Mechanical Engineering and Automation,* vol. 1, pp. 1-7, 2011.

[85] H. Saarinen, V. Hämäläinen, J. Karjalainen, T. Määttä, M. Siuko, S. Esqué, and D. Hamilton, "Simulating and visualizing deflections of a remote handling mechanism," *Fusion Engineering and Design,* 2013.

[86] M. J. Pratt, "Virtual Prototypes and Product Models in Mechanical Engineering," *Virtual Prototyping - Virtual environments and the products design process,* vol. Chapter 10, pp. 113-128, 1995.

[87] R. McHugh, "Virtual Prototyping of Mechatronics for 21st Century Engineering and Technology," *International Journal of Engineering Research & Innovation,* vol. 3, pp. 69-75, Fall/Winter 2011.

[88] C. Morris, "Academic Press Dictionary of Science and Technology," *Harcourt Brace Jovanovich,* 1991.

[89] C. K. Chua, S. H. Teh, and R. K. L. Gay, "Rapid Prototyping Versus Virtual Prototyping in Product Design and Manufacturing," *Springer - International Journal on Advanced Manufacturing Technology,* vol. 15, pp. 597-603, 1999.

[90] C. Alexandru and C. Pozna, "Dynamic Modeling and Control of the Windshield Wiper Mchanisms," *WSEAS Transactions on Systems,* vol. 8, pp. 825-834, 2009.

[91] Antonino Gomes de Sa and G. Zachmann, "Virtual Reality as a Tool for Verification of Assembly and Maintenance Processes," *Computers & Graphics,* vol. 23, pp. 389-403, 1999.

[92] P. McLeod and P. Knowledge, "The Availability and Capabilities of 'Low-End' Virtual Modelling (Prototyping) Products to Enable Designers and Engineers to Prove Concept Early in the Design Cycle," *PRIME Faraday Technology Watch,* 2001.

[93] R. Curran, M. Price, S. Raghunathan, E. Benard, S. Crosby, S. Castagne, and P. Mawhinney, "Integrating Aircraft Cost Modeling into Conceptual Design," *Concurrent Engineering,* vol. 13, p. 321, 2005.

[94] G. Wöhlke and E. Schiller, "Digital Planning Validation in automotive industry," *Computers in Industry,* vol. 56, pp. 393-405, 2005.

[95] K. J. Arrow and S. S. Arrow, "Methodology Problems in Airframe Cost-Performance Studies," *Rand Ciroiratuib Document,* vol. RM-456-PR, p. 33, 1950.

[96] J. Isdale. (1998). *What is Virtual Reality?* Available: http://www.isdale.com/jerry/VR/WhatIsVR.html

[97] H. G. Hoffman, T. Richards, B. Coda, A. Richards, and S. R. Sharar, "The illusion of presence in immersive virtual reality during an fMRI brain scan," *PubMed,* 2003.

[98] U. Jasnoch, H. Kress, and J. Rix, "Towards a Virtual Prototyping Environment," *Virtual Environments,* vol. Proceedings, 1994.

[99] D. Gubler, A. Schälin, and A. Moser, "Virtual Prototyping and Virtual Reality in the Design Process of Industrial Ventilation," *Air Flow consulting,* 2002.

[100] T. J. Bell and H. S. Fogler, "Low Cost Virtual Reality and its Application to Chemical Engineering - Part two," *Conputing and Systems Technology Division Communications,* vol. 18, 1995.

[101] T. S. Mujber, T. Szecsi, and M. S. J. Hashmi, "Virtual reality application in manufacturing process simulation," *Journal of Materials Processing Technology,* vol. 155-156, pp. 1834-1838, 2004.

[102] R. Ryan, "Digital Testing in the Context of Digital Engineering "Functional Virtual Prototyping"," *Mechanical Dynamics, Inc,* vol. ADAMS user Conference, 1999.

[103] K. Dvorak and S. J., "Solution of technical projects using computer virtual prototypes," *International Journal of MAthematics and Computers in Simulation,* vol. 6, pp. 290-297, 2012.

[104] A. Jimeno and A. Puerta, "State of the art of the virtual reality applied to design and manufacturing processes," *International Journal oon Advanced Manufacturing Technology,* vol. 33, pp. 866-874, 2007.

[105] R. G. Sargent, "Verification and Validation of Simulation Models," *Proceedings of the 2005 Winter Simulation Conference,* pp. 130-143, 2005.

[106] M. Zaeh and D. Siedl, "A New Method for Simulation of Machining Performance by Integrating Finit Element and Multi-body Simulation for Machine Tools," *Annals of the CIRP,* vol. 56/1/2007, pp. 383-386, 2007.

[107] S. Redon, "Fast continuous collision detection and handling for desktop virtual prototyping," *Virtual Reality,* vol. 8, pp. 63-70, 2004.

[108] ANSYS, "Mechanical APDL Multibody Analysis Guide," *Mechanical APDL Multibody Analysis Guide,* vol. Release 13.0, 2013.

[109] E. Pezzuti, R. Stefanelli, P. P. Valentini, and L. Vita, "Computer-aided simulation and testing of spatial linkages with joint mechanical errors," *International Journal for Numerical Methods in Engineering,* vol. 65, pp. 1735-1748, 2006.

[110] A. Jeang, "Computer-Aided Tolerance Synthesis with Statistical Method and Optimization Techniques," *Quality and Reliability Engineering International,* vol. 14, pp. 131-139, 2001.

[111] H. Li, T. Huang, C. W. Kong, H. L. Guo, A. Baldwin, N. Chan, and J. Wong, "Integrating design and construction through virtual prototyping," *Elsevier - Automation in Construction,* vol. 17, pp. 915-922, 2008.

[112] B. Elzendoorn, M. D. Baar, R. Chavan, T. Goodman, C. Heemskerk, R. Heidinger, K. Kleefeldt, J. Koning, S. Sanders, P. Späh, D. Strauss, T. Verhoeven, and F. D. Vreede, "Analysis of the ITER ECH Upper Port Launcher remote maintenance using virtual reality," *Fusion Engineering and Design,* vol. 84, pp. 733-735, 2009.

[113] A. Raneda, P. Pessi, M. Siuko, H. Handroos, J. Palmer, and V. Vilenius, "Utilization of virtual prototyping in development of CMM," *Fuusion Engineering and Design,* vol. 69, pp. 183-186, 2003.

[114] R. Curran, G. Gomis, S. Castagne, J. Butterfield, T. Edgar, C. Higgins, and C. McKeever, "Integrated digital design for

manufacture for reduced life cycle cost," *Elsevier - Internation Journal on Production Economics,* vol. 109, pp. 27-40, 2007.

[115] L. Mariti and P. P. Valentini, "Improving the design of squat machine using motion cpture and virtual prototyping," *International Sports Engineering Association,* vol. 14, pp. 73-84, 2011.

[116] K. H. Chang, "Design Theory and Methods using CAD/CAE," *The Computer Aided Engineering Design Series,* 2015.

[117] K. S. Chin, A. Chan, and J. B. Yang, "Development of a fuzzy FMEA based product design system," *International Journal on Advance Manufacturing Technology,* vol. 36, pp. 633-649, 2008.

[118] L. A. Zadeh, "Fuzzy sets," *Information and control,* vol. 8, pp. 338-353, 1965.

[119] A. Hambali, S. M. Sapuan, N. Ismail, and Y. Nukman, "Application of analytical hierarchy process in the design concept selection of automotive composite bumper beam during the conceptual design stage," *Scientific research and Essay,* vol. 4, pp. 198-211, 2009.

[120] O. S. Vaidya and S. Kumar, "Analytic hierarchy process: An overview of application," *European Journal of Operational Research,* vol. 169, pp. 1-29, 2004.

[121] D. Y. Chang, "Applications of the extent analysis method on fuzzy AHP," *European Journal of Operational Research,* vol. 95, pp. 646 - 655, 1996.

[122] R. H. Yeh and M.-H. Hsieh, "Fuzzy assessment of FMEA for a sewage plant," *Journal of the Chinese Institute of Industrial Engineers,* vol. 24, pp. 505-512, 2007.

[123] Y. Kazancoglu and M. Aksoy, "A fuzzy logic-based QFD to identify key factors of e-learning design," *Social and Behavioral Sciences,* vol. 28, pp. 322 - 327, 2011.

[124] N. Belu, D. C. Anghel, and N. Rachieru, "Application of Fuzzy Logic in Design Failure Mode and Effects Analysis," *Applied Mechanics and Materials,* vol. 371, pp. 832-836, 2013.

[125] D. Duminică and M. Avram, "Criticality Assessment Using Fuzzy Risk Priority Numbers," in *MECAHITECH'10*, Bucharest, 2010, pp. 349 - 356.

[126] Y.-M. Wang, K.-S. Chin, G. K. K. Poon, and J.-B. Yang, "Risk evaluation in failure mode and effect analysis using fuzzy weighted geometric mean," *Expert Systems with Applications,* vol. 36, pp. 1195-1207, 2009.

[127] P. R. Adduri and R. C. Penmetsa, "System Reliability Analysis for mixed uncertain variable," *Structural Safety,* vol. 31, pp. 375-382, 2009.

[128] G. Ciardo and C. Lindemann, "Analysis of Deterministic and Stochastic Petri Nets," *IEEE Computer Society,* vol. Performance Evaluation, pp. 160-169, 1993.

[129] US Department of Defense, "Military Handbook - Reliability Prediction of Electronic Equipment - MIL-HDBK-217F " 1995.

[130] Naval Surface Warfare Center (NSWC), *Hanbook of Reliability Prediction Procedures for Mechanical Equipment*, 2011.

[131] ITEM Software Inc. (2007). *Reliability Prediction Basics* Available: http://www.reliabilityeducation.com/ReliabilityPredictionBasics.pdf

[132] O. Ditlevsen and H. O. Madsen, *Structural Reliability Methods*. Chichester: John Wiley & Sons Ltd, 1996.

[133] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, "Fault Tree Handbook with Aerospace Applications," 2002.

[134] P. Brooks, "Markov Chain Monte Carlo Method and Its Application," *Journal of the Royal Statistical Society,* vol. 47, pp. 69-100, 1998.

[135] A. Naess, B. J. Leira, and O. Batsevych, "System reliability analysis by enhanced Monte Carlo simulation," *Structural Safety,* vol. 31, pp. 349-355, 2009.

[136] H. Phan, *Springer Handbook of Engineering Statistics*. London: Springer-Verlag, 2006.

[137] J. I. McCool, *Using the Weibull Distribution: Reliability, Modeling and Inference*: Wiley, 2012.

[138] A. Demri, A. Charki, F. Guérin, and H. Chiristofol, "Functional and Dysfunctional Analysis of a Mechatronic System," in *Reliability and Maintainability Symosium*, Las Vegas, 2008, pp. 114-119.

[139] R. David and H. Alla, *Discrete, Continuous, and Hybrid Petri Nets*: Springer, 2010.

[140] Y.-C. Ho, "Scanning the issue - Dynamics of discrete events systems," *IEEE,* 1989.

[141] R. Champagnat, P. Esteban, H. Pingaud, and R. Valette, "Petri net based modeling of hybrid systems," *Computers in Industry,* vol. 36, pp. 139-146, 1998.

[142] E. Villani, J. C. Pascal, P. E. Miyagi, and R. Valette, "A Petri net-based object-oriented apporach for the modelling of hybrid productive systems," *Nonlinear Analysis: Theory, Methods & Applications,* vol. 62, pp. 1394-1418, 2005.

[143] A. Kossiakoff, W. N. Sweet, S. J. Seymour, and S. M. Biemer, "The System Development process," in *Systems Engineering Principles and Practice, Second Edition*, I. John Wiley & Sons, Ed., ed, 2011.

[144] G. Pahl and W. Beitz, *Engineering design - A systematic approach [BOOK]*, 1996.

[145] K. T. Ulrich and S. D. Eppinger, *Product design and development*. Boston, MA: McGraw-Hill, 2004.

[146] D. Dori, "Object-Process Methodology Applied to Modeling Credit Card Transactions," *Journal of Database Management,* vol. 12, pp. 4-4, 2001.

[147] D. Nicholls, *System Reliability Toolkit*: RIAC, 2005.

[148] V. Rathod, O. P. Yadav, A. Rathore, and R. Jain, "Probabilistic Modeling of Fatigue Damage Accumulation for reliability Prediction," *International Journal of Quality, Statistics and Reliability,* vol. 2011, 2011.

[149] A. J. Nixon-Pearson and S. R. Hallett, "An experimental investigation into quasi-static and fatigue damage development in bolted-hole specimens," *Elsevier - Composites Part B,* pp. 462-473, 2015.

[150] W. Guo, H. Cao, Z. He, and L. Yang, "Fatigue Life Analysis of Rolling Bearings Based on Quasistatic Modeling," *Shock and Vibration,* 2015.

[151] A. D. Swain and H. E. Guttmann, "Handbook pf Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Albuquerque, 1983.

[152] S. Stancliff, J. M. Dolan, and A. Trebi-Ollennu, "Towards a Predictive Model of Robot Reliability," Carnegie Mellon University - Robotics Institute - School of Computer Science, 2005.

[153] EPSMA, "Guidelines to Understanding Reliability Prediction," Europen Power Supply Manufacturers Association, 2005.

[154] D. J. Fonseca and M. Sequera, "On MEMS Reliability and Failure Mechanisms," *International Journal of Quality, Statistics, and Reliability,* vol. 2011, 2011.

[155] F. Afshaarnia, M. Asoodar, A. Abdeshahi, and A. Marzban, "Failure rate analysis of four agricultural tractor models in southern Iran," *Agricultural Engineering International: CIGR Journal,* vol. 15, pp. 160-170, 2013.

[156] Y. Levin and M. Lyutikov, "On the dynamics of mechanical failures in magnetized neutron-star crusts," *Monthly Notices of the Royal Astronomical Society,* vol. 427, pp. 1574-1579, 2012.

[157] M. L. Hamilton, F.-H. Huang, W. J. S. Yang, and F. A. Garner, "Mechanical Properties and Fracture Behavior of 20% Cold-Worked 316 Stainless Steel Irradiated to Very High Neutron Exposures," presented at the 13th International Symposium (Part II), Philadelphia, 1987.

[158] L. C. Cadwallader, "Preliminary Failure Modes and Effects Analysis of the US MAssive Gas Injection Disruption Mitigation System Design.pdf," U.S. Department of Energy National Laboratory, 2013.

[159] R. J. Sadhlon, "Mechanical Applications in Reliability Engineering," Reliability Analysis Center, 1993.

[160] C. J. M. Lasance, "Temperature and reliability in electronics systems," *Aerospace, Defense, Design, Test&= & Measurement,* 2001.

[161] V. Lakshminarayanan and N. Siriraam, "The Effect of Temperature on the Reliability of Electronic Components," *IEEE CONECCT2014,* 2014.

[162] C. L. Hanks and D. J. Hamman, "Radiation Effects Design Handbook - Electrical Insulating Materials and Capacitors," NASA, Columbus, Ohio, 1971.

[163] E. Umbach, "Energy Research for Tomorrow," ed. Berlin, Germany: Helmholtz-Gemeinschaft Deutscher Forschungszentren, 2011.

[164] F. Romanelli, V. Barabacshi, D. Borba, G. Federici, L. Horton, R. Neu, D. Stork, and H. Zohm, "A Roadmap to the Realisation of Fusion Energy," EFDA2013.

[165] S. Esque, J. Mattila, M. Siuko, M. Vilenius, J. Järvenpää, L. Semeraro, M. Irving, and C. Damiani, "The use of digital mock-ups on the development of the Divertor Test Platform 2," *Proceeding of the 25th Symposium on Fusion Technology,* vol. 84, pp. 752-756, June 2009.

[166] A. S. Kukushkin, H. D. Pacher, V. Kotov, G. W. Pacher, and D. Reiter, "Finalizing the ITER divertor design: The key role of SOLPS modeling," *Fusion Engineering and Design,* vol. 86, pp. 2865-2873, 2011.

[167] A. Muhammad, J. Mattila, M. Vilenius, M. Siuko, and L. Semeraro, "Advantage of redundancy in the controllability of remote handling manipulator," *Fusion Engineering and Design,* vol. 86, pp. 1882-1885, 2011.

[168] H. Saarinen, J. Tiitinen, L. Aha, A. Muhammad, J. Mattila, M. Siuko, M. Vilenius, J. Järvenpää, M. Irving, C. Damiani, and L. Semeraro, "Optimized hardware design for the divertor remote handling control system," *Fusion Engineering and Design,* vol. 84, pp. 1666-1670, 2009.

[169] V. Lyytikäinen, P. Kinnunen, J. Koivumäki, J. Mattila, M. Siuko, S. Esque, and J. Palmer, "Divertor cassette locking system remote handling trials with WHMAN at DTP2," *Fusion Engineering and Design,* vol. 88, pp. 2181-2185, 2013.

[170] H. Saarinen, T. Kivelä, L. Zhai, V. Hämäläinen, J. Karjalainen, L. Aha, L. Heikkilä, H. Mäkinen, J. Järvenpää, S. Kiviranta, B. Krassi, M. Viinikainen, M. Siuko, J. Mattila, S. Esque, and L. Semeraro, "Results of CMM standalone tests at DTP2," *Fusion Engineering and Design,* vol. 86, pp. 1907-1910, 2011.

[171] H. Mäkinen, J. Järvenpää, P. Valkama, J. Väyrynen, F. Amjad, M. Siuko, J. Mattila, L. Semeraro, and S. Esque, "Concept design of the cassette toroidal mover," *Fusion Engineering and Design,* vol. 86, pp. 2092-2095, 2011.

[172] K. Hölttä-Otto, "Modular Product Platform Design," Doctoral Dissertation, Department of Mechanical Engineering, Helsinki University of Technology, TKK Dissertations 10, 2005.

[173] H. Mäkinen, "DEMO-AWP2015 - D013 - RM3.2.2 - Conceptual Design Description of the horizontal port divertor cassette mover," VTT, Tampere, 2015.

[174] R. A. Center, "RAC NPRD-91 - Nonelectronic parts reliability data," W. Denson, Ed., ed. Rome, NY, 1991.

[175] Department of Defense, "MIL-HDBK-338B - Military Handbook electronic reliability design handbook," in *Department of Defence*, ed. USA, 1998.

[176] A. Mihalache, F. Guerin, M. Barreau, A. Todoskoff, and B. Dumon, "Reliability assessment of mechatronic systems: operating field data analysis," presented at the IEEE International Conference on Industrial Technology (ICIT), 2004.

[177] J. K. Korane, "Maximizing Cylinder Performance," in *Machine Design*, ed: Bimba, 1998.

[178] I. Organisation, "Design Description Document - Remote Handling Equipment," 2006.

[179] J. Palmer. (2012). *ITER's divertor remote handling system signed off*. Available: http://www.iter.org/newsline/244/1372

[180] J. Palmer, M. Siuko, P. Agostini, R. Gottfried, M. Irving, E. Martin, A. Tesini, and V. M. Uffelen, "Recent developments towards ITER 2001 divertor maintenance," *Fusion Engineering and Design,* vol. 75, pp. 583-587, 2005.

[181] M. Siuko, J. Mattila, S. Esque, J. Palmer, and D. Hamilton, "DTP2 - The Platform for Verifying and Validating the ITER Divertor Remote Handling," *Proceeding of the 27th Symposium on Fusion Technology,* 2012.

[182] I. Ribeiro, C. Damiani, A. Tesini, S. Kakudate, M. Siuko, and C. Neri, "The remote handling systems for ITER," *Fusion Engineering and Design,* vol. 86, pp. 471-477, 2011.

[183] R. Hemmings, V. Baulo, Y. Gotoh, B. Green, V. Ivanov, M. Mills, E. Mochizuki, and C. Woodward, "The ITER-FEAT building layout - design considerations for the reduction in scale," *Fusion Engineering and Design,* vol. 58, pp. 913-918, 2001.

[184] D. Maisonnier, G. Cerdan, S. Chiocchio, C. Damiani, J.-P. Friconneau, R. Haange, M. Irving, E. Martin, J. Palmer, A. Poggianti, M. Siuko, E. Tada, N. Takeda, A. Tesini, R. Tivey, and A. Turner, "Divertor Remote Maintenance," in *18th Fusion Energy Conference*, Sorrento, Italy, 2000.

[185] G. Janeschitz, R. Tivey, A. Antipenkov, V. Barabash, S. Chiocchio, G. Federici, H. Heidl, C. Ibbott, and E. Martin, "Overview of the divertor design and its integration into RTO/RC-ITER," *Fusion Engineering and Design,* vol. 49, pp. 107-117, 2000.

[186] A. Tessini, "ITER Remote Handling: Overview and Technical Requirements," in *The Annual Finnish Fusion Seminar*, 2010.

[187] J. Palmer, "SRD-23-02 Divertor Remote Handling System," ITER IDM 2823C3, 2009.

[188] S. Esque, C. V. Hille, R. Ranz, C. Damiani, J. Palmer, and D. Hamilton, "Progress in the design, R&D and procurement preparation of the ITERDivertor Remote Handling System," *Fusion Engineering and Design,* vol. 89, pp. 2373-2377, 2014.

[189] T. Tanaka, "Reliability Analysis of Structural Components under Fatigue Environment Including Random Overloads," *Elsevier - Engineering Fracture Mechanics,* vol. 52, pp. 423-431, 1995.

APPENDIX A: DEMO remote handling system requirements

Table 16 – Customer Needs

CN ID	CN Statement : Functional needs
CN-1	Divertor cassette replacement will have to be accomplished fully remotely and under harsh environmental and radiation conditions.
CN-2	These cassettes shall be inserted radially through a lower level port and moved toroidally before being locked into position (TBC).
CN-3	The divertor remote handling system must perform disconnection and reconnection of divertor pipe elbows
CN-4	The divertor remote handling system must perform cutting, welding, and inspection of divertor pipe elbows
CN-5	The divertor remote handling system must perform handling of divertor pipe elbows
CN-6	The divertor remote handling system must perform disconnection and reconnection of divertor pipes to and from the divertor manifold
CN-7	The divertor remote handling system must perform disconnection and reconnection of port inner closure plate
CN-8	The divertor remote handling system must perform handling of divertor pipe and closure plate assembly between vessel and cask
CN-9	The DPICC must provide the tools and manipulators required for the cutting, welding, testing and handling of the divertor pipes and flanges
CN-10	The divertor remote handling system must provide divertor cassette transportation into and out of the vacuum vessel and divertor connection and disconnection to the vessel during maintenance and first assembly
CN-11	The inlet and outlet radial cooling pipes shall be cut, and orbitally re-welded, to allow the dismounting/mounting of the cassettes.
CN-12	Mechanisms should be unloaded to create clearance before movement
CN-13	Mover shall be able to support and handle one central cassette in the angled port.
CN-14	Mover shall be able to support and handle left and right hand second cassette
CN-15	Remote Maintenance SHALL disconnect and transfer hardware from the power plant to the maintenance facility
CN-16	Remote Maintenance SHALL transfer and install all hardware
CN-17	The remote handling system SHALL perform disconnection, reconnection and inspection of all the services for components requiring removal or installation
CN-18	The RMS must be able to remotely replace the complete divertor system
CN-19	The RMS must be able to remotely replace any single failed divertor cassette
CN-20	RM SHALL rescue all RM equipment that cannot self-recover
CN-21	The RM equipment SHALL have rescue features compatible with the RM rescue equipment
CN-22	RM hardware on notification of system failure SHALL enter a safe state, whereby the motion is stopped and remains in the same position indefinitely even if the equipment is holding load.

Table 17 – Customer Input Constraints

CC ID	Customer Constraints statement
CC-1	The maximum shut-down time for exchange of a complete Divertor is 3 months.
CC-2	Recovery and deployment of a repaired or alternative system SHALL take no longer than 2 days once the failed system is removed/recovered
CC-3	All RM hardware SHALL be designed to reduce the planned maintenance operation using the estimated loss of earnings cost of €3,000,000/day
CC-4	In-vessel RM System SHALL operate in an environment that is contaminated with tritium and activated dust (C, Be and W).
CC-5	All Remote Maintenance operations SHOULD be completed during a short maintenance period
CC-6	Failure of any remote maintenance system SHALL not result in an unacceptable safety risk
CC-7	The RMS must perform a complete Divertor replacement in 4 months
CC-8	The RMS must replace a failed Divertor cassette in 2 months
CC-9	All components must be designed to be fully remotely maintained, no manual assistance will be available on the hot side of the bio-shield or when the bioshield port plugs are open.
CC-10	Blankets and Divertor cassettes still connected to the vessel must be cooled before and during RM operations
CC-11	Vessel ambient temperature during remote operations must be <50C
CC-12	Simple movers must be used for planned in-vessel remote maintenance activities
CC-13	The materials involved in the construction of in-vessel RH equipment shall be compatible with vacuum quality clean conditions.
CC-14	The Divertor replacement lifetime is assumed to be ~ 2 fpy. In the 20 year lifetime of the DEMO, which is equivalent to 6 fpy at 30% availability, ~ 2 Divertor replacements are foreseen.
CC-15	The materials to be used in the construction of the DEMO tokamak shall withstand the fusion operating environment and meet design criteria
CC-16	Clearances around Divertor system must be taken into account to facilitate access for the installation path and in-situ positioning by the RH equipment and suitable clearances and materials must be used to facilitate viewing and sensing by the RH equipment.
CC-17	Divertor remote handling system shall supply and receive components, tools and equipment during remote handling operations at a rate that does not increase the overall maintenance downtime
CC-18	The RMS SHALL be designed such that any failure does not damage or compromise the DEMO hardware and systems (i.e. failsafe)
CC-19	The parts subjected to the highest risk of failure (flexing cables, mechanism parts, etc.…) should be located on the Divertor cassette rather than the vacuum vessel to facilitate maintenance when the cassettes are removed to the hot cell.
CC-20	All remote maintenance hardware SHALL self-recover
CC-21	The RMS SHALL be recoverable in the event of failure
CC-22	RM SHALL be capable of working for X hours with an environment of 3 kGy/hr

CC-23	RM Divertor hardware SHALL operate with no loss of function or reduction in performance at temperatures between 5 - 50 deg Celsius
CC-24	The RM System SHALL be manufactured, assembled, tested, and integrated in a manner such that no oils, greases (including finger grease), can be transferred to surfaces in the vacuum vessel or that any debris, including particulates, can be shed from it.
CC-25	Radiation sensitive items that are built into the RM Equipment (Except motors, sensors, cameras, lubricant, cables) SHALL have a minimum demonstrated (or manufacturer guaranteed) radiation lifetime of 2000 hours under the highest level radiation conditions expected for such items during its operational lifetime under normal use.
CC-26	All hardware SHALL retain their structural integrity during maintenance operations (including installation, removal, transportation/transfer and decommissioning) under all loading conditions including seismic events even with end of life decay heating and neutron damage effects
CC-27	The RMS must be designed for recovery from the beginning of the design process
CC-28	RMS systems must be designed with series production in mind
CC-29	Peak radiation levels experienced by the RMS at the start of RH operations must be less than 3kGy/hr
CC-30	Divertor RH system locating devices must reduce degrees of freedom progressively so that one degree of freedom is constrained at a time and the locking sequence is controlled. One solution is using the dowel and pin features of different lengths described in ITER Remote Handling Code of Practice.
CC-31	The Divertor remote handling system must be modular.
CC-32	Divertor RH System must be assessed for probability and mode of failure to ensure that any credible failure or damage scenario shall not result in an irrecoverable situation.
CC-33	Divertor RH system must be flexible to prepare for the unexpected new future needs for remote operations
CC-34	RH System must withstand vacuum and high current effects.
CC-35	Consideration and configuration check shall be made to what RH tooling is to be used and what are the physical constraints for using it to ensure the tasks can be carried out remotely by single RH system.
CC-36	The Supplier shall complete a RAMI analysis of the DRHS according to the ITER RAMI Analysis Programme [AD01: ITER_D_28WBXD].
CC-37	The FMECA within the RAMI analysis shall identify those failure modes with potential consequences to the personnel, public and/or environment
CC-38	The Supplier shall carefully justify the assumptions made or the sources used to define reliability values for selected components
CC-39	Whenever the available reliability data is insufficient, the Supplier shall collect further reliability data during the next Divertor RH System qualification phase to support any assumptions
CC-40	Maintenance procedures for Divertor maintenance shall be developed in detail and verified on mock-ups prior to their first assembly
CC-41	RMS design processes must be based on the worst case scenario for other designs not yet fully defined

APPENDIX B: Design structure matrix and respective clustered matrix of DEMO RH requirements

Table 18 – Mapping Customer Needs (CNs) and Functional Requirements (FRs) using Design Structure Matrix

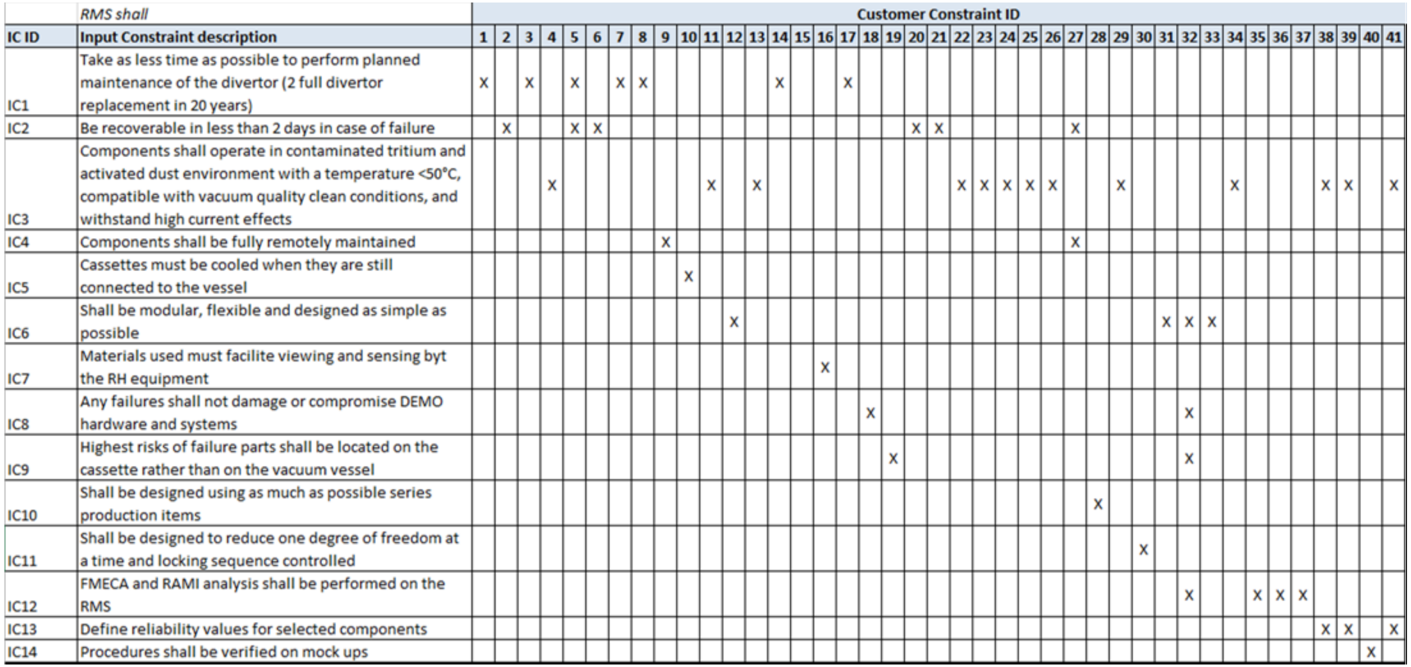
	RMS shall	CN ID																					
FR ID	**FR Description**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
FR1	Provide radial motion	X	X								X			X	X	X	X		X	X			
FR2	Provide lifting motion	X									X			X	X	X	X		X	X			
FR3	Provide toroidal motion	X	X								X			X	X	X	X		X	X			
FR4	Provide interface with Divertor Cassette	X	X								X			X	X	X	X		X	X			
FR5	Provide interfaces to support various end-effectors			X							X		X	X	X	X	X	X	X	X			
FR6	Provide interfaces to support manipulator			X	X	X	X	X	X	X	X	X				X	X	X	X	X			
FR7	Provide tooling for cutting, welding and pipes inspection				X		X			X		X					X						
FR8	Provide interfaces for handling pipes					X	X		X	X		X					X						
FR9	Provide interfaces for handling port inner closure plate							X	X	X							X						
FR10	Provide transfer cask for transporting hardwares from powerplant to maintenance facility	X									X					X	X		X	X			
FR11	Provide brakes to enter into a safe state												X										X
FR12	Provide rescue system																				X	X	
FR13	Provide rescue features compatible with RM rescue equipment																				X	X	

Table 19 – Functional requirements DSM after clustering approach

	RMS shall	CN ID																					
FR ID	FR Description	22	2	13	14	1	15	18	19	10	16	8	7	9	12	4	5	6	11	17	3	20	21
FR10	Provide features for transporting hardwares from powerplant to maintenance facility					X	X	X	X	X	X	X											
FR11	Provide brakes to enter into a safe state	X	X												X								
FR1	Provide radial motion		X	X	X	X	X	X	X	X	X												
FR6	Provide interfaces to support manipulator and tooling						X	X	X	X	X	X	X	X		X	X	X	X	X	X		
FR5	Provide interfaces to support various end-effectors			X	X		X	X	X	X	X				X					X	X		
FR13	Provide rescue features compatible with RM rescue																					X	X
FR12	Provide rescue systems to RH equipment																					X	X
FR3	Provide toroidal motion		X	X	X	X	X	X	X	X	X												
FR2	Provide lifting motion		X	X	X	X	X	X	X	X	X												
FR4	Provide interface with Divertor Cassette		X	X	X	X	X	X	X	X	X												
FR9	Provide interfaces for handling port inner closure plate										X	X	X	X									
FR7	Provide tooling for cutting, welding and pipes inspection as well as for connecting and disconnecting the divertor cassettes to the vessel									X	X			X	X	X		X	X				
FR8	Provide interfaces for handling pipes										X	X		X			X	X	X				

🟩	Transfer cask
🟧	Mover
🟪	Manipulator and toolings
🟦	End-effectors
⬜	Rescue systems
▨	Function shared between tooling and end-effectors
▨	Function shared between Mover and rescue systems

Table 20 – Mapping Customer Constraints (CCs) and Input onstraints (ICs) using Design Structure Matrix



	RMS shall	Customer Constraint ID																																								
IC ID	**Input Constraint description**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**
IC1	Take as less time as possible to perform planned maintenance of the divertor (2 full divertor replacement in 20 years)	X		X		X		X	X						X			X																								
IC2	Be recoverable in less than 2 days in case of failure		X			X	X														X	X						X														
IC3	Components shall operate in contaminated tritium and activated dust environment with a temperature <50°C, compatible with vacuum quality clean conditions, and withstand high current effects				X							X		X									X	X	X	X	X			X					X				X	X		X
IC4	Components shall be fully remotely maintained									X																		X														
IC5	Cassettes must be cooled when they are still connected to the vessel										X																															
IC6	Shall be modular, flexible and designed as simple as possible												X																			X	X	X								
IC7	Materials used must facilite viewing and sensing byt the RH equipment																X																									
IC8	Any failures shall not damage or compromise DEMO hardware and systems																		X														X									
IC9	Highest risks of failure parts shall be located on the cassette rather than on the vacuum vessel																			X													X									
IC10	Shall be designed using as much as possible series production items																												X													
IC11	Shall be designed to reduce one degree of freedom at a time and locking sequence controlled																														X											
IC12	FMECA and RAMI analysis shall be performed on the RMS																																X			X	X	X				
IC13	Define reliability values for selected components																																						X	X		X
IC14	Procedures shall be verified on mock ups																																								X	

Table 21 – Input Constraints DSM after clustering approach

	The RMS shall respect the following constraints	**Customer Constraints ID**																																							
IC ID	**Input Constraints description**	1	3	7	8	14	17	5	2	20	21	6	27	28	30	16	4	11	13	22	23	24	25	26	29	34	38	39	41	9	10	12	31	33	40	32	18	19	35	36	37
IC1	Take as less time as possible to perform planned maintenance of the divertor	X	X	X	X	X	X	X																																	
IC2	Be recoverable in case of failure							X	X	X	X	X	X																												
IC10	Shall be designed using as much as possible series production items													X																											
IC11	Shall be designed to reduce one degree of freedom at a time and locking sequence controlled														X																										
IC7	Materials used must facilite viewing and sensing byt the RH equipment															X																									
IC3	Components shall operate in contaminated tritium and activated dust environment with a temperature <50°C, compatible with vacuum quality clean conditions, and withstand high current effects																X	X	X	X	X	X	X	X	X	X	X	X	X												
IC13	Define reliability values for selected components																										X	X	X												
IC4	Components shall be fully remotely maintained																													X											
IC5	Cassettes must be cooled when they are still connected to the vessel																														X										
IC6	Shall be modular, flexible and designed as simple as possible																															X	X	X							
IC14	Procedures shall be verified on mock ups																																		X						
IC8	Any failures shall not damage or compromise DEMO hardware and systems																																			X	X				
IC9	Highest risks of failure parts shall be located on the cassette rather than on the vacuum vessel																																			X		X			
IC12	FMECA and RAMI analysis shall be performed on the RMS																																			X			X	X	X

🟦	Availability
🟦	Recoverability
🟪	Design constraints
🟧	Reliability
🟫	Procedures constraints
🟥	Failure analysis (occurrence, risk, severity)

APPENDIX C: Functional and dysfunctional Petri Net models of the CMM

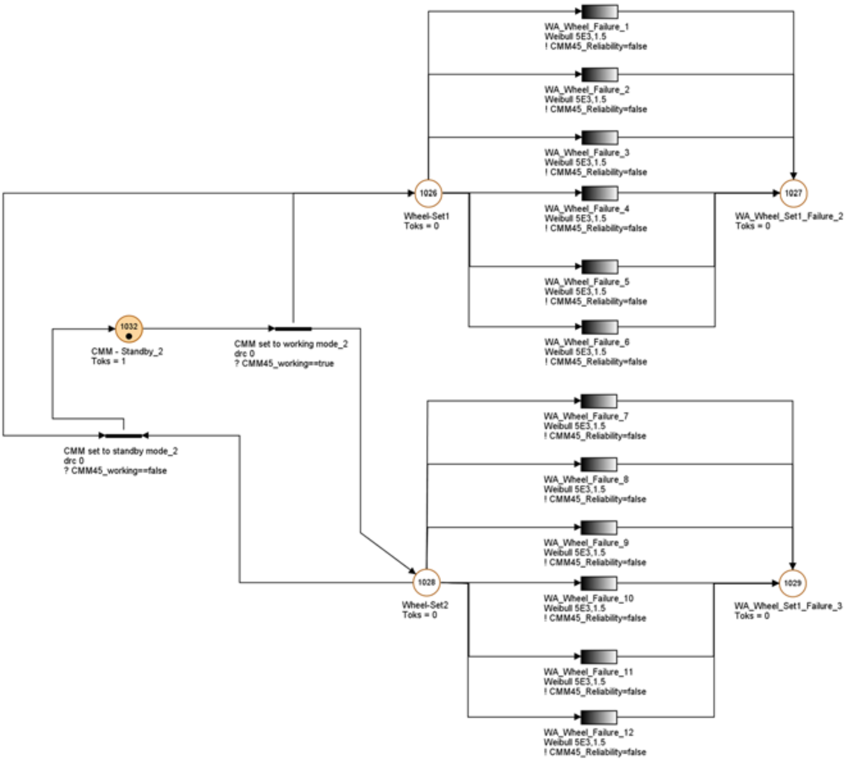


Fig. 82 - Wheel assembly

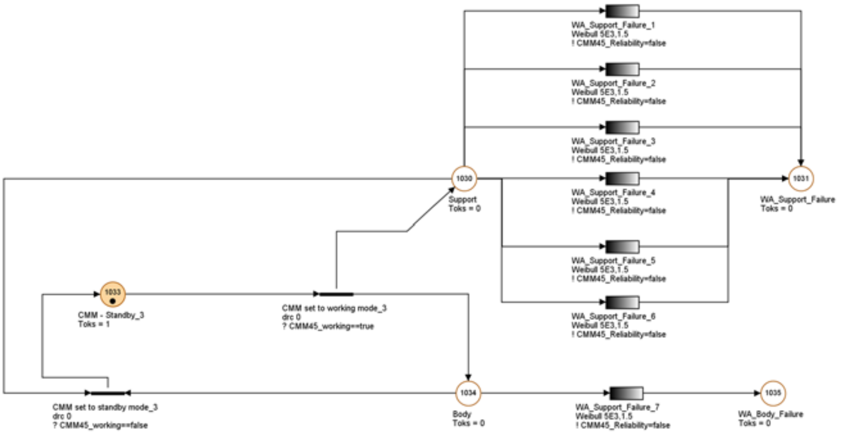


Fig. 83 - Support & body

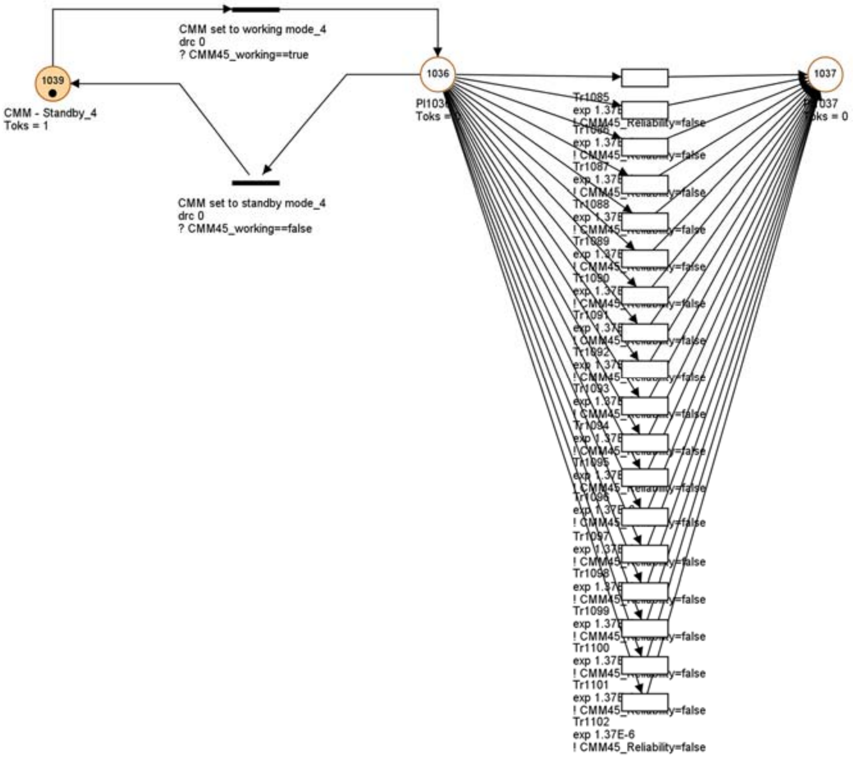


Fig. 84 - Set of 18 bearings (similar models)

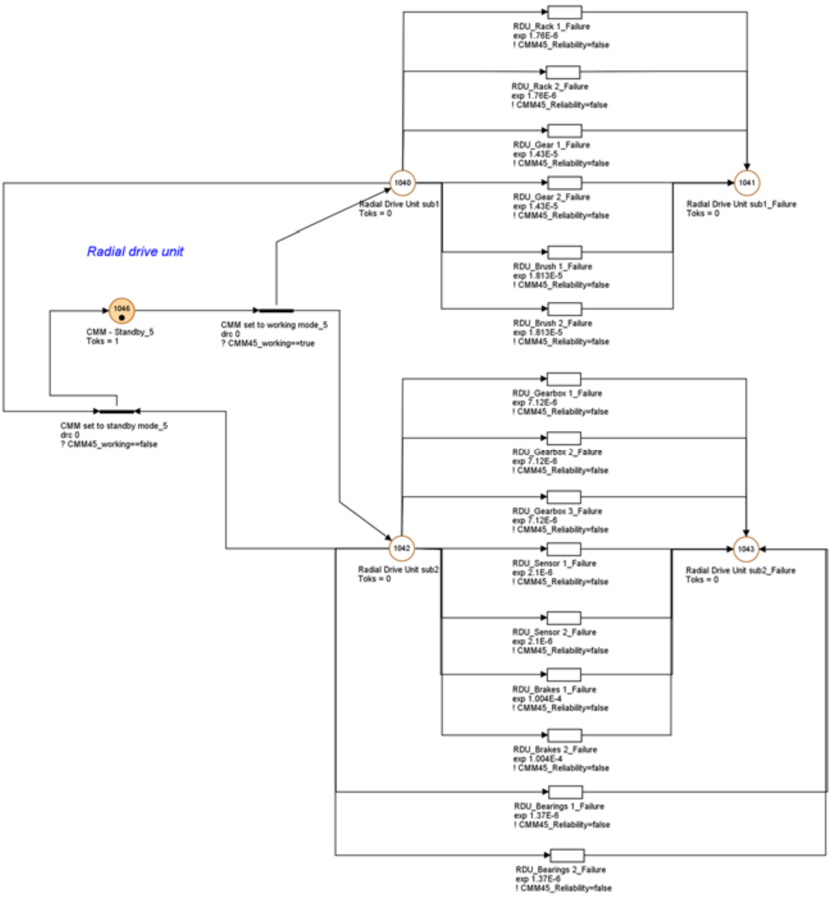


Fig. 85 - Radial Drive Unit

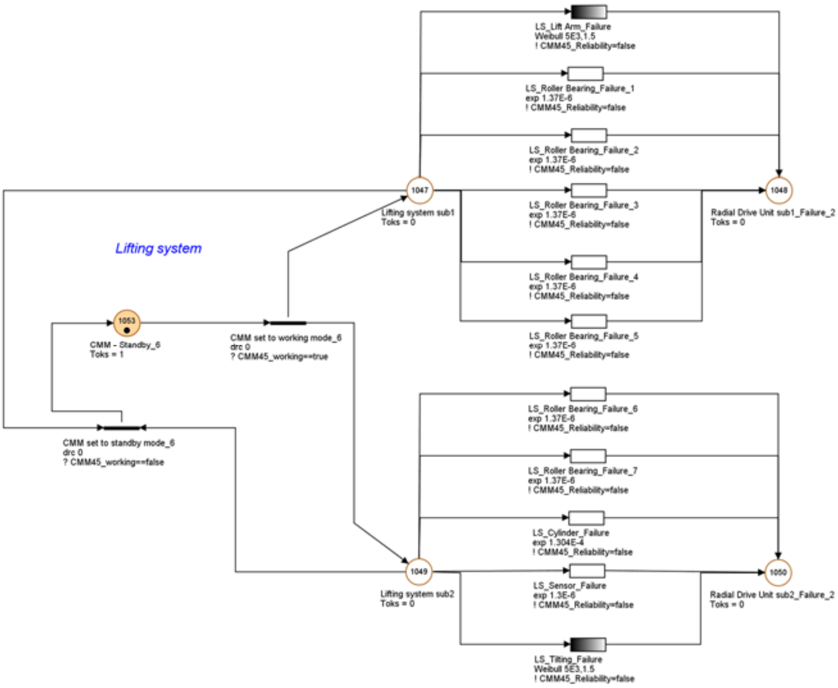

LS_Lift Arm_Failure
Weibull 5E3,1.5
! CMM45_Reliability=false
LS_Roller Bearing_Failure_1
exp 1.37E-6
! CMM45_Reliability=false
LS_Roller Bearing_Failure_2
exp 1.37E-6
! CMM45_Reliability=false
1047
Lifting system sub1
Toks = 0
LS_Roller Bearing_Failure_3
exp 1.37E-6
! CMM45_Reliability=false
1048
Radial Drive Unit sub1_Failure_2
Toks = 0
Lifting system
LS_Roller Bearing_Failure_4
exp 1.37E-6
! CMM45_Reliability=false
1053
CMM - Standby_6
Toks = 1
CMM set to working mode_6
drc 0
? CMM45_working==true
LS_Roller Bearing_Failure_5
exp 1.37E-6
! CMM45_Reliability=false
LS_Roller Bearing_Failure_6
exp 1.37E-6
! CMM45_Reliability=false
CMM set to standby mode_6
drc 0
? CMM45_working==false
LS_Roller Bearing_Failure_7
exp 1.37E-6
! CMM45_Reliability=false
LS_Cylinder_Failure
exp 1.304E-4
! CMM45_Reliability=false
1049
Lifting system sub2
Toks = 0
LS_Sensor_Failure
exp 1.3E-6
! CMM45_Reliability=false
1050
Radial Drive Unit sub2_Failure_2
Toks = 0
LS_Tilting_Failure
Weibull 5E3,1.5
! CMM45_Reliability=false

Fig. 86 - Lifting system of the CMM (hydraulically actuated)

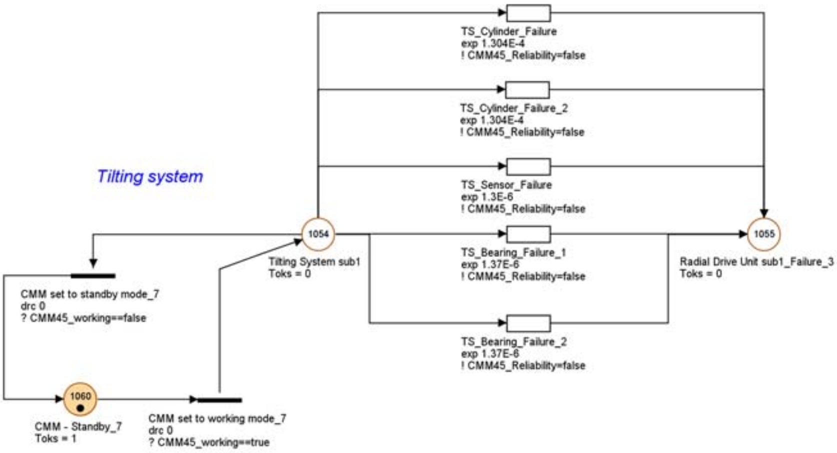


Fig. 87 - Tilting system of the CMM (hydraulically actuated)

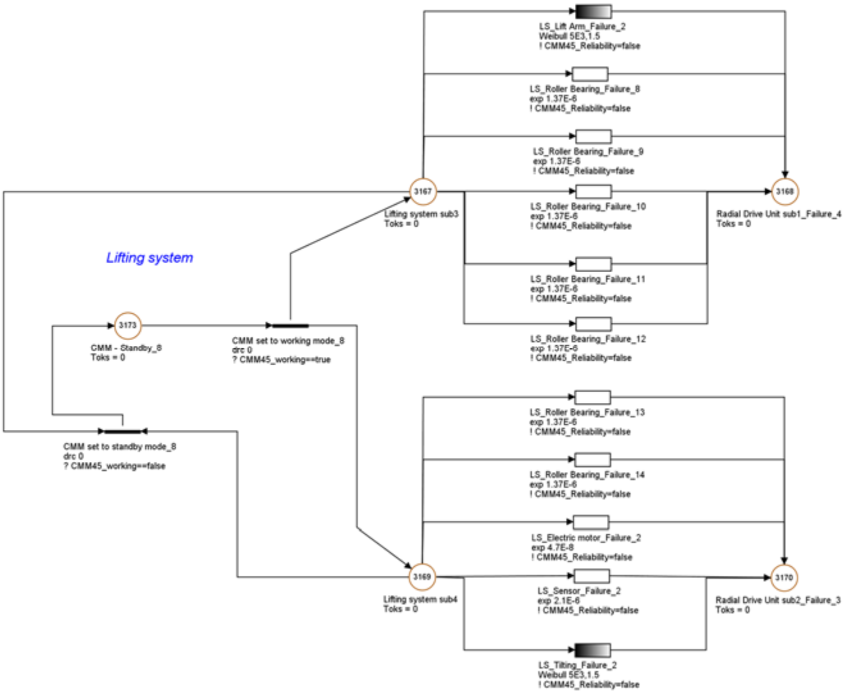

LS_Lift Arm_Failure_2
Weibull 5E3,1.5
! CMM45_Reliability=false
LS_Roller Bearing_Failure_8
exp 1.37E-6
! CMM45_Reliability=false
LS_Roller Bearing_Failure_9
exp 1.37E-6
! CMM45_Reliability=false
3167
Lifting system sub3
Toks = 0
LS_Roller Bearing_Failure_10
exp 1.37E-6
! CMM45_Reliability=false
3168
Radial Drive Unit sub1_Failure_4
Toks = 0
Lifting system
LS_Roller Bearing_Failure_11
exp 1.37E-6
! CMM45_Reliability=false
3173
CMM - Standby_8
Toks = 0
CMM set to working mode_8
drc 0
? CMM45_working==true
LS_Roller Bearing_Failure_12
exp 1.37E-6
! CMM45_Reliability=false
LS_Roller Bearing_Failure_13
exp 1.37E-6
! CMM45_Reliability=false
CMM set to standby mode_8
drc 0
? CMM45_working==false
LS_Roller Bearing_Failure_14
exp 1.37E-6
! CMM45_Reliability=false
LS_Electric motor_Failure_2
exp 4.7E-8
! CMM45_Reliability=false
3169
Lifting system sub4
Toks = 0
LS_Sensor_Failure_2
exp 2.1E-6
! CMM45_Reliability=false
3170
Radial Drive Unit sub2_Failure_3
Toks = 0
LS_Tilting_Failure_2
Weibull 5E3,1.5
! CMM45_Reliability=false

Fig. 88 - Lifting system of the CMM (electrically actuated)

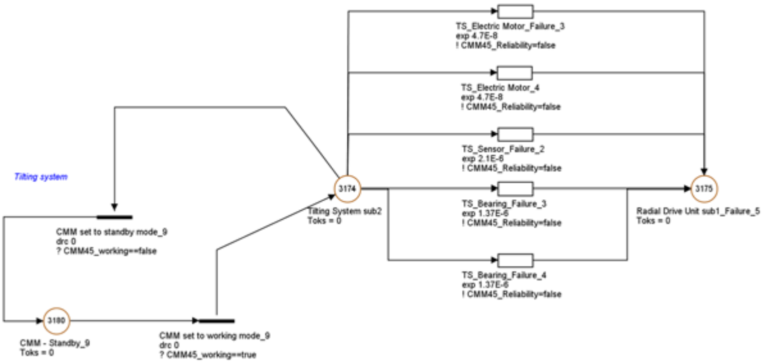


Fig. 89 - Tilting system of the CMM (electrically actuated)

Series title and number

VTT Science 140

Title	**Quantitative evaluation method for the verification of complex mechatronic systems** Development of a reliability-based design process using stochastic Petri Nets
Author(s)	Romain Sibois
Abstract	The verification of complex engineering systems from the very early phases of the design process is of primary importance, as it directly influences performance and system functionalities. Traditional design approaches aim at using simulations as a set of tools during the verification process. However, the current trend in the industry is towards simulation-based design processes in an iterative manner so as to constantly evaluate the system development. This perspective conveys the design process towards a verification-based design process. In the very early phases of the design process, evaluating different concepts for further development is not without problems, since a certain amount of product information is missing in the early phases. Therefore, traditional approaches have aimed at considering expert's opinions as the main evaluation criteria for assessing pre-concepts and concept designs. However, qualitative-based methods are highly limited according to expert's subjective judgements, level of expertise, as well as the ability to take into account multidisciplinary criteria in the case of complex systems. This dissertation presents research work related to the verification-driven design process of complex mechatronic systems using a stochastic reliability method for evaluating the concept design from the early phases of the product development. The main objective of this thesis consists in demonstrating the advantages of an innovative system design process based on a quantitative evaluation method using reliability as the main criteria. This thesis reviews the state of the art of the verification and validation process, describes different trends in the system design processes towards simulation-based design processes and reviews the best practices of decision-making processes in the engineering field. The work conducted during this thesis consists of the development and modelling of the verification-driven design approach. The method uses the stochastic Petri Net approach for modelling the operational and functional sequence of the system as well as its dysfunctional behaviour. Reliability parameters of each concept are estimated based on their level of design and thus various concepts can be evaluated against each other. The method is applied to case studies that consist of the development of a Remote Handling system for the maintenance of a fusion reactor called DEMO. The results confirm the benefit of such a method for designing and evaluating the concept design from the very early phases of the system development. The purpose of this research is to maintain the usefulness of the findings for other developments at a larger scale and in other fields than fusion engineering.
ISBN, ISSN, URN	ISBN 978-951-38-8473-4 (Soft back ed.) ISBN 978-951-38-8472-7 (URL: http://www.vttresearch.com/impact/publications) ISSN-L 2242-119X ISSN 2242-119X (Print) ISSN 2242-1203 (Online) http://urn.fi/URN:ISBN:978-951-38-8472-7
Date	December 2016
Language	English
Pages	167 p. + app. 15 p.
Name of the project	
Commissioned by	
Keywords	Verification and Validation, Design Process, Reliability, Stochastic Petri Net, Decision Making process, Complex Systems, Fusion Engineering
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

VTT SCIENCE 140 Quantitative evaluation method for the verification of...

Quantitative evaluation method for the verification of complex mechatronic systems

Development of a reliability-based design process using stochastic Petri Nets

The verification of complex engineering systems from the very early phases of the design process is of primary importance, as it directly influences performance and system functionalities. The current trend in the industry is towards simulation-based design processes in an iterative manner so as to constantly evaluate the system development. This perspective conveys the design process towards a verification-based design process.

This dissertation presents research work related to the verification-driven design process of complex mechatronic systems using a stochastic reliability method for evaluating the concept design from the early phases of the product development. The main objective of this thesis consists in demonstrating the advantages of an innovative system design process based on a quantitative evaluation method using reliability as the main criteria. The method uses the stochastic Petri Net approach for modelling the operational and functional sequence of the system as well as its dysfunctional behaviour. Reliability parameters of each concept are estimated based on their level of design and thus various concepts can be evaluated against each other.

The method is applied to case studies that consist of the development of a Remote Handling system for the maintenance of a fusion reactor called DEMO. The results confirm the benefit of such a method for designing and evaluating the concept design from the very early phases of the system development.

ISBN 978-951-38-8473-4 (Soft back ed.)
ISBN 978-951-38-8472-7 (URL: http://www.vttresearch.com/impact/publications)
ISSN-L 2242-119X
ISSN 2242-119X (Print)
ISSN 2242-1203 (Online)
http://urn.fi/URN:ISBN:978-951-38-8472-7