NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Reliability Systems Engineering for the Shell Eco-marathon Competition

by

Hossein Neizan Hosseini

A thesis submitted in partial fulfillment for the degree of Master of Science

in the

Faculty of Engineering Science and Technology
Department of Production And Quality Engineering

January 28, 2015

Abstract

Today, companies have a great attention to their product's cost and time-to-market, to become more competitive in the global market. Reliability engineering as one of the most important topics in system engineering is employed by companies to not only assess the value of the product, but also to identify, prevent, and reduce the risks of potential failures associated with design and manufacture of a product.

This study is conducted to implement reliability systems engineering in DNVGLFF 2015 as a partial preparation of DNVGL prototype to participate in SEM 2015. The author's objective is to investigate the effect of reliability engineering on DNVGL prototype system. The scope of this thesis is mainly focused on the initial three stages of the system life-cycle.

The former DNVGL team have been faced with problems in the prototype's braking system during the completion. As a result, the author decided to apply design for reliability (DFR) techniques on braking sub-system with the aim of identifying potential failures and propose possible solutions to mitigate their risks. In doing so, the reliability methods including RBD, FMECA, and FTA are employed in this thesis.

Acknowledgements

I would like to give my gratitude and appreciation to my supervisor, Dr. Cecilia Haskins, for her great support, weekly feedback, and for being generous. Without her advice, I wouldn't have grown in the field of system engineering. Finally, I would like to give my sincere thanks to Dr. Erlend Alfnes, who gave me the opportunity of studying in NTNU.

Abbreviations

DNVGL	Det Norske Veritas and Germanischer Lloyd
DNVGLFF	Det Norske Veritas and Germanischer Lloyd Fuel Fighter
SEM	Shell Eco-Marathon
NTNU	Norwegian University of Science and Technology
IEEE	Institute of Electrical and Electronics Engineers
SE	Systems Engineering
CE	Concurrent Engineering
DFX	Design For X
DFMA	Design For Manufacture And Assembly
DFM	Design For Manufacture/Design For Maintainability
DFS	Design For Safety
DFR	Design For Reliability
MTTF	Mean Time To Failure
MTBF	Mean Time Between Failure
RBD	Reliability Block Diagram
FMECA	Failure Modes Effect, Criticality Analysis
FTA	Fault Tree Analysis
MCS	Minimal Cut Set

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

This thesis is conducted to apply design for reliability techniques as a part of principles of systems engineering in order to contribute to the DNVGLFF team to better acquire requirements specification, plan, and increase reliability of the legacy system. The main concentration of this thesis is on design for reliability in the first stages of the system development. Also, assigned systems engineer of this project endeavors to make a reliability plan not only for this year project, but also for next future contest driven projects. In order to obtain better insight of the thesis, a brief story of the competition is given in the next section.

Systems engineering is considered as a technique that gathers various engineering and science disciplines and uses their knowledge to achieve a goal through the planning and development stages of a system. Systems engineering mostly is employed to solve a complex engineering problem in an effective and efficient manner. There is a saying that system engineering is mainly involved in development of new technological possibilities with the aim of putting them to use as rapidly as economic, and with considering all constraints [Online, 2014].

There is no industry that can continue effectively without the application of reliability engineering. Today, this discipline as one of the most important topics in

systems engineering has been developed to the high degree as the need for that is much felt than before [Clausing and Frey, 2005]. The reason behind that is the growth of products with high complexity in their life cycle. According to [Kececioglu, 2002, P. 2], reliability engineering is a set of techniques which "...provides theoretical and practical tools whereby the probability and capability of parts, components, equipment, products, subsystems, and system to perform their required function without failure for desired period and specified environment,...".

Although, reliability engineering can be used for development, manufacturing, testing, and delivering of the system, however, design is the most critical stage in system development that the reliability engineering must be integrated into it [Yang, 2007a]. The reason behind is that any changes in the system in design phase is considerably less expensive than the next phases [Avontuur and van der Werff, 2001, Soleimani and Pourgol-Mohammad, 2014].

In designing and developing of vehicles, reliability play a significant role to describe their level of performance and quality [Popovic et al., 2011]. Today, reliability methods and robust engineering techniques help engineers to identify potential failures and reduce their impact on the whole system. This needs detailed information about vehicle parts and components, and the potential failure modes that must be recognized as early as possible in the system lifecycle [Popovic et al., 2011]. According to [Zhang and Liu, 2002], the primary objective of vehicle design is to increase the reliability and safety of the vehicle components. For example, damage to a critical component of a vehicle, might be at the cost of the accident. For this reason, it is important to analysis the reliability of the critical subsystems such as braking subsystem, wheels, etc., to avoid such a significant event.

1.1.1 History

Shell Eco-Marathon (SEM) is a unique race that gathers students around the world and challenges them to design, produce and drive the most energy consumption efficient vehicle. This completion is held as three events in different cities in Asia,

Americas and Europe to observe the student's performances, and track that team drives further with minimum usage of energy [She, 2014]. The energy sources can be diesel, petrol, liquid fuel made from natural gas, and electricity supplied from batteries and solar panel. SEM 2015 takes place in Manila, the Philippine, Detroit, Michigan, and Rotterdam, the Netherlands. Shell Oil's Wood River Laboratory was the first place that the Shell mileage marathon was started by an argumentation among engineers about efficient usage of fuel. Today, the primary goal of Shell with the competition is to spark debate about the future of mobility and inspires young engineers to push the boundaries of fuel efficiency [W.S.Afleck, 2013]. During the last years, this goal has been achieved and at time goes by significant result will be achieved. For instance, some of the pioneer vehicles have managed to go 3000 Km per litter of fuel. Although, it is not fair to compare these vehicles with ordinary cars, however, this is a beginning of having the future with low usage of energy among typical cars.

1.1.2 Vehicles Classes

According to the SEM rules, six propulsion systems categories are allowed to participate in the competition. Bio-fuel, hydrogen, fuel made from natural gas (GTL), diesel, and conventional petrol and electricity are organized into the categories. Also, solar panel, as supporting energy source, can be used into all classes. Two different classes participate in this competition: the Urban concept and the Prototype class. The propulsion systems mentioned previously can be applied to both classes that based on their propulsion system, and they can participate in twelve different races. Competitors, who intend to participate with prototype, need to achieve the best possible mileage. They have full freedom in terms of designing and developing of the Prototype. The prototype class is considered as most remarkable class and oldest one to participate. The main aim of the Prototype is to minimize the usage of energy consumption. This class is a little smaller than the Urban concept, and it has different shape and features such as three wheels, droplet shaped body and the horizontal driving position. Another class is

the Urban concept that completely inspired from the conventional cars. Designer and developer of the Urban concept must following more restrictive rules than Prototype. For example, some of this rules point out that every Urban concept must have doors, head and tail light, windshield wiper, and luggage compartment [Johannes Aalberg, 2014].

1.1.3 NTNU and Shell Eco-marathon

The DNV GL Fuel Fighter team is organized by NTNU to participate in the Shell Eco-marathon on behalf of Norway. The team is usually formed by fourth and fifth-grade student from different educational background to construct a new vehicle or improve the legacy one in order to take part in the race. Since 2008, DNVFF has competed in the SEM races and has got different awards. They also couldn't raise many of the SEM's cups due to failure in testing, and so on. 2011 was the first year that the team decided to recruit a systems engineer to have better insight of the system and sub-systems and tried systematically to find the solution for their potential problems. Despite it is not fair to believe that the systems engineer was the only reason of winning of the team in year 2012, however, systems engineer has contributed very well to achieve this goal. The assigned systems engineer of DNVGLFF 2015, with inspiration from the former systems engineers, tended to apply the SE principles into the development process of vehicle. Also, he tried to have more focus on design for reliability of the system that also is considered as the main aim of this thesis.

1.2 Motivation

Despite, the design of the prototype class of the previous team was very attractive, and it was selected as one of the ten most exciting newcomers, the design award went to another team. Also, it had lost the safety award to its competitor, due to not testing the car before the competition. These problems of the Prototype class

along with other reasons, caused that the team couldn't stand on their real place in the contest, although they put a lot of effort on it.

An analysis of the prototype system in a knowledge-transfer meeting with the previous members of the DNVGL team revealed that they had been facing a major problem: having failures in the system. It is true that even the most advanced systems have failures. But, the central issue is: to what extent failures must be tolerable? For example, in an aerospace, as long as a system with a failed component can function at least for the length of the mission and the potential failure risk will be mitigated prior to the next mission, the failure can be bearable. In order to do so, reliability engineers besides the designers must foresee the critical failures during the requirement analysis and incorporate them into the design.

The primary motivation of this thesis is to apply reliability engineering for one of the vulnerable subsystems: prototype braking system. Also, the reliability engineering and safety analysis of the system are carried out for the first time in the DNVGLFF projects. At the beginning, it was decided to examine the whole prototype system in terms of the reliability. However, due to lack of time, it was recommended by the safety engineer of the DNVGL to select one of the systems that expected to not work very well. As a result, since the previous team was faced a couple of problems with the braking system during the competition, it is wise to make a reliability plan for this critical system. Some of these problems are explained in [Johannes Aalberg, 2014].

1.3 Problem Statement

In the current state of the prototype braking system, number of concerns related to the reliability of the system arise. Some of these concerns are as follow:

1. How reliability engineering can be valuable for the DNVGLFF system?
2. How the Prototype braking system can be designed to be reliable?

3. To what extent the potential failures can be tolerable?

This thesis is conducted in response to the questions raised above. In order to do so, first all requirements of the prototype system were organized into a document. Then, the whole structure of the system(prototype) was designed with its subsystems and components. Finally, all steps needed for design for reliability of the system was carried out. These steps including reliability block diagram(RBD), failure mode effect and critically analysis(FMECA), fault tree analysis (FTA), and failures analysis.

1.4 Scope

In reality, a couple of different failures in braking system can be pointed out. These potential failures might be from the components such as actuator, friction lining, seals, bearing, and hydraulic [CARDEROCKDIV, 2010]. Failure in one of these components might have an adverse effect on functioning of the braking system. Also, the failure might be due to not well-design of the system. In this project, all these concerns are analyzed. In order to perform the said analysis, following steps are carried out:

1. Develop literature review in systems engineering and design for X.
2. Develop literature review in reliability theory and reliability engineering.
3. Conduct qualitative analysis of braking system through RBD, FMECA, and FTA.
4. Discuss about the contribution of the reliability systems engineering in DNVGLFF project.

Chapter 2

Research Methodology

The research method of this thesis is based on 1)reviewing literature and 2)case study. A method is designed to qualitative analyze the reliability of the prototype braking system based on the literature to propose potential solution for the mentioned research problem. This model is adopted from [Yang, 2007b]. This chapter explains the research methodology in details.

2.1 Literature Study

One of the important parts of this thesis is to review the proper literature to identify the existing body of knowledge. In this thesis, the literature study aims to response to the research question of how to implement design for reliability plan for DNVGLFF prototype vehicle.

In this thesis, it has been tried to use the reliable literature including book, journals paper, thesis, and so on through valid databases such as NTNU library, ScienceDirect portal, SAGE journal, and other online sources. Also, the author tried to pay more attention to IEEE Reliability Society, Reliability Engineering and System Safety journal from Elsevier portal in order to gather proper information in the field of reliability. The keywords used in this thesis were systems engineering, reliability engineering, and design for reliability. Also the other keyword about

concurrent engineering and design for X are used as well. Although, the concept of concurrent engineering and design for X were not related to this thesis, but they were discussed to better show the aim of this thesis. One of the limitations of this thesis was the lack of information in reliability of the particular braking system used in prototype. Despite, there are number of available articles regarding general braking system, but limited number of those articles could be used in the context of this thesis. The couple of these article which relatively are related to this thesis are listed in table 2.1. Also, the reliability study is done for the first time in such projects and there is no information regarding reliability of the system from the former teams.

Type of Brakes	References
Motorcycle	[Boniardi et al., 2006]
Automobile	[Sharvia and Papadopoulos, 2015, Sinha, 2011]
Truck	[Zhifa et al., 2011]
Train	[Cheng et al., 2009, Kohda and Fujihara, 2008, Min et al., 2010, Tan et al., 2012]
Airplane	[Al-Garni et al., 1997]

TABLE 2.1: Related work references

2.2 Case Study

Generally, cases studies are used when questions such as "WHY", or "WHAT" are being raised [Yin, 2014]. Same reference also has mentioned three different research purpose- exploratory, descriptive, or explanatory. Exploratory researches are those in which the problem has clearly been defined, and the potential solution(s) is(are) consequently proposed. By assuming that the problem statement in this thesis regarding reliability engineering in braking system of DNVGL prototype class is defined, and a solution for reaching this goal is specified, this study can be considered as an exploratory research.

This thesis is conducted based on real life case study where the author endeavored to apply his finding in reliability. Also, these findings have been assessed through analyzing the result. According to [Jung et al., 2012] reliability blocks diagram (RBD), failure mode effect, and critically analysis (FMECA), and fault tree analysis (FTA) are the most proper reliability tools to analyze the level of the system reliability. The outcomes from the mentioned tools are analyzed and the possible solution are proposed. All these processes are well-explained in this thesis.

The reliability and validity of the gathered information are the key concerns of the research at this stage. Many researchers "go to great lengths" to make sure that the interpreted information is both valid and reliable [Bronwyn Becker and Palmquist, 2012]. All gathered information in this project are gained through cross-functional meeting with all responsible engineers. Particularly, the information regarding the braking system has been checked with its assigned engineer in the form of expert judgment. Expert judgment is an alternative way to elicit information from expert person, when the statistical information doesn't exist or it is not available [Vatn, 2013]. Also, regularly feedback from the responsible supervisor, added many value to validity of this project.

2.3 Research Model

Figure 2.1 is illustrated to better show the process of the research in this thesis. This model consists of three phases. The assigned system engineer has concurrently perused two goals. First, doing the system engineering process which including requirements acquisition, high level design architecture, and the other tasks that are presented in this model. Second, following the design for reliability process. The main focus of reliability engineering in this project is at the phase 2 which is design and development. All tasks are discussed comprehensively in the body of this study.

As it shown in figure 2.1, in the first phase the requirements analysis has been done. This process including specifying all necessary system requirements as well

as specifying reliability needs, is performed to achieve the goal. In the phase 2, based on specified requirements, the system architecture was designed. This process including designing the high-level of system architecture. Also, designed system architecture was reviewed in the form of iterative process to see whether the specified requirements will be met. Concurrently, the reliability techniques for designing the system has been performed. As it can be seen in the picture, the reliability tools which have been applied in this phase are reliability modeling (RBD), reliability allocation, FMECA, FTA, and failure analysis. Finally, in in phase 3 the system has been tested regarding meeting the reliability requirements.

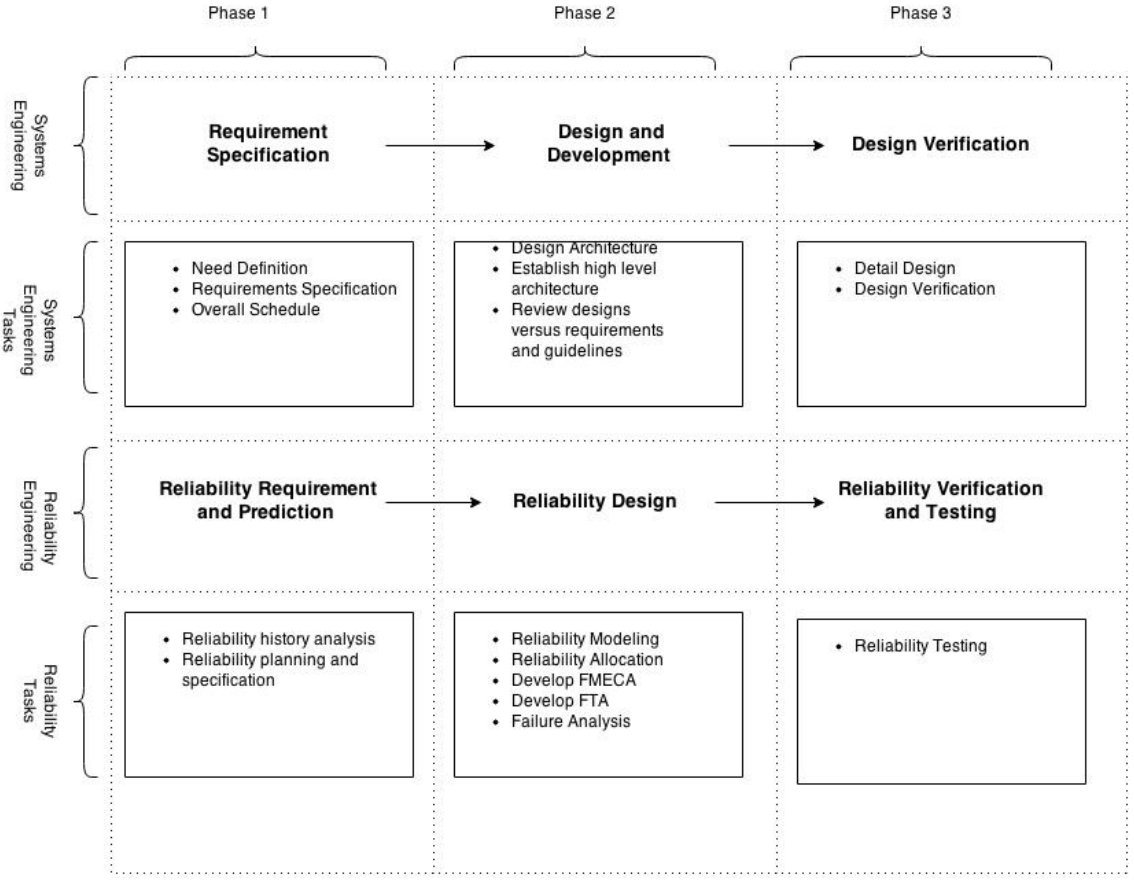


FIGURE 2.1: Research model used in this thesis adopted from [Raheja and Gullo, 2012]

Chapter 3

Background and Literature Review

This chapter is built based on literature and aims to give a proper explanation of systems engineering principles, design for X, and specially design for reliability in order to address the research questions.

3.1 Systems Engineering

"*A system is an assemblage or combination of functionally related elements or parts forming a unitary whole, such as a river system or a transportation system*" [Blanchard and Fabrycky, 1990, P. 17]. A system is not each set of facts, items, or method. Some connection can be found between a set of elements in a box, however, due to lack of functional relationships, it is not considered as a system. Also, interrelated components should functioning together to achieve common and specified purposes or objectives [Blanchard and Fabrycky, 1990].

Although, a system might have sub-systems, components, parts and its interfaces, however, each sub-system or even components might be a system per se. As a result, when a system is going to be developed, all purposes and objectives of each sub-system and components must be defined and understood explicitly.

Considering all these characteristics of a system under development, especially a complex one, is not an easy task. Therefore, systems engineering methodology is required, in order to consider all customer requirements into the system with specified outcome(s).

"*To this day, there is no commonly accepted definition of systems engineering in the literature*" [Blanchard and Fabrycky, 1990, P. 31]. There are a lot of definitions of systems engineering that are written based on its author or particular organization approach. One of the comprehensive definition of systems engineering belongs to International Council on Systems Engineering (INCOSE). According to [Haskins, 2010, P. 7], Systems engineering is "*an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs*".

3.1.1 Need for Systems Engineering

One of the main reasons that the need for systems engineering is felt is the ambiguity in requirements acquisition and the absence of proper planning. Usually, the process of developing a system, can be divided into four phases [Kamrani and Azimi, 2012];

- conceptual design
- preliminary design
- detailed design
- development and operation and management

Studies show that the current methods can only cover the last two phases. These last two phases comprise 75 percent of total project cost. However, through applying systems engineering techniques to the initial concept design and preliminary architect, the expenditure of next phases can drastically be reduced. This contribution is done not in a direct way. Systems engineering principles through improving the quality of the design, reducing failures and defects, reducing development time period, and improving the relation between component and process can lead to lower total cost of the project [Kamrani and Azimi, 2012].

Many projects are facing with problems and challenges such as lag behind the schedule, run over the expected expenditures, or poor functionality as planned. Systems engineering is more about design and integration of the proposed system(s) with requirements acquisition and broad outlook. The main concentration of systems engineer is to identify and evaluate requirements, alternatives, uncertainties and risks, and manage the technical activities of the project. In the initial phase that is called identification phase, systems engineer aims to determine the different trade-offs and then continues with selected design(s). Analyzing the trade-offs, and then formulation of the methodology techniques are done in the second phase. Finally, the assigned systems engineer decides on the best choice [Gonzalez, 2002].

Sometimes the boundary of systems engineering and project management is not clear. For this reason, it is necessary to give an insight to the reader about the differences between systems engineering and project management responsibility and tasks.

3.1.2 Project Management and Systems Engineering

According to [Pyster et al., 2012], effective communication between the system engineer(SE) and project manager(PM) leads to mission accomplishment. The link between the project manager and system engineer must be established as early as possible.

Management issues are the primary concern of PM, while, technical problems are the main concern of SE. PM leading the project management team, but the systems engineering team is run by an experienced and trained SE, who has good knowledge in technical fields. PM aims to lead the project to success with respect to the limitations while SE aims to lead the system to success. According to [Kamrani and Azimi, 2012] lack of effective systems engineering causes failures in projects. Some of the held on common issues that have an impact on the whole project such as schedule changes, resource reallocation, risk changes, and system changes [Pyster et al., 2012]. An example of SE and PM interaction is well illustrated in figure 3.1.

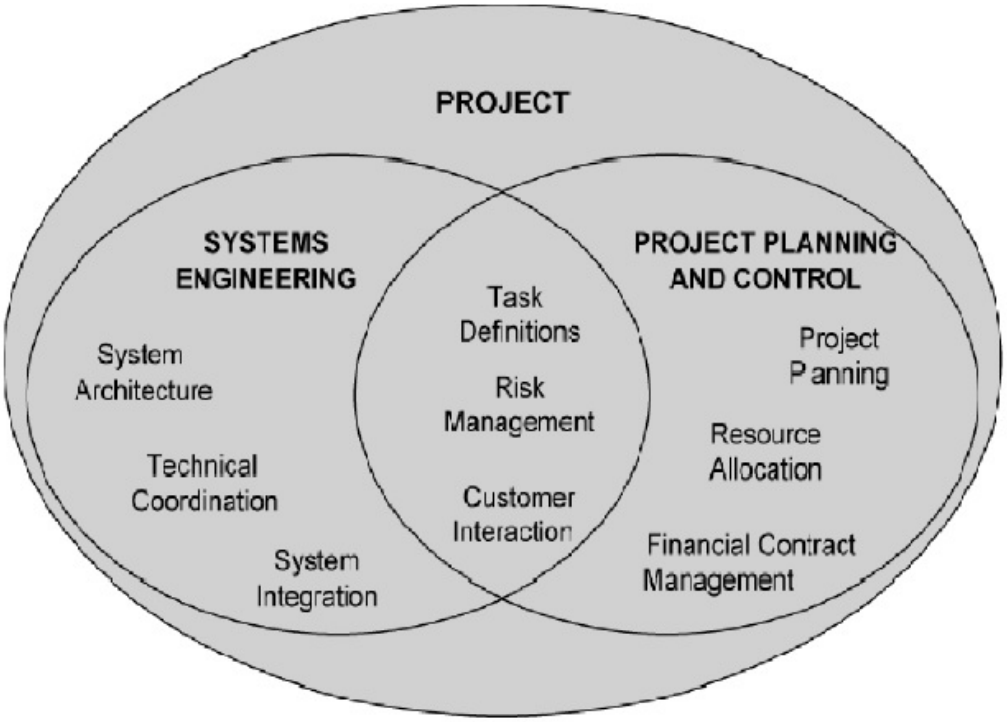


FIGURE 3.1: SE and PM overlap [Kossiakoff and Sweet, 2003]

3.1.3 Systems Engineering Roles

Before systems engineering roles are discussed, it is better to clarify the difference between systems engineering and systems engineers. There has been much discussion about the difference between Systems Engineering and Systems Engineers. The question is, whether all of the engineers in a project must be involved as

"systems engineer" or the title of systems engineering is for specific engineers with particular skills. [Sheard, 1996], categorized systems engineering roles into twelve parts that can be seen in figure 3.2. In the following, only those roles that are relevant to this project are described.

Role	Abbr.	Short Name
1	RO	Requirements Owner
2	SD	System Designer
3	SA	System Analyst
4	VV	Validation/Verification Engr.
5	LO	Logistics/Ops Engineer
6	G	Glue Among Subsystems
7	CI	Customer Interface
8	TM	Technical Manager
9	IM	Information Manager
10	PE	Process Engineer
11	CO	Coordinator
12	CA	Classified Ads SE

FIGURE 3.2: Systems Engineering Roles [Sheard, 1996]

- *Requirements Owner*: Several requirements-related tasks are set together by this role. Translation of customer needs into technical requirements, and which system and subsystems must be architected and designed are defined by this role.

- *Systems Designer*: After the requirements and functional architecture are developed, a system designer makes the high-level architecture and selects critical components. In this section, the important part is that the systems designer makes sure that all requirements incorporated into designed system.

- *Systems Analyst*: In this role the systems analyst confirms whether the designed systems will meet specified requirements. Conventional analyzes including systems power, weight, input, and output, interface traffic, and so on.

- *Validation and Verification(VV)*: The systems verification is planned and implemented by VV engineers to ensure the systems will meet specified requirements as designed. VV engineers are responsible to respond to unexpected and unwanted events with the best possible understanding of the system design. Also, they must be aware which experts need to be called when needed.

- *Glue*: This role also is called system integrator in which the systems engineer acts as a "proactive troubleshooter", tries to find problems and plans to prevent them.

- *Coordinator*: The broad viewpoint of the system engineer makes him/her capable of coordinating the groups and resolving the system issues. Engineering of the complex system needs coordination.

Thus far, general aspects of systems engineering have been discussed. In the following, systems engineering process are presented.

3.1.4 Systems Engineering Process

Despite there is a consensus concerns about systems engineering principles and objectives, the process of implementation of its principles varies from a project to the next. The steps of implementing process and its approach are highly depending on the nature of the system application and the experience of the experts on the team [Blanchard and Fabrycky, 1990]. Developing a complex system fundamentally needs great commitments of resources in entire systems lifecycle. Also, the risks that might jeopardize the whole system must be identified and resolve as early as possible. In order to consider these factors, systems engineering methods must be conducted in a step-by-step manner. In this way, not only the success of each step is demonstrated, but also before making a decision to continue to the next phase, the basis for the next one is validated [Kossiakoff et al., 2011].

3.1.5 System Life-Cycle

According to [Haskins, 2010, P. 21], "*Every man-made system has a life cycle, even if it is not formally defined*". In system development, with respect to environmental issues, the life cycle must including development, production, and utilization as well as retirement stage when disposal of the system will happen. The role of the system engineer is crucial to the entire systems life cycle. System engineer does the organization of a system development from requirements acquisition through production process and systems disposal. System engineer must rest assured that all experts are adequately involved in their specified domain, and the significant risks are recognized and mitigated [Haskins, 2010].

A simple sequential development approach is shown in figure 3.3. The subsequent life-cycle begins with user requirement to the completion of the operation. This model shows a set of process from user requirements, through system requirements, architectural design, and development of the component to the testing phases of integration, installation and operation. By reviewing and monitoring each process boundary, a commitment is made to the next step. The information must be produced in a defined order in which the users, developer and designer are responsible for separate parts of the information. The components are produced and considered as an entity that must be fitting inside the overall system framework. Then, in order to complete the system, the components must be integrated [Stevens and Arnold, 1998].

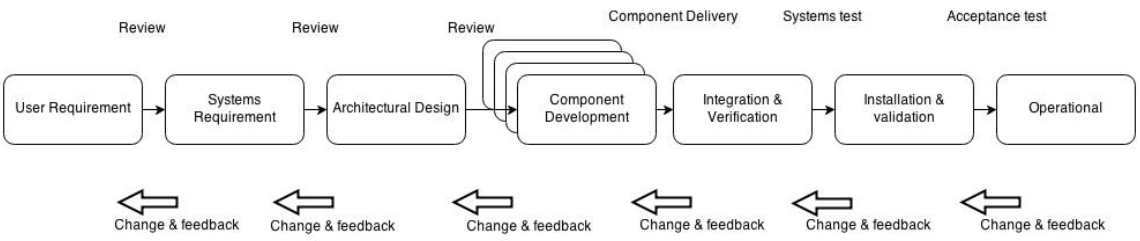


FIGURE 3.3: Simple System Life Cycle [Stevens and Arnold, 1998]

There are a large number of system life cycle models. One of the well-known system life cycle models is Vee model. Figure 3.4 shows a Vee model in which the

verification process is happening across the parallel links as well as defining the phases. In this model, the process of systems engineering starts from the left-hand side by describing what exactly must be produced. Then it continues by building the system from the components, and finally will end with the right-hand side by verifying the built system based on the left-hand side specification. The testing of the components during the integration phase is done based on the information produced to specify those components. The process of acceptance, integration, and verification of the components will continue until they are formed into a tested and completed system. In order to make works on the right-hand side easy, the hard work must be done on the left-hand side [Stevens and Arnold, 1998].

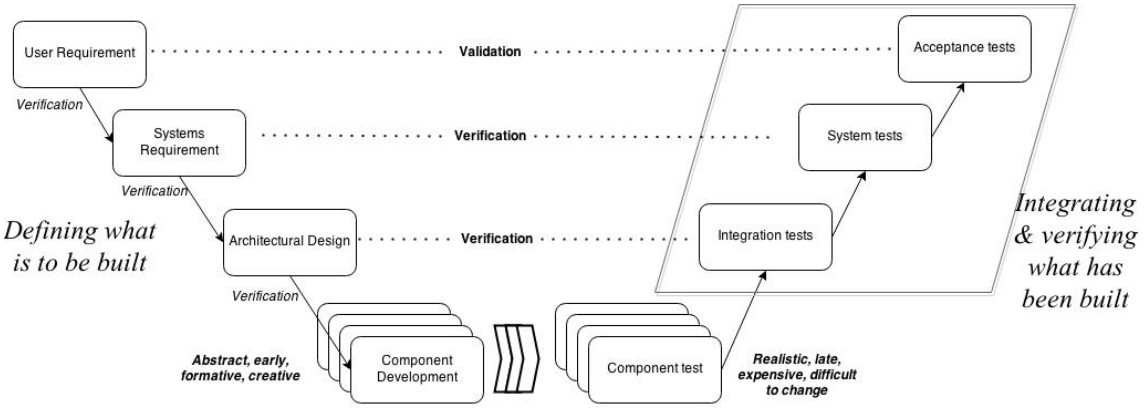


FIGURE 3.4: The Vee model from the simple life cycle [Stevens and Arnold, 1998]

3.1.5.1 User Requirements

In order to avoid misunderstanding regarding the actual meaning of the requirement in a system, one of the useful definitions of requirement is chosen and followed in this project. According to [Sage and Rouse, 2009, P. 209], "a requirement is a statement that identifies a capability or function needed by a system in order to satisfy a customer need".

The first step of defining a system is user requirements. In order to move toward success of the system, the primary users of the systems and their needs must be identified and satisfied respectively. The entire customer needs define how the process of system development will be. Requirements acquisition stage is

different from the other phases of the life-cycle and must be short and precise, and highly interactive. All requirements must be understood, even those that are not practical. Poor acquisition of user needs might leads to irreparable consequences later [Stevens and Arnold, 1998].

The process of user requirements acquisition must be carried out in the concept development stage of the system life-cycle. In many projects the views of the user might be considered, even those that are not necessary, that can causes confusion in decision-making. SE process translates the user's views of the desired system to a standard top-level program, which all participants can understand it. This process is called requirement analysis process [Haskins, 2010]. According to [Haskins, 2010, P. 72], "*The purpose of the Requirements Analysis Process is to transform the stakeholder, requirement-driven view of desired services into a technical view of a required product that could deliver those services*".

There are many tools and techniques that can be used to specify user requirements. Some of these tools are technical questionnaires and marketing, prototypes, and beta release of the system. Besides these techniques, trade-off analysis and simulation are very useful to select desired mission alternative by evaluating the project operational alternatives [Haskins, 2010].

The definition of the user requirements must be in the terminology of the problem domain that precisely specifies what the users intent to do with the system. In other words, definition of the user requirement should be from an operational viewpoint, instead of system functionality or equipment. It is important to distinguish between user and system requirements. In fact, system requirements are driven by user demand, and they must be kept separate. Unfortunately, this usually not happen in many project that leads to confusion and misunderstanding later [Stevens and Arnold, 1998].

The process of user requirements acquisition is well shown in figure 3.5. In this model, the process starting with defining user type, and capturing requirement from them. The gathered requirements must be reviewed and agreed by user, and updated into user requirement document (URD).

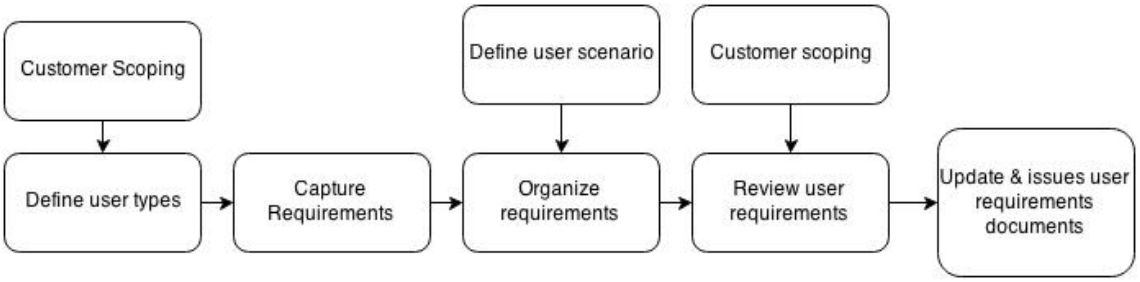


FIGURE 3.5: Capturing user requirements [Stevens and Arnold, 1998]

Given information from the user usually is short, general and might not be correct that lead to scattering the whole design decision. It is the system engineer's responsibility to turn this noisy information into measurable, testable requirements that are proper for moving the project toward success [Stevens and Arnold, 1998]. In order to do so, the requirements must be specified accurately. According to [Young, 2002, 2006], the characteristics of a good requirement are necessary, verifiable, attainable, complete, unambiguous, traceable, consistent, implementation-free, concise, and have a unique identifier.

3.1.5.2 System Requirements

In order to design an item in a system, first its requirements must be defined. Setting of the system requirements is a creative process. The primary focus of systems requirements analysis is to show what the system will do. In fact, system requirement analysis looks for a set of resources to meet a system needs. A system is formed based on system requirements, which is acting as linkage between user requirement and design. In other word, customer's system needs are translated into a design model through system requirements [Grady, 2014, Stevens and Arnold, 1998].

System requirements encompass both descriptive information and formal requirements. They are very conducive in several way such as, showing a short view of the system, allowing to conduct trade-offs and optimization before committing to the planned design, providing a good basis for design, and so on. Designers, test engineers, system engineers who are working on a smaller assigned part, and the

planner are individuals who use the systems requirements document. It is necessary to mention that the utilization of the word "document" does not mean that the information of a project is kept in a paper form [Stevens and Arnold, 1998].

Although, systems engineers are those who own system requirements, but the user also must be aware of the systems requirement to be sure that their needs will be met. In this way, the users can check their needs are being met, or at least observe which one will or will not be achieved. Also, the systems requirement gives an insight to the users to find out those that they didn't think through correctly. This is a good way to control the user requirements during the project period [Stevens and Arnold, 1998].

3.1.5.3 Architectural Design

Architecture process of a large-scale complex system is the heart of systems engineering. Such a architecture process is expected to be insufficient and disorganized if it is done without systems engineering process [Eisner, 2008].

Architectural design process aims to synchronize a solution that fulfills systems requirements. The process of architectural design is iterative. The systems engineers joined by related and significant experts in the system domain need to participate in this process. One of their responsibilities in this stage is to present the alternative solution. Once the alternative solution is given, technical analysis and decisions must be made as part of architectural design process to find a set of system elements and components [Haskins, 2010].

The simple process of architectural design is shown in figure 3.6. As it presented, architectural design determines what must be built, but not how. This process is highly creative and differs from project to project. Usually, in this stage the large cost of the project is fixed and it is hard to be changed. As a result, it must be done very carefully as well as the other system engineering process. This process through assigning functions to software, hardware, or people, transforms systems requirement into more explicit form.

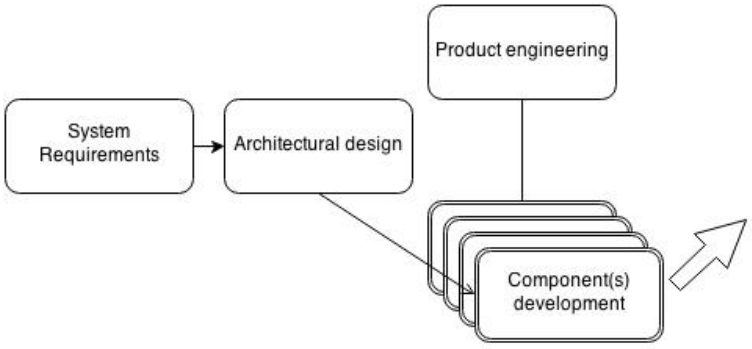


FIGURE 3.6: Architectural design process [Stevens and Arnold, 1998]

3.1.5.4 Verification, Validation, Test (VVT)

Verification, validation, and test (VVT) process aim to identify and correct the failures in the whole system. This process is done through a set of tools, and analytic methods to make sure the potential risks are reduced, and finally all customer requirements are fulfilled. As detecting the possible failures late leads to increase risk and cost, the VVT process must be performed in the first stages of the life-cycle as well as its final phases. The process of VVT can be complex, and its complexity depends on the complexity of the system [Pineda and Kilicay-Ergin, 2012].

The term of verification means to "*evaluate realized product against specified requirements*". The purpose of verification is to determine whether the final system met the planned customer requirements. In addition, the verification process tries to answer this question: Was the system produced correctly? [Engel, 2010, P. 16]. On the other hand, validation confirms whether the built (or will be built) system, meet the stakeholders needs. System validation ensures that the solution provided by the requirements and the system implementation is right for the customer problem. In addition, the validation tries to answer this question: was the right system produced? [Haskins, 2010]. The final term of VVT acronym is test, and it suffice to say, "*testing is operating or activating a realized product or system under specified conditions and observing or recording the exhibited behavior*" [Engel, 2010, P. 17].

3.1.6 Design for X

The following section will give a brief introduction to concurrent engineering, design for X. Also the other solution in product design such as design for manufacturing, design for maintenance, design for safety, and the design for reliability that is the main topic this thesis.

In today's dynamic market, the companies must response to the customer demand as fast as possible. Also, they should provide the products with a reasonable price, good quality, and prompt availability. In order to do so, they need to produce their products in an efficient way. Success stories show this can be achieved by using a manufacturing method that is called concurrent engineering (CE). In this method, all aspect of product's life cycle, at the design stage, are considered simultaneously. The CE approach is different from the traditional manufacturing process where after design phase products get noticed regarding their manufacturability, quality, safety, reliability, and so on, [Fohn et al., 1995].

In the traditional production method, product design was carried out serially. In this way, after completion of the design stage, the communication occurs only after completion of the specific phase. For example, designers define a product usually without consulting with manufacturing engineers. As the design is verified through simulation, prototype, etc., it goes directly to manufacturing department. Then, the manufacturing department defines the production process and determines the time and cost estimation. Then purchasing and quality departments are involved to propose their plan based on their responsibility. If any defect or error are discovered, it would directly pass back to the responsible department. This method was very costly as the whole process must be stopped for fixing any potential problem happened at any stage of the production process. However, CE prevents any bottleneck and rework in the production process, through collaboration of many people from different departments with the different point of view [Fohn et al., 1995].

One of the most practical approaches to apply CE is Design for X (DFX). The primary focus of DFX is on vital business elements of CE [Maskell, 1991]. DFX techniques and methods are considered as a part of detail design and are very conducive to improve the cost and quality of the product life cycle. Also, they increase productivity and efficiency using the concept of concurrent engineering [Maskell, 1991]. DFX techniques through systematic approaches try to analyzes design from different perspectives. [Holt and Barnes, 2010].

The letter "X" in DFX can be replaced by the performance ability of the design such as manufacture and assembly, maintainability, safety, reliability, or even the environment. There are a lot of design purposes including the serviceability, life cycle cost, and so on, which due to being irrelevant to this project, they are not described. In order to achieve the particular purpose, some of these abilities can be combined. For example, in order to develop an airplane, and due to the sensitivity of this product, a couple of design for safety, reliability, manufacturability, etc., must be taken into account.

3.1.6.1 Design for Manufacturing and Assembly

Traditionally, manufacturing process makes design and production been implemented independently. This kind of process usually resulted in poor manufacturing, assembly, safety, maintenance, and finally increases in time and cost. Design for manufacturing and assembly (DFMA) is one of the DFX family, and new technique to cope with these kinds of problems. The combination of design for manufacturing (DFM) and design for assembly (DFA) makes DFMA that they are discussed below respectively.

DFM and DFA, not always work very well, and might create a conflict. For instance, DFM mainly focuses on simplifying components while DFA emphasis on simplifying the structure of the product by combination of parts. Implementation of one of these techniques per se might result to false economics. For example, a minor decrease in production cost is equivalent to increase in assembly cost and

vice versa. For this reason, both of these methodologies must be applied together, under the heading DFMA [Holt and Barnes, 2010, P. 124].

This recognition, which the cost of producing a product is mainly defined by its design, develops DFMA. If the manufacture and assembly are not considered in the design, some products are either impossible to produce or much less profitable than they could be. By employing these techniques, through minimizing manufacturing and assembly cost and avoiding unnecessary design iteration, the time and cost of product development will be drastically reduced [Holt and Barnes, 2010].

Design for Manufacturing DFM is a set of techniques that determines the features of a product that helps to have an efficient and high-quality manufacture. The primary goals of these methods are minimization of cost and time. In fact, each product can be made by many production processes with different characteristics that must be considered during the design stage. DFM tools and methods are defined based on what aspects of product development should be focused. For example, the type of product, its size, the separate or continuous production process, and many other issues define these aspects [Filippi and Cristofolini, 2009].

Design for Assembly DFA is a design method that can be applied in two ways, 1) a tool for analyzing the assembly, 2) a guide for developing the assembly process. In tradition form of assembly planning, after designing the product, the engineers estimate the possibility of assembly through analyzing all the factors that might affect the process of assembly, and suggest the best solution. On the other hand, in the DFA methods, the knowledge and experiences of the assembly expert are incorporated into the design stage [Xie, 2003]. In the process of assembly, there are two factors that affect the assembly cost of a product. 1) "the total number of parts and 2) the ease of handling, insertion, and fastening of the parts". The evidences show that DFA methods provide many guidelines to reach this goal [Kuo et al., 2001, P. 244].

3.1.6.2 Design for Maintainability

Designing and developing a system that can be maintained effectively, with minimum time and cost, and with minimum usage of the resource is one of the important objectives of systems engineering. Maintainability can be defined as "ability of a system to be maintained, whereas maintenance constitutes a series of actions to be taken to restore or retain a system in an effective operational state" [Blanchard and Fabrycky, 1990, P. 425]. Maintainability is parameter that is dependent on the design, while maintenance is achieved after design.

Maintenance elements describe maintenance concepts and requirements for any system. These elements including the analysis and verification customer needs. The selection of each element is necessary and depends on specific requirements. These elements, as well as their connection, are shown in figure 3.7. Before designing the system, these elements must be studied to achieve effective maintenance. During the system development, some other maintenance elements might be found that need to be fully integrated into the whole system. It would be very time and cost efficient if these elements be found as early as possible [Mital et al., 2014].

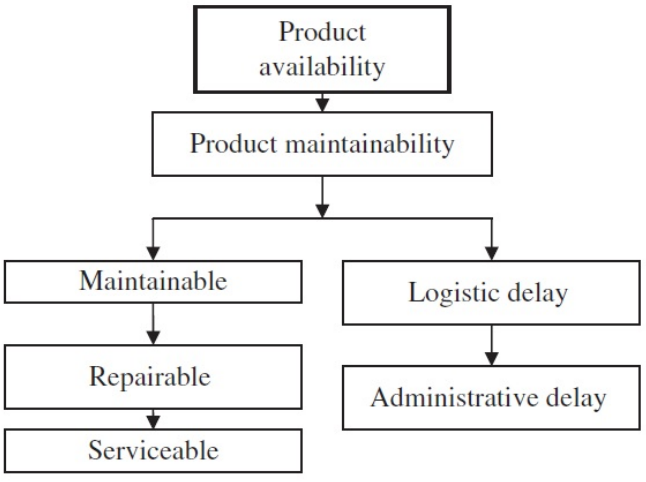


FIGURE 3.7: maintenance elements [Mital et al., 2014]

3.1.6.3 Design for Safety

In this section, a brief introduction about design for safety is given. Despite, the primary focus of this project is on design for reliability, it is necessary to understand the concept of design for safety as "design for safety and design for reliability are inseparable" [Moriarty, 2012, P. 253].

Design for Safety (DFS), same as all design for Xs is a methodology, however with different concentration. The main focus of DFS is to assure all potential hazards associated with a system under development have been recognized , and those hazards either mitigated or accepted for operation of the system. In order to do so, the design team and safety team must work together to reach a consensus that the design can be used reliably and the recognized hazards are acceptable for the system [Bahr, 2000].

According to [Bahr, 2000] the process of system safety is a close-loop system in which the hazards are identified, their potential risks are evaluated, a control system to prevent the potential hazards and their effects is developed, and periodically this process is reviewed . This process is made through combination of engineering analysis and management oversight. First, the objectives of the system of interest must be defined. Second, the whole system including peoples, software, equipment, the environment condition, etc., need to be reviewed [Bahr, 2000]. In this step, through various techniques the hazards are identified and evaluated. Safety experts should assess each hazard and its corresponding effect on the whole system. If they realize that the identified risks are unacceptable, they must develop a control system and implement it into the entire system to prevent or mitigate the risks. The management part of this process is paramount as well. Management must decide whether the risks are acceptable or not. If the risks are not acceptable, the whole system must be modified through changes in the design [Bahr, 2000].

A general model of integration of safety activities and systems engineering is shown in figure 3.8. This model is proposed by [Teller, 2014] to show the incorporating

safety principles into system development. The shaded blocks are safety activities that must be done during each step of systems engineering.

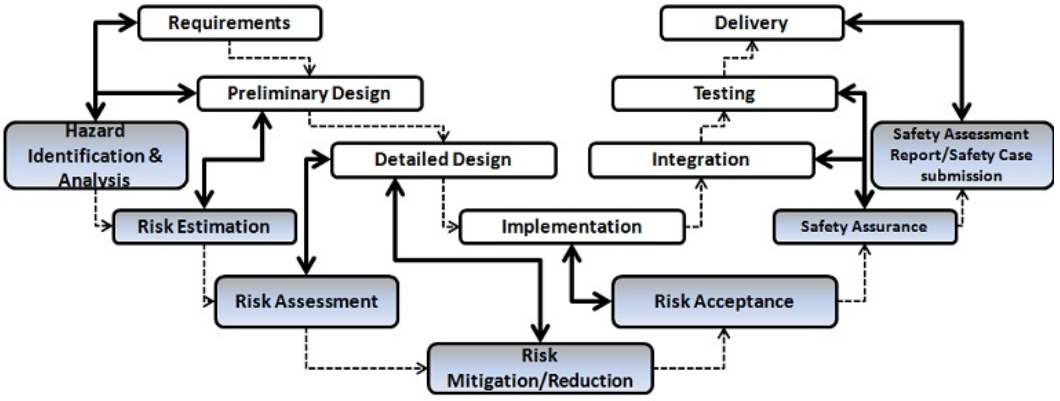


FIGURE 3.8: Integrated scheme for system development and safety activities in a project [Teller, 2014]

3.1.6.4 Design for Reliability

The comprehensive discussion of reliability theories, and the design for reliability techniques and principles is explained in the next chapter.

Design for Reliability(DFR) as one of the *design-for-requirements* tends to incorporate the reliability techniques into system design with the aim of increasing the reliability of the whole system. According to [Birolini, 2007, P. 2] "*Reliability is a characteristic of an item, expressed by the probability that the item will perform its required function under given conditions for a stated time interval*". Evidences show that failures have consistently occurred in the systems that lead to high needs for maintenance, and accordingly the cost of the entire system life cycle has been increased [Birolini, 2007].

The reason of system failures can be sought in the design of the system from beginning where the reliability and its characteristics have not been considered. The conceptual design must adequately indicate reliability with respect to the other specifications of the system Blanchard and Fabrycky [1990].

The process of the design must be well organized to make sure that the "failure-free" design principles are taken into consideration, and all potential failures are

identified and mitigated. The primary focus of the designer must be on creating a system that will not fail as specified. The designers through DFR process that must be well-integrated into the system engineering process can reduce the failure impact on the system [Liu].

According to [Liu], The process of DFR is conducted through various tools and practices that an organization must employ them to integrate reliability principles into the process of system development. The DFR process as a technical discipline is still under development and needs to be improved. Depending on the type of project, organization, or product/system, the process of DFR can vary. However, the general form of its activity flow is shown in figure 3.9. In this model shows the necessary activities to achieve a failure-free design. Also, this figure shows the well-integrated of reliability engineering into the system engineering process from concept design. A couple of analysis methods and tools must be applied at each stage to accomplish the whole process.

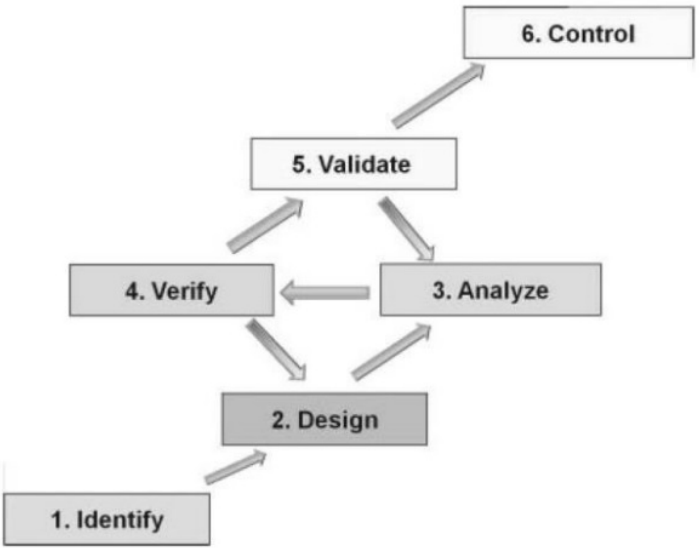


FIGURE 3.9: Design for Reliability Activity Flow [O'Connor and Kleyner, 2011]

Chapter 4

Design for Reliability

This chapter describes the "Design for Reliability" principles, tools, and techniques as the main focus of this thesis that has been implemented in DNVGL Prototype. Before going through DFR in details, it is wise to discuss reliability theory.

4.1 Reliability Theory

Reliability has broad meaning and usually is defined as dependability. According to [60050-191, 1990, Chapter: 191-02-06], reliability is defined as "*the ability of an item to perform a required function under given conditions for a given time interval*". This definition points out to three important elements: required function, given condition and given time. There are four terms that clarify the concept of reliability [Yang, 2007a, P. 10]:

- *Binary state*: the function of a product is either success or failure.
- *Multistate*: the product function can be the complete success, partial success or failure. The special case of multistate is performance degradation.
- *Hard failure*: this failure is catastrophic that leads to complete cessation of the function. Such a failure mode happens to a binary state product.

- *Soft failure*: this failure is the partial loss of a function that occurs in a multistate product.

Reliability is specified based on the intended function. The intended function for a binary state is distinct. For instance, the function of a light bulb is lighting. If the light bulb is blown out, it can be said that the failure occurs. The definition of the intended function of a multistate product is usually subjective. For example, a remote key to a car needs to be operated successfully at a distance up to 20 meters (hypothetical). This threshold can be specified somehow subjectively; however it mostly defines the level of the reliability. Assume, a product is a component that must be mounted in a large system. So, its intended function must be specified by system requirements. As a result, the same component, if installed in a different system, may have different failure measures [Yang, 2007a].

Reliability is defined as the function of time. In the reliability, the period is crucial. The warranty length, mission time, or other significant periods of time are specified by the concept of time in the reliability. Durability of a product reflects the customer expectations and can be a competitive advantage for a company. For instance, in defining the most of the passenger automobile that are recently produced, the durability of the car is ten years or 150,000 miles. On the other hand, the reliability can be defined as a function of operating condition. The conditions vary from product to product and may including usage rates, stress type and levels, operation profiles, and so on. The frequency of operation of a condition is imperative that have an impact on the system reliability. For example, there is a study in [Tanner et al., 2002] shows that micro-engines can operate longer at the high-speed condition than the low speed.

Reliability study mainly aims to provide information for decision-making. In the past, decision makers should specify the problem, and then the boundary condition and the objectives should be clarified. As a result, this information is considered as inputs for making a decision. However, by reliability study this process is conducted efficiently in the short period and with minimum cost.

Reliability technology can be applied in wide range areas including risk analysis, environmental protection, quality analysis, optimization of maintenance and operation, and so on. One of these fields is *engineering design*. In the technical products, reliability plays an important role. This means that reliability must be integrated into design process of a system/product. According to Blanchard and Fabrycky [1990], reliability is considered as an inherent characteristic of the design that must be integrated in the overall system engineering process. Many companies have realized the importance of reliability engineering, and they have employed it in their system/product development from beginning in the conceptual design. This is true especially for industries such as nuclear power, the aerospace, the aviation, the automobile, and offshore that a little failure can cause irreparable damage.

4.1.1 Measures of Reliability

In this section, reliability measures and terms are discussed. Before discussing the main topic of this thesis, some basic knowledge of these terms and measures are required as they will be used in this chapter. Reliability function, failure rate, mean time to failure(MTTF) and component relationship are depicted in this section.

4.1.1.1 The Reliability Function

The *reliability function* which is also known as the *survival function* shows the probability that an item operates successfully at least during the specific time. The t and the $R(t)$ representing the time and the reliability function respectively. Therefore, the reliability function is defined as [Blanchard and Fabrycky, 1990]

$$R(t) = 1 - F(t) \tag{4.1}$$

Here, the *F(t)* shows the probability that the item will be failed by time *t*. *F(t)* generally is considered as unreliability function. *R(t)* is also called survivor function that can shown as follow if the t has a probability density function of *f(t)*, then *R(t)* can be shown as

$$R(t) = 1 - F(t) = \int_t^{\infty} \mathrm{f(t)dt} \tag{4.2}$$

4.1.1.2 Failure Rate

According to [60050-191, 1990, Chapter: 191-04-01], failure is defined as "*the termination of the ability of an item to perform a required function* ". Failure rate is a rate that shows the occurrence of the failures in a specified time interval. The failure rate per hours is shown as

$$\lambda = \frac{number\,of\,failures}{total\,operating\,hours} \tag{4.3}$$

Failure rate might be considered in terms of failures per hour, per 1,000 hours or even million hours. The following example from Blanchard and Fabrycky [1990] clarifies the concept of failure rate. Suppose that 15 component from an extensive system has been tested for 700 hours under particular operating condition. The components that were unreliable, failed as follow: component 1 failed after 85 hours, components 2 after 135, component 3 after 145, components 4 after 350, and finally component 5 was failed after 155 hours. Hence, five components were failed, and the total operating hours was 3,830. By using equation (4.3), the failure rate per hour is

$$\lambda = \frac{5}{3830} = 0.001305 \tag{4.4}$$

4.1.1.3 Mean Time To Failure (MTTF)

According to Rausand and Høyland [2004], mean time to failure of an item is described as

$$MTTF = \int_0^\infty \mathrm{tf(t)\,dt} \tag{4.5}$$

MTTF can be representative of mean time between failure (MTBF), if the required time to replace or repair of a failed item is very short. For the exponential distribution, MTTF also can be written as [Yang, 2007b]

$$MTTF = \int_0^\infty exp(-\lambda t)dt = \frac{1}{\lambda} \tag{4.6}$$

4.2 Reliability Engineering

Today, the expectation of the customers is to purchase a high-reliable product at low price at minimum time. This is the responsibility of the manufacturers to design, develop, test, and produce such products. In other words, the critical factors that determine whether a product is successful in the market are reliability, time to market, and cost. Many companies have been making every effort to increase their market shares, and improve the competitiveness in terms of the mentioned factors. Reliability techniques are considered as powerful tools to meet these challenges. Many large-scale companies such as Ford Motor Company, General Electric, and IBM through recognizing the benefits of these techniques, have employed them to enhance their reliability program proper to their products. Even small-medium enterprises (SEM's) have tried to implement reliability techniques in their program as its benefits are inevitable [Yang, 2007a].

According to [Yang, 2007a], Reliability engineering is the discipline to ensure that a product (system) is operated reliably at a specified time and condition. In other word, reliability engineering tries to avoid failures. In reality, a system will be

failed sooner or later which means the failures in systems are inevitable. In fact, reliability engineering aim to minimize the effects of the failures, through planned and feasible actions, and consequently maximizing the reliability. The process of reliability engineering is carried out through three steps. First, during the design and development stage the system must be created with maximum reliability. There is a consensus among engineers that this step is most critical step. Next step is to reduce production process variation. This step is for certainty that the production process doesn't have any impact on the planned reliability. Finally, the third step starts once the system is deployed. In this step, proper maintenance operations must be used to increase durability of the system. These three steps are performed through various reliability techniques including reliability planning and specification, allocation, prediction, robust design, reliability modeling, failure mode, effect, and criticality analysis (FMECA), fault tree analysis (FTA), accelerated life testing, degradation test, verification and testing, and warranty analysis. The application of these techniques are various from system to system, and they must be employed appropriately based on the system specification. In subsequent sections, those reliability methods that are employed in this project are described in details.

The decisions made during the design process have an enormous impact on the reliability of the system [Avontuur and van der Werff, 2001]. As development proceeds, it is more expensive to correct those items that are affected by deficiencies in the design. In figure 4.1 , shows the cost of failures that are increased during the system development life-cycle. For this reason, designing discipline plays a significant role in minimizing the failures through detection and correction of them as early as possible. Besides this important responsibility, designers also must consider all other factors that can affect the reliability of the system, including production methods, maintenance, and failures not caused by load. As a result, designers should design a system that will not be failed if used as intended [O'Connor and Kleyner, 2011].

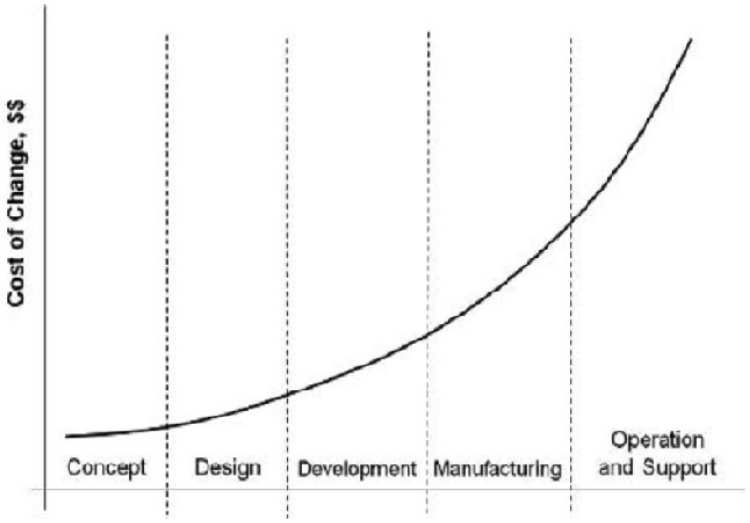


FIGURE 4.1: Cost of design change [O'Connor and Kleyner, 2011]

The old design process "test-analyze-and-fix" (TAAF) in which the reliability problems is shown up in the test stage, no longer is used in modern design and production. The reason is shorter design cycle, cost reduction, warranty cost issues, and many other concerns. For this reason, the reliability must be incorporated into the design through best available science-based techniques. This process is called Design for Reliability (DFR). This process begins from the first stages of system development and must be well integrated into the other stages. DFR process can change the role of engineers in the design process. For example, the role of the reliability engineer is changed to the mentor, who is responsible for finding best design techniques and method for reliability as well as training the designers to use them. In order to do so, the reliability and design teams must be integrated with the first step of DFR process [O'Connor and Kleyner, 2011].

4.2.1 Life Cycle Reliability Engineering

One of the ways in which companies can gain a competitive advantage is minimizing the product life cycle with respect to time and cost. Also, once they find their position in the market, they need to keep the customer satisfied by producing reliable products. These concerns have motivated companies to incorporate their

reliability program into the product life-cycle. Integration of product life cycle and reliability techniques can add value to the product. In the product realization process, each stage has its reliability tools that must be well-implemented. When the reliability methods are considered in design phase, they make engineers able to choose proper among available technology options and to assess the impact of design changes on system life-cycles [Pecht and Dasgupta, 1995]. Although a comprehensive reliability program adds more value to the product, due to lack of time and budget, this project only covers the first three steps of the system life cycle. The figure 4.2 shows the reliability program used for analyzing DNVGL prototype braking system. In this model, the suitable reliability techniques are allocated to each stage of product life cycle.

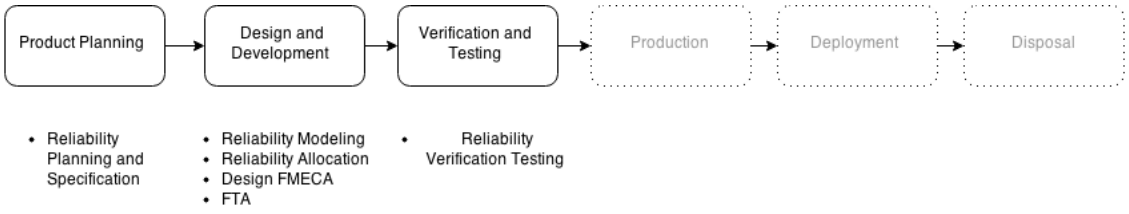


FIGURE 4.2: Reliability Tasks for DNVGL prototype braking system adopted from [O'Connor and Kleyner, 2011]

In the first stage, product planning, a team including multidisciplinary members must be organized to determines a proper reliability program for the particular product. The team must have a reliability target, translate customer needs into engineering requirements, and propose a reliability plan. As it has been repeated, the decisions made in terms of reliability have a tremendous impact on the next stages. For example, the reliability target must be feasible to meet the planned time and cost. An overly ambitious goal might jeopardize the whole project in which the design and development will be unaffordable, and the product realization process will be extended. On the contrary, if the reliability target will be weak, lack of meeting the planned reliability requirements merely undermines competitiveness [O'Connor and Kleyner, 2011].

Design and development is a critical phase in which the role of reliability tasks is significant so that they can add more value to the product in this phase than the

other ones. In this stage, reliability activities aim to ”design-in” the reliability of the product while ”designing-out” the potential failure modes. This might be achieved by assigning the target of reliability to the internal subsystem or components, as well as applying reliability design techniques including RBD, FMECA, and FTA to assure achievement of the respective reliability goals. These proactive reliability activities are developed to create things right at the first time. Undoubtedly, a reliability program can save the cost by accelerating the design and development cycle [O'Connor and Kleyner, 2011].

In the verification and testing phase, reliability tasks are vital elements. In this stage, reliability verification testing is carried out to show that the reliability requirements are met. For example, reliability data analysis is often necessary to achieve a meaningful result regarding the reliability of the product under functioning. The reader can find more discussion about integration of reliability activities and product life-cycle in [O'Connor and Kleyner, 2011].

4.2.2 Reliability Requirements

Reliability requirement specification is considered as one of the system requirements specification (SRS) tasks. General process of SRS is explained in 3.1.5.1 and 3.1.5.2. Sometimes the reliability requirements are precisely specified by customer. Usually, the producer must determine whether the stated requirements is feasible and realistic and translate them into the design specification form. Commonly, it is difficult for the consumer to define the desired reliability requirement. For example, how the specification of ten years operation or 150,000 miles can be translated into the reliability terms?

The process of developing reliability requirements is shown in figure 4.3. In order to meet customer reliability expectation, each step is important in selecting the level of reliability that determine the scope of design. In the following, each step is discussed.

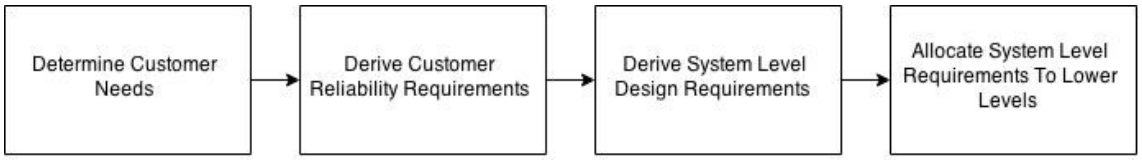


FIGURE 4.3: Reliability Requirements Development Process [Norman B, 2005]

Determine Customer's System Needs In order to develop operational performance reliability requirement and subsequent design requirements, it is essential to determine customer needs as early as possible in the system planning phase. Several approaches are used to determine the customer needs. One of these approaches is *Market Surveys*. This approach tries to find best attributes of the system from basic functionality and general appearance. It is very helpful to define customer needs by asking them. Despite, this approach can lead to bias and sampling error, but with well-planned effort this effect can be minimized [Norman B, 2005]. Another approach is *Benchmarking*. "*Benchmarking is a proactive process for making organizational improvements*" [Crowe and Feinberg, 2010, Ch. 2-P. 3] . In benchmarking, the manufacturing process, product, and service are comparing with a pioneer industry. This process aims to find the success factors of competitor(s) and to benchmark them [Crowe and Feinberg, 2010]. *Environmental characteristic*, also, is an important approach to determining environmental conditions that the system will experience when it put into use. Temperatures, shock, vibration, humidity, pressure, and so forth are the examples of environmental conditions that need to be assessed. For example, if a system expected to have MTTF of 500 hours in an average state, it might experience MTTF of 200 hours under pressure [Crowe and Feinberg, 2010, O'Connor and Kleyner, 2011].

Customer Reliability Requirements It is important to elicit the performance reliability requirements of the customer from the general customer needs. Sometimes the needs might be defined as qualitative requirements (e.g., good reliability). Reliability needs, also, might be hidden in the other stated requirements. For example, reliability can be defined as the availability of the system, or as a

safety concern. If the reliability performance requirements are defined as quantitative (e.g., MTTF), there is no need to further actions. However, usually the reliability requirements are "hidden" and it is necessary to conduct a needs analysis to derive the reliability requirements. In order to do so, two ways are introduced into this project. *Modeling and Simulation* can be used as an effective technique to find the level of the system reliability, or at least the range of reliability. Information gained from modeling and simulation can be used to conduct a trade-off among various solution to select the best one for meeting the customer requirements [Crowe and Feinberg, 2010]. According to [O'Connor and Kleyner, 2011], FMECA, also can be used to derive customer reliability requirements. Traditional FMECA was implemented to check the whole system for a post-engineering activity. However, performing the FMECA process in the concept design stage makes the engineers able to incorporate the customer needs into the system capabilities. In this way, the engineers collect the proper information through customer needs while ranking each requirement based on their importance. As a result, the ranking system makes the engineers able to make a trade-off between customer needs and design capability.

System Level Design Reliability Requirements In order to develop design reliability requirements, a couple of factors needs to be considered. As it shown in figure 4.4, the failures in a system can be caused by the mentioned factors from below to above of the pyramid. Despite some factors are not under producer's control, but they must be taken into account in establishing design reliability requirements. Design reliability requirements must be derived before design and development phase. This process sometimes referred as *translating* customer reliability expectation to produce design reliability. There

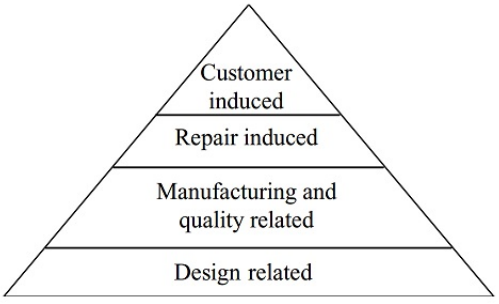


FIGURE 4.4: System Performance Failures [Crowe and Feinberg, 2010]

are a number of reliability oriented methods such as quality function deployment (QFD), or reliability design requirements from analysis that can be useful to develop design reliability requirements from customer reliability expectation. QFD is a tool for translating customer expectations to the to proper design requirement in the design stage. Another technique is reliability design requirement from analysis in which number of various *analysis* are employed to develop reliability design requirements. These analysis methods include thermal analysis, durability assessments, prediction, fault tolerance, dormancy analysis, and derating Crowe and Feinberg [2010]. However, application of these analyzes is very costly and time consuming that many projects can not deal with them. Also, these analysis need some technological equipment that is hard to be provided. The provision of this information is one of the supplier's responsibilities.

When a product(system) is purchased, the information regarding its reliability must be provided by supplier. IEEE Reliability Program Standard 1332 [720, 1998], classes the supplier's responsibilities into three objectives: 1) supplier that working with the customer must understand the client carefully needs, to generate a comprehensive design specification. 2) Supplier needs to follow a set of activities to ensure that the final product will satisfy the customer about the product reliability. 3) Supplier must assure the client that the reliability requirements has been satisfied.

Allocate Lower Level Requirements The final stage of the reliability requirement process is the allocation of reliability to the lower level of the system. The concept of reliability allocation is clarified through an example here. Assume that a system with four major subsystems requires a *mean time between failure (MTBF)* of 500 hours (Figure 4.5). The requirements document has specified only the overall system MTBF requirements of 500 hours and not the lower level MTBF requirements for subsystems. It is therefore one of the responsibilities of the reliability engineer to derive and allocate MTBF requirements for the subsystems. At it shown in figure 4.5, reliability engineer might derive a set of MTBF requirements for the subsystem, based on technical information or data from previous program

and experience. The MTBF can be attained by following formula:

$$MeanTimeBetweenFailure(MTBF) = \frac{1}{failure\,rate} \tag{4.7}$$

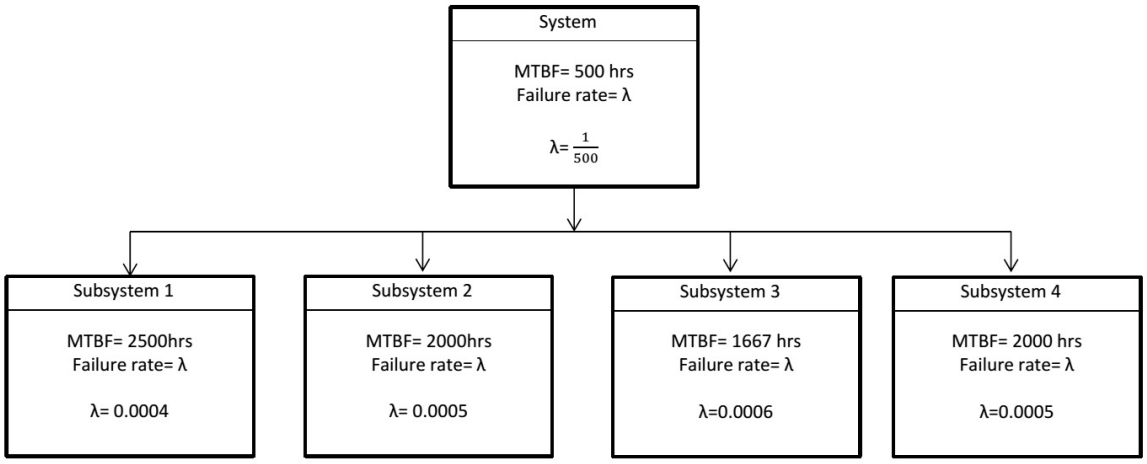


FIGURE 4.5: Derived and Allocated Reliability Requirements [Eisner, 2008]

4.2.3 Reliability Modeling

Modeling is one of the useful tools to show the actual behavior or performance of a system, and predict its function in a real life. According to [Rechtin and Maier, 2000, P. 11] "*Modeling is the creation of abstractions or representations of the system to predict and analyze performance, costs, schedules, and risks, and to provide guidelines for systems research, development, design, manufacture, and management. Modeling is the centerpiece of systems architecting, a mechanism of communication to clients and builders, of design management with engineers and designers, of maintaining system integrity with project management, and of learning for the architect, personally*".

Reliability modeling aims to set expectations of reliability performance of a system with the purpose of foreseeing future behavior and reliability performance. The primary objective of reliability modeling is to ensure no failures will happen in a critical component during a required operation time. Reliability engineers through

reliability modeling can identify design weaknesses, analysis and test it, and find improved design. Reliability modeling can add value to the system life cycle. It also helps the designer to decide how much redundancy and fault tolerance are needed to meet system requirements in the design and development stage. Moreover, it can be conducive to system development when engineers consider redesigning the system to make some enhancement or add additional features [Raheja and Gullo, 2012].

The reliability block diagram (RBD) as an inductive method is employed to analyze systems in terms of reliability. The main focus of reliability block diagram is to show the overall system schema with its distinctive components and interrelation between them by using the graphical representation that can be useful to predict and analyze the probability of system failures. The connections between block within the block diagram shows their effects on the system [Cepin, 2011].

Components In Series One of the most commonly used structure is series relationship that can directly be analyzed. In series structure, if the system expected to function properly, all components need to operate in a satisfactory manner as a failure in one component leads to failing the whole system. An example of the series structure is shown in figure 4.6. This system including three subsystem A, B, and C. The reliability of this system expressed as follow [Blanchard and Fabrycky, 1990]:

$$R = (R_A)(R_B)(R_C) \tag{4.8}$$

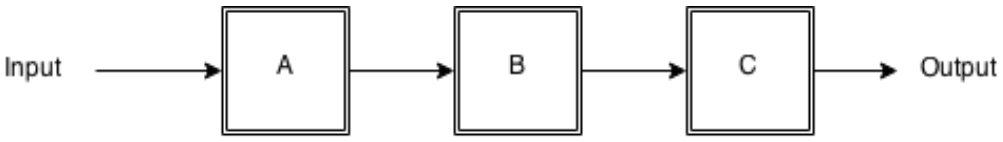


FIGURE 4.6: A series structure

If a series structure is planned for a desired time period, its reliability can be written as:

$$R_Sys = (e^{-\lambda_1 t})(e^{-\lambda_2 t})...(e^{-\lambda_n t}) \tag{4.9}$$

for a series system with n components, the equation can be written as:

$$R_Sys = e^{-}(\lambda_1 + \lambda_2 + ... + \lambda_n)^t \tag{4.10}$$

Components In Parallel When several of the same components in a system are located in parallel, the system has a so-called *parallel network*. In this structure, all components are functioning independently, and all components must be failed to cause overall system failure. The reliability of a system with identical components in parallel, as shown in figure 4.7, is calculated as follow [Blanchard and Fabrycky, 1990]:

$$R_Sys = R_A + R_B - (R_A)(R_B) \tag{4.11}$$

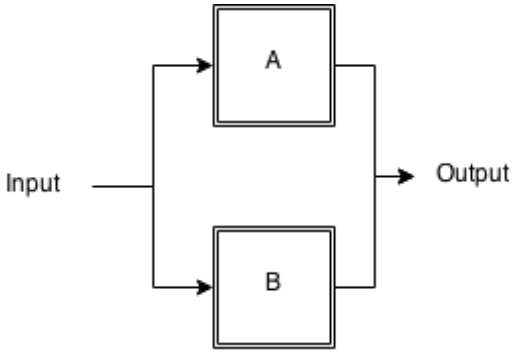


FIGURE 4.7: A Parallel structure

Assume a structure with three components in parallel. The reliability of this structure, as presented in figure 4.8, is expressed as follow:

$$R_Sys = 1 - (1 - R_A)(1 - R_B)(1 - R_C) \tag{4.12}$$

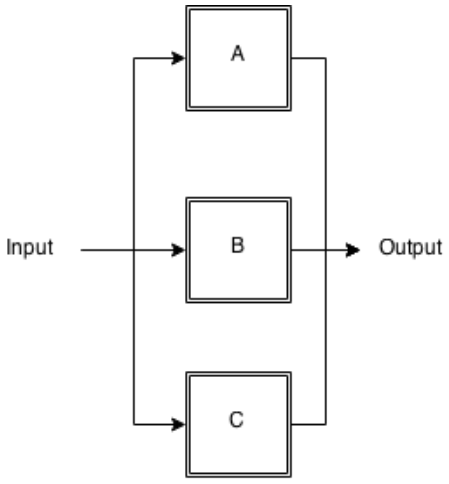


FIGURE 4.8: A Parallel structure With Three Components

Above calculation can be simplified as follow, if the three components are identical:

$$R_Sys = 1 - (1 - R)^3 \tag{4.13}$$

Generally, the reliability of a parallel structure with n identical components can be written as:

$$R_Sys = 1 - (1 - R)^n \tag{4.14}$$

Combination of Series-Parallel Structure The combined series-parallel relationship between components can be very helpful for showing the structure of a complex system as well as analyzing its reliability. Here, an example is explained to clarify the concept of the series-parallel network. The reliability of the a series-parallel structure in figure 4.9 is given by:

$$R_{Sys} = [1 - (1 - R_A)(1 - R_B)(1 - R_C)][R_D][R_E + R_F - (R_E)(R_F)] \tag{4.15}$$

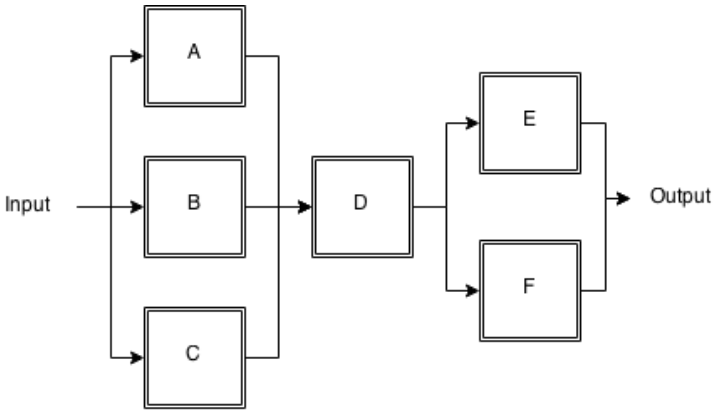


FIGURE 4.9: A Example of Series-Parallel structure

4.2.4 Failure mode, effects, and criticality analysis

One of the well-known systematic techniques to find and analyze failures is failure mode and effect analysis (FMEA). Reliability study of a system usually starts with FMEA. In this method, almost all components, assemblies, and subsystems are reviewed to identify failure mode and the root of such failures. The causes of each failure associated with a particular component and its effect on the whole system are documented into an appropriate FMEA worksheet [Rausand and Høyland, 2004]. An example of FMEA worksheet is shown in figure 4.10.

Description of Unit			Description of Failures			Effect of Failures		Failure Rate	Severity Ranking	Risk Reducing Measures	Comments
Ref No	Function	Operational Mode	Failure Mode	Failure Cause	Detection of Failure	On the subsystem	On the system function				

FIGURE 4.10: FMECA worksheet [Rausand and Høyland, 2004]

FMEA has changed to failure mode, effect, and criticality analysis (FMECA) where criticalities are allocated to the failure mode effects [Rausand and Høyland, 2004]. According to [159, 1987], some of the objectives of FMECA related to this project are as follow:

- To choosing design alternatives with maximum reliability and safety potential during the early design phase.

- To make sure that all possible failure modes and their effect on the overall system are taken into consideration.
- Listing all potential failures and finding the level of their effects on the system.
- To document all information regarding failure modes for future references in case the redesign of the system is considered.
- Provision of input data for trade-off studies
- To make available a basis for conducting corrective action priorities.
- To help in evaluating the design requirements associated with redundancy, failure detection system, fail-safe characteristics, and automatic and manual override.

FMECA usually is conducted during the design phase. The primary objective of FMECA in this phase is to reveal the weaknesses of the system and potential failures as early as possible. For this reason, designers can incorporate the possible barriers and corrections into the system design [Rausand, 2014].

According to [Carlson, 2012], there are two types of FMECA: *Quantitative* and *Qualitative*. The procedure of both kinds is same, but their criticality analysis are different. The Quantitative FMECA uses the quantitative criticality analysis, where the Qualitative FMECA uses qualitative criticality analysis. The FMECA employed in this project is qualitative.

Qualitative FMECA This approach does not have any calculation and qualitative criticality analysis. An example of quantitative FMECA is shown in Appendix A. Qualitative approach follows three steps [Carlson, 2012]: 1) The severity of the potential effects of failure must be rated (table 4.1), 2) rank the likelihood of occurrence of each potential failure modes (table 4.2), and 3) and the failure modes are compared with a criticality matrix. There are unique severity and occurrence scales for FMECA.

Catastrophic	A failure that may cause death or system loss
Critical	A failure that may cause severe injury, major property damage, or major system damage which will result in mission loss
Marginal	A failure that may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of availability or mission degradation
Minor	A failure that is not serious enough to cause injury, property damage, or system damage, but will result in unscheduled maintenance or repair .

TABLE 4.1: Severity classification [Carlson, 2012]

Frequent	A high probability of occurrence during the item operating time interval
Reasonably Probable	A moderate probability of occurrence during the item operating time interval.
Occasional	An occasional probability of occurrence during item operating time interval
Remote	An unlikely probability of occurrence during item operating time interval.
Extremely Unlikely	A failure whose probability of occurrence is essentially zero during item operating time interval.

TABLE 4.2: Probability of potential failure Occurrence [Carlson, 2012]

4.2.5 Fault Tree Analysis

Fault tree analysis (FTA) is defined as "*a graphic depiction or model of the rationally conceivable sequences of events within a complex system that could lead ultimately to the observed failure or potential failure*" [Harkins, 1999, Online].

FTA is a logic approach that shows the relationship between an event(accident) and the cause of this event through a diagram. Reasons of the failure might be

environmental condition, human error, ordinary events, and specific component failure. Depending on the objective of the analysis, the FTA can be qualitative or quantitative, or both [Rausand and Høyland, 2004]. Same as FMECA conducted qualitatively in this project, qualitative FTA is used in this project.

The construction of the FTA always starts with *TOP Event*. From that point forward, the process is continuing with identifying all fault events that cause the TOP event. The fault events must be immediate, necessary, and sufficient reasons to make the TOP event. The identified causes are linked to the TOP event through a *logic gate*. The fault tree must proceed level by level and should be completed from top to bottom. In other words, the analysis is deductive in which this question that "*what are the reasons for this event?*"repeatedly must be asked [Rausand and Høyland, 2004].

The figure 4.11 shows how the FTA procedure is performed. TOP event is the undesired event that must be prevented. A TOP event usually is caused by one or many contributors. The contributors are shown in a box and connected. The connections are shown in the form of "**AND**-gate" and "**OR**-gate". The logic gates describe the relationship between contributes. This process is continued until the basic events are gained.

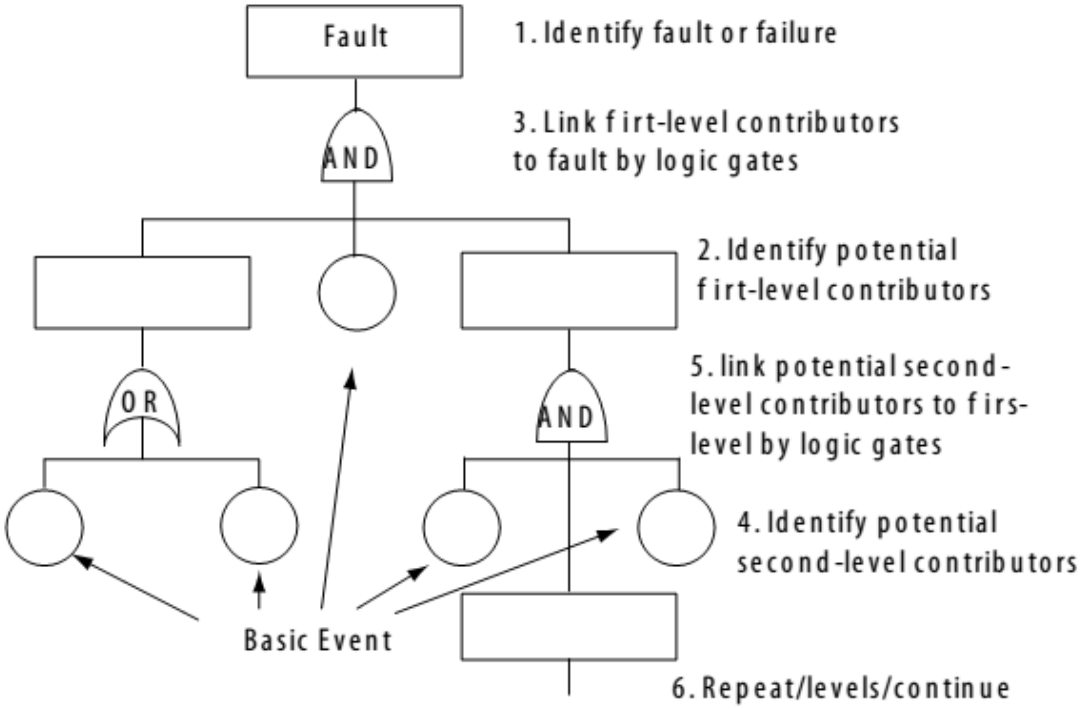


FIGURE 4.11: Fault Tree Process [Harkins, 1999]

There are four main elements in the fault tree, . According to [Xing and Amari, 2008] these elements are defined as follow:

- TOP event: that shows a undesired event, system failure or accident.
- Basic event: that shows the basic causes for the identified undesired event. For the basic event there is no need to continue the development of the failure causes.
- Undeveloped event: that is presenting the fault events that are not analyzed further due to the lack of information or being insignificant of its consequences.
- Gates: that are presenting the outputs of one or combination of basic events or the other gates.

Chapter 5

Reliability System Engineering Of DNVGLFF Project

The assigned systems engineer was responsible for implementing the systems engineering principles for the first three stages of system life cycle as well as implementing the reliability engineering techniques simultaneously. All efforts of the author were before the production of the system in the design stage. In this thesis, the main focus was to design the braking system more reliably through the reliability techniques. It was very challenging to implement the discussed theories of reliability engineering in the real life case study. The reasons for the challenges in thesis were mainly due to lack of experience on this topic as it had not been done before. Also, lack of time, budget, and especially proper information regarding the reliability of the purchased components made this project very difficult to get the actual result. All in all, the author did his best to establish a baseline for the reliability study in the SEM's projects.

In this chapter, the essential efforts that needed to be done to achieve the goal of this thesis are described. First, the process of system and reliability engineering proposed in this thesis is described. Also, the systems engineering results including requirements specification, systems design architecture, and detail design are

presented. Then the results of reliability engineering consist of RBD, FMECA, and FTA, as well as failure analysis and suggestions, are discussed.

Reliability methods introduced in chapter 4.2, are the conventional ways to analyze the reliability of the system that are being used in real industries. The causes of potential failures are either in the design and manufacturing stages or how the customers use the system. Reliability study provides proper techniques to recognize and mitigate the failures that can be caused by any of the mentioned reasons.

Ingrid Almas Berg, in her master thesis, [AlmasBerg, 2010] discuss design for reliability techniques that need to be carefully conducted. She believes that in order to have a more reliable outputs, the reliability study must be implemented through a general methodology. In order to do so, she suggests a general methodology for the reliability study that can be used independently to industry, system, or even organization.

The reliability engineering process used in this project is adopted from suggested methodology in [AlmasBerg, 2010]. This process is shown in figure 5.1. As suggested by literature, the author believes that reliability engineering must be conducted with systems engineering tasks concurrently. Based on this thought, the introduced process is developed. Although this process only shows the first three stages of the system development, however it can be expanded to the other stages. The main objective of this process is to demonstrate that each reliability task should be carried out in a proper stage in systems development. In other words, in a systems engineering program, each stage has its reliability activity that must carefully be taken into account. This process is explained in details in the next sections.

5.1 Systems and Reliability Engineering Process

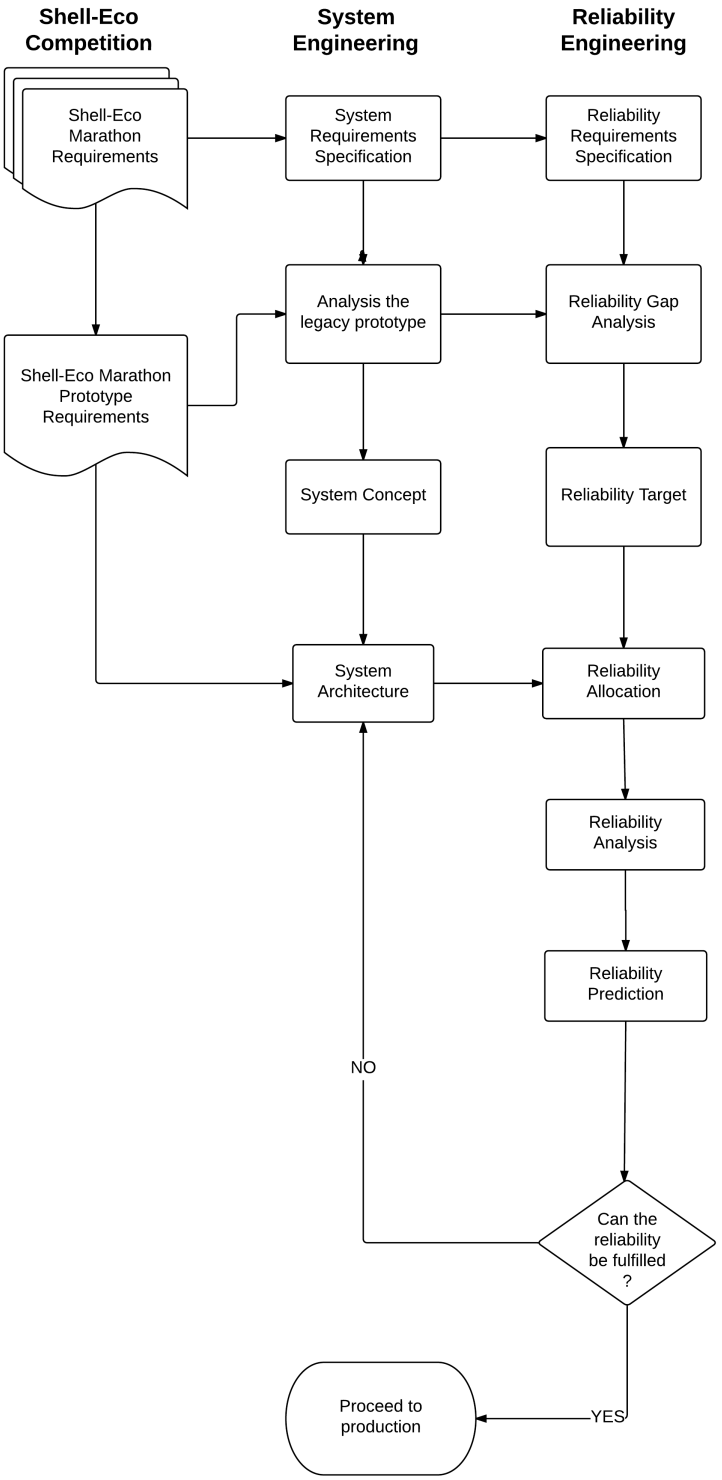


FIGURE 5.1: Systems and reliability engineering process

Figure 5.1 shows the process of reliability system engineering applied in the DNVGLFF 2015 project. In the beginning, the team was requested by the assigned system engineer to participate in the weekly meetings. The team was bound to go through the SEM rules [she, 2015] to identify the system specification. The assigned systems engineer, by gathering all necessary requirements into a standard requirements document, made this task easy for the team. As it mentioned before, the reliability engineering is carried out for the first time in DNVGLFF project. For this reason, system engineer decided to familiarize the team with the concept of reliability and to explain the necessity to have reliability engineer beside the other disciplines. The reliability study began with reliability requirements that were stemmed from system specification. The reliability requirements must be achievable with accordance to reasonable time, budget, condition, and success ratio of the system. The system requirement specification (SRS) is explained in section 5.2.1.

Once the requirements was specified, the team with accordance to meet the specified requirements, started to analysis the legacy prototype. This step was done through a cross-functional meeting including the new members of various disciplines and the previous team of DNVGLFF 2014. The meeting called ”knowledge transfer meeting” in which the old group shared their experiences with their new counterparts. The gained knowledge was very helpful to the team, especially for the reliability study of the system. It was revealed that what subsystems mostly needed to be improved. Also, the vulnerable subsystems, that the reliability analysis should be conducted on them, were specified.

Reliability gap analyzing of the whole system within the limited time was a very difficult. Usually, reliability engineering of a complex system should be performed by a reliability team. For this reason, it was decided to conduct reliability analysis for braking system as the most vulnerable subsystem. This decision was made due to two reasons. First, it was proposed in a meeting by Kjell Olav Skjolsvik, principal consultant of DNVGL. In order to have a reliable result with accordance to the project constraints, he suggested conducting the reliability study only for one subsystem. Second, as the former team has been faced with a couple of

problems with braking system during the completion, it seemed to be a good idea to select this subsystem as a subject of reliability engineering.

As it shown is figure 5.1, once the analysis of the legacy prototype was done, the team started to define the concept of the system. This process was done by setting the goals, solutions, and boundary of the system. According to the limited time, budget, and the facilities that the team had, improvement areas of the system were selected. These areas are shown and explained in appendix C.2.2. Also, the reliability target was specified. This process was carried out in accordance with reliability requirements specified in SEM rules. The system engineer defined a reliability program through reviewing carefully of the literature. The reliability methods introduced in this program were designing and updating FMECA, reliability modeling of the braking system by RBD, and fault tree analysis (FTA). The author believes that this reliability program can help to find the potential failures in braking system and the braking system will probably function successfully by reducing the risks of found potential failures.

After the team was reached a consensus regarding improving the system, a general timeline of the project was built by the project manager. Also, the system engineer decided to make a Gantt chart for the improvement areas. As a result, all assigned engineers for a particular areas estimated their due date for completing their tasks. The Gant charts for different improvement areas can be found in appendix B.

As it shown in figure 5.1, the process of designing the system architecture was started after defining the system concept. The team by spending around four weeks, and through weekly meeting, has tried to specify the system architecture. The responsibility of the system engineer was to break down the system into its subsystems and components to describe them in detail. This task was done in order to specify what subsystems and components are needed to fulfill the specified requirements.

After specifying subsystems and components, their required functions, needed to be cleared. The assigned system engineer defined the intended role of each subsystem by keep asking from engineers. In parallel, braking system as the primary

focus of the reliability study of this project, was carefully analyzed. In order to do so, the system engineer collaborated with assigned mechanical engineer who was responsible for braking system. Through this collaboration, the braking system was broken down into components and parts with the aim of allocating the reliability.

The process was proceeded by performing reliability analysis. The reliability analysis of the braking system was carried out by FMECA, RBD, and FTA. In order to make sure that braking system will functioning successfully, desired reliability must be assigned to its lower level components and parts. Reliability allocation was very helpful to identify more potential failures in braking system. These potential failures are identified by FMECA that is explained in section 5.3.2. Despite the designed system architecture well shown the subsystems and components, however, it was necessary to show the interrelationship between these subsystems and components. For this reason, system engineer decided to use RBD to illustrate the links in the system structure. The whole system, as well as braking system, were designed in details by RBD that are explained in section 5.3.1. Another reason, for conducting RBD, was to identify the series and parallel structure of the system that was helpful to predict the reliability of the system. Depending on the industry, it is more wisely to use different reliability methods to observe different reliability aspects of the system of interest. As a result, conducting FTA seemed to be reasonable to identify accident events of the braking system. FTA was a very helpful reliability tool in which the causes of the potential failures in braking system were revealed. Consequently, the braking system's team, saved significant time and money, and predict the reliability of the braking system by only focusing on the vulnerable parts of the braking system. Braking system's team including assigned system engineer and mechanical engineer.

The outcomes from FMECA, RBD, and FTA are used as inputs for predicting reliability of the braking system. The process of reliability prediction specified whether the proposed design can meet the desired requirements. According to the proposed process shown in figure 5.1, if the team achieves a consensus regarding

the system design, the process is proceeded to production. Otherwise, the system architecture must be refined to make another solution.

5.2 Results from System Engineering in DNVGLFF

System engineering of DNVGLFF 2015 was started with the definition of the system life cycle. As it mentioned earlier, the prototype class was selected as the system of interest. The team decided to improve the legacy vehicle from the last year. The system life cycle model used in this project is Vee model. This model is shown in figure 5.2.

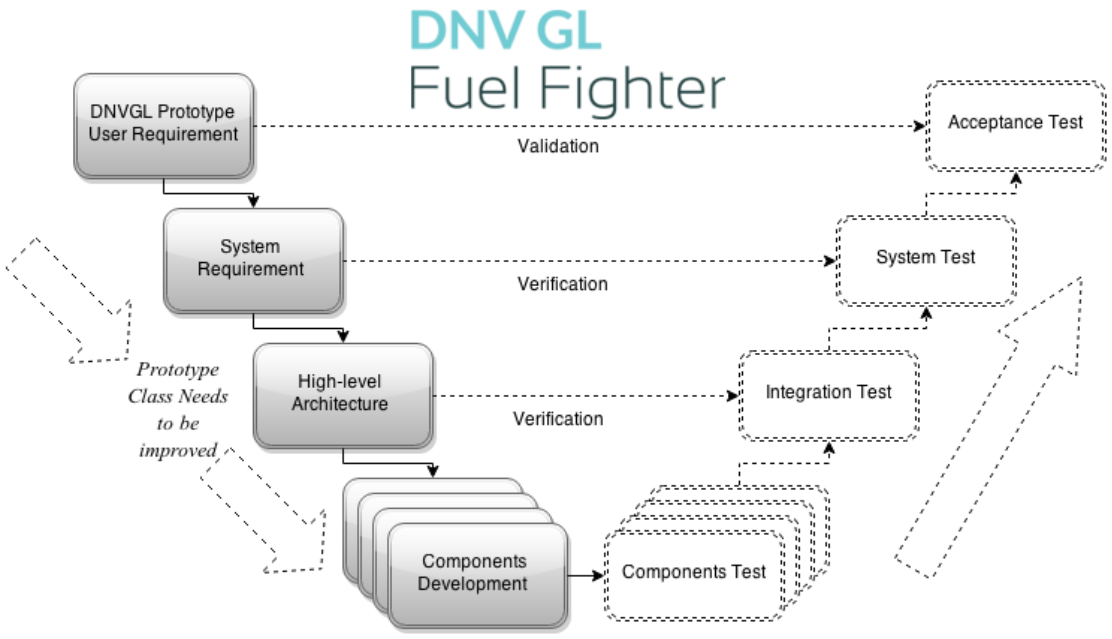


FIGURE 5.2: Vee Model For DNVGLFF Prototype 2015

The scope of this thesis was focused on the left side of the system life cycle. The left side of the Vee model is related to system design. The process of systems engineering was explained to the team members through weekly meeting. Before each meeting, assigned system engineer sent agenda to the members included the require information that he needed as inputs. During the meeting, all necessary

activities, for developing the system, were discussed. Once the team reached the consensus regarding the project activities, the systems engineering started its activities that are explained respectively in the next sections.

5.2.1 Requirements Analysis

As it discussed in literature review chapter, the first step in any systems engineering program is requirements specification. All stakeholders and their needs must be carefully recognized prior to any further activity. Every year Shell prepares a document called "Eco-Shell Marathon Rules" that all requirements are gathered into it. This document provides information in details regarding competitors, safety rules, design rules, and energy sources. Some of these requirements are changed annually. The Shell-Eco Marathon Rules 2015 can be found in [she, 2015].

Assigned systems engineer have tried to make a standard requirements document by selecting those requirements that have been appropriate for the project. According to the literature, selected requirements should have been traceable, understandable, clear, precise, correct, complete and feasible. In order to avoid ambiguity, the author has organized all requirements into the specific subtitle that shows which requirement is related to which part of the system (i.e., functional requirements, design requirements, operational requirements, etc.). The requirements of DNVGLFF 2015 prototype can be found as appendix C.

After having clarified all necessaries requirements, all constraints and limitations have been revealed. It was discovered that what kinds of roles and how many of them needed in this project. Also, based on the gathered requirements, the estimation of the time and budget was relatively accurate.

Once the roles of members were specified, the requirements list associated with the particular role was shared with members who were assigned to it.

5.2.2 System Architecture

The system architecture in this project is designed based on system architecture made by system engineer 2012. This system design including top-level subsystems and the components in details. All necessary subsystems and their corresponding components that were essential for meeting the requirements are taken into consideration. The system engineer have tried to identify and update all essential subsystems and components by working closely with members of the project. The system architecture can be seen in appendix C.2.2.

The system architecture of 2015 has divided the prototype vehicle into the subsystems Body, Driver, Brake system, Rear Suspension, Front Suspension, Steering, Wheels, Car control system, Propulsion, Transmission, Interior, and Electronics. As it mentioned before, the team decided to improve the legacy prototype vehicle from the previous year. Subsystems and component that were needed to be improved are shown as red blocks into the system architecture. All improvements are explained in appendix C.2.2.

5.3 Results from Reliability Engineering in DNVGLFF

Reliability engineering in DNVGLFF project 2015 has been conducted concurrently with systems engineering principles. The applied method in this project are FMECA, RBD, and FTA to identify potential failures in braking system. In this project, the reliability engineering is conducted with the aim of designing out the identified potential failure and proposing the possible solution to mitigate their effects. The reliability techniques performed in this project are explained in the following subsections.

5.3.1 RBD

The primary objective of reliability block diagram (RBD) is to estimate the reliability of the system based on the structure of subsystems. Prototype system and braking system are modeled by GRIF. This software can be used for reliability modeling of systems based on RBD logic. At the beginning of the project, RBD was conducted for showing the subsystems and their interrelationships in the prototype system (figure 5.3).

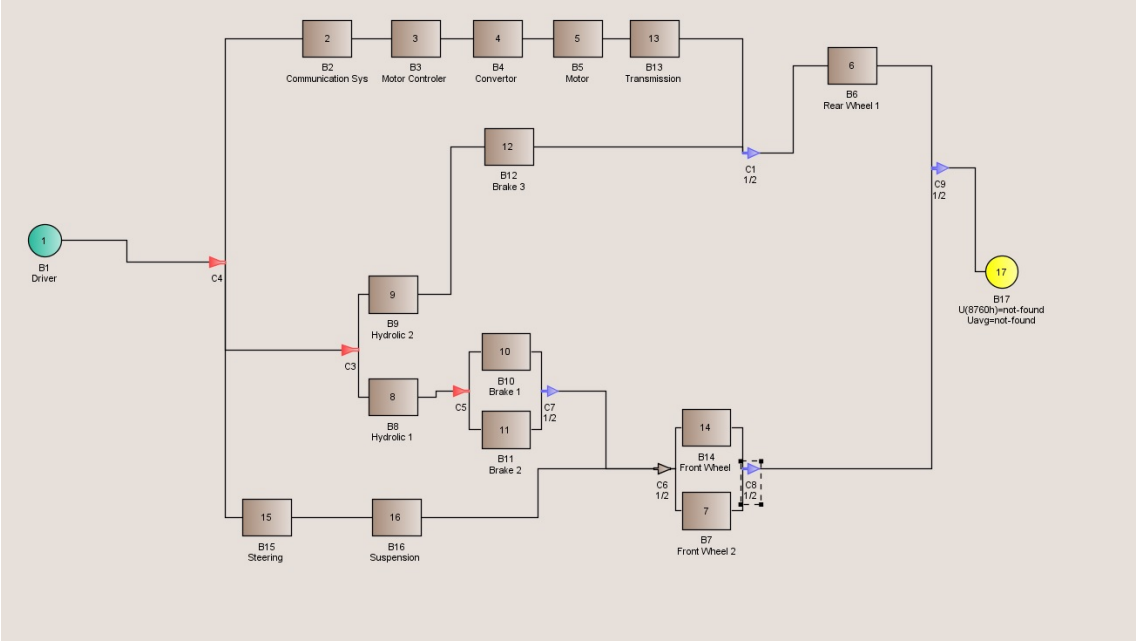


FIGURE 5.3: Reliability Block Diagram (RBD) for Prototype system

As it can be seen in figure 5.3, the system consists of subsystems that are structured in the series, parallel, and both (combined series-parallel). A chain of functions must be occurred to gain a desired outcome in the system. The system takes the inputs as three different commands from the user (driver), process them, and derive the outputs. The three commands comprise acceleration, brakes, and steering of the vehicle. The blocks number 2-5 plus 13 make the acceleration system. As it shown clearly, all of these subsystem that are structured in the series must operate properly to transfer the power to the rear wheel. In the middle of the picture, the blocks number 8-12 make the braking system. The driver put the order to stop or to control the speed of the vehicle through these subsystems. And finally the

blocks 15 and 16 make the steering system. These dependent subsystems transfer the user's command to the front wheels to change the position of the vehicle.

The figure 5.4 shows the structure of braking system in details. The braking system is broken down into two independent subsystems: front and rear. The system is made from two braking lever, two hydraulic lines, three calipers, and three braking disks. The braking system consists of two general parallel lines. In fact, these two lines are presenting the independent front and rear subsystems. The above of the picture shows the line that form the components associated with the front subsystem. As it can be seen, this line made from the combination of series and parallel components. The bottom side of the picture shows the rear braking subsystem. This line structures the components associated with the rear subsystem in a series form.

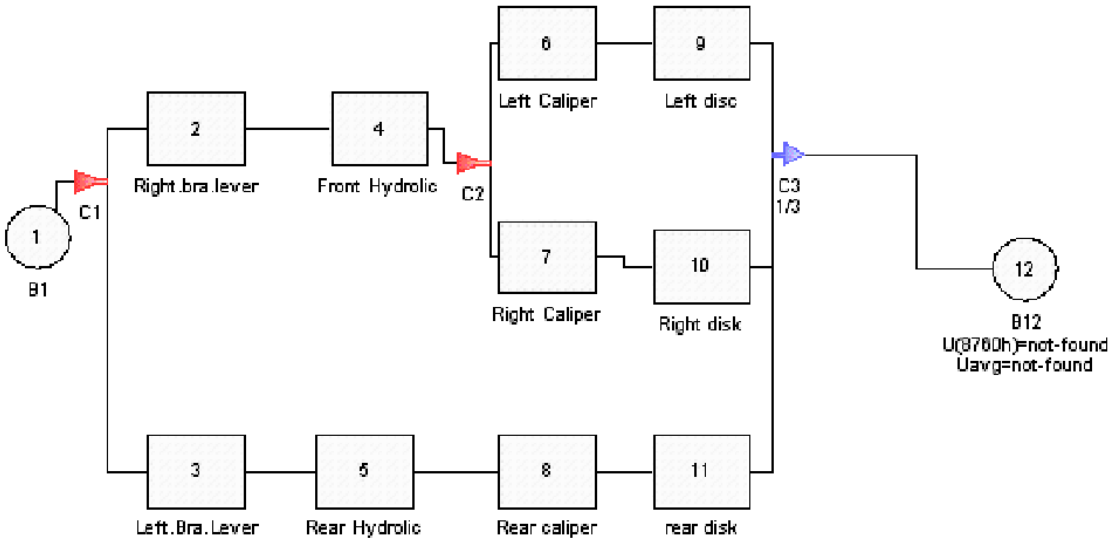


FIGURE 5.4: Reliability Block Diagram (RBD) for Braking system

The reliability of the braking system depends on how the components properly function. This means occurrence of failures in the components effects directly on the whole system reliability. As it shown in figure 5.4, the front braking subsystem has two calipers and disks that are formed in parallel. This means if a failure happens in blocks 6 or 9, the components 2, 4, 7, and 10 can work properly. Although, in this case, the reliability of the braking system will be decreased, the

system still works. Based on the assumption that all components have same failure rate, it can be said that reliability of the front brake subsystem is higher than the rear one.

As it discussed before, one of the applications of RBD is to calculate the reliability of the system based on its structure. In order to do so, the failure rate of each component needs to be provided. This information usually is gained through expert judgment, handbooks, standards, and tests. Also, it can be found from information of purchased components provided by the seller.

According to section 4.2.3, the reliability of the braking system can be expressed as follow:

$$R_{LC,LD} = R_6 R_9 \tag{5.1}$$

Where LC means Left Caliper and LD means Left Disk. Also

$$R_{RC,RD} = R_7 R_{10} \tag{5.2}$$

If $R^\star$ is showing the reliability of the $R_{LC,LD}$ and $R_{RC,RD}$, therefore the reliability of the components 6,9,7, and 10 can be expressed as follow:

$$R^\star = R_{LC,LD} + R_{RC,RD} - R_{LC,LD} R_{RC,RD} \tag{5.3}$$

From above calculation the reliability of the front braking subsystem might be gained as follow. The reliability of the front braking subsystem can be called R_{FB}.

$$R_{FB} = R_2 R_4 R_\star \tag{5.4}$$

Also, as the components of rear braking subsystem are located in series, its reliability might be expressed as follow. The reliability of rear braking subsystem is called R_{RB} .

$$R_{RB} = R_3 R_5 R_8 R_{11} \tag{5.5}$$

As the result of above calculation, the reliability of the whole braking system can be formulated as follow:

$$\boxed{R_{BrSys} = R_{FB} + R_{RB} - R_{FB} R_{RB}}$$

5.3.2 FMECA

Failure Modes, Effects and Criticality Analysis (FMECA) has been conducted as a partial reliability assessment of the braking system. As it discussed earlier, FMECA is a conducive reliability method in which the potential failures, their effects, and the ways of mitigating them can be specified. This method has been applied with the aim of qualitative assessment of braking system. The conducted FMECA in this project was productive of several good ideas.

As it explained in the proposed process in figure 5.1, the FMECA has been developed and updated during the project. The final result of FMECA is shown in figure 5.5. According to the conducted FMECA, the potential failures only can occur if the braking system is on demand. In the other word, when the vehicle is not moving, obviously there is no need for stopping the vehicle. In order to present FMECA in details, the potential failures of braking system are explained as follow.

- **Assembly**: Assembly and adjustments of the components are considered as one of the concerns that the braking team has been faced with it. Wrong assembly of the components can cause several problems. Optimistically, it causes that the vehicle stop too early. In this scenario, the vehicle is safe, but it might causes friction between pads and disks. Wrong assembly, also, can results in stopping the vehicle too late. This situation is riskier than the

previous one. This can happen if the caliper isn't properly adjusted with disk. Finally, bad assembly might cause that the vehicle doesn't stop. This failure can leads to the catastrophic accident, as the vehicle is not safe in this situation. Although, the probability of this failure for both caliper (front and rear) is relatively low, it needs to be taken into consideration.

- **Pressure**: In order to control the speed of the vehicle or to stop it completely, the user (driver) should put proper (not too high and not too low) pressure on braking levers. Despite, this human failure seems to be negligible, but as it happened before in the former competitions, it has been taken into account.

- **Hydraulic**: The central concerns of the braking team is on the hydraulic system. In this system, the hydraulic fluids that are flowing in the hydraulic lines, transfer the power from the levers to the calipers. The probable failure, which a hydraulic system might be faced with it, is aeration. When the hydraulic fluid is contaminated by the air, aeration happens. Aeration can cause several problems. Air in hydraulic lines can reduce the amount of pressure that leads to caliper dysfunction. Depending on the quantity of the air, the aeration effects are different. In few cases, it reduces the friction between caliper's pads and disk that leads to stop the vehicle too late. However, in many instances, the aeration doesn't let the enough pressure to be passed to the caliper. In this case, the caliper's pads and disk can not be engaged that leads to major, or even catastrophic failure as the vehicle can not be stopped.

In order to mitigate the risks of the potential failure, the braking system team has developed a reliability checklist. Figure 5.6 shows the proposed checklist in which all necessary questions, about reducing the risk of potential failures, are asked. The braking system team, by assembling and disassembling of the braking system in several times, have tried to identify the sources of the potential failures. As a result, possible solutions are foreseen and in the form of checklist's questions are proposed. In the appendix E the possible problems during assembly are shown.

Performed By: Hossein Neizan Hosseini

Systems: Prototype Braking system
Ref.No: 1.1

Description Of Units			Description of failure			Effect of failure		Failure Rate	Severity ranking	Risk reducing measures	Comments
Ref.N	Function	Operational Mode	Failure Mode	Failure Cause	Detection of failure	On the sub-system	On the system function				
1	Stop the Car	Ready to function on demand	Vehicle Stops too early	Bad assembly and adjustment	Detected	Friction force	Protected	4	Minor	Following the checklist	
				High Pressure Input	Detected	Reduce the durability of cliper and disk	Protected	4	Minor	Train the driver	
			Vehicle Stops too late	Bad assembly and adjustment	Detected	N\P	Protected	4	Minor	Following the checklist	
				Existing air in hydraulic lines	Detected	N\P	Protected	4	Major	Beeliding to remove the air	
				Low pressure input	Detected	N\P	Protected	4	Minor	Train the driver	
			Vehicle doesnt Stop	Bad assembly and adjustment	Detected	Reducing durability of the disk/pads	Unprotected	3	Catastrophic	Following the checklist	
				Leakage from seals/connectors/fasteners	Detected	loss of force flow	Unprotected	5	critical	Beeliding to remove the air	
				Caliper doesnt function	Detected	N\P	Unprotected	3	Catastrophic	Using spares parts	
				Existing air in hydraulic lines	Detected	N\P	Unprotected	4	Major	Beeliding to remove the air	

FIGURE 5.5: Failure modes effect, and criticaly analysis for braking system

Reliability Checklist				
System _____ Assembly _____		Ref.No. _____ Date _____		
NO.	M* or A*	Checklist question	Yes	No
1	M	Have the hoses been connected to the connectors?	❑	❑
2	M	Have the calipers been properly adjusted with suspensions?	❑	❑
3	M	Have the hydraulic systems been bled to remove the air?	❑	❑
4	M	Have the caliper pads been properly adjusted with disks?	❑	❑
5	M	Have the levers been properly mounted on steering wheel?	❑	❑
6	M	Have the bolts been checked to avoid leakage?	❑	❑
M* = Mandatory		A*= Advisory		

FIGURE 5.6: Reliability checklist for braking system

5.3.3 FTA

Fault tree analysis, also has been performed to assess the reliability of the braking system. This method has been employed with the aim of qualitative analyzing the braking system. The fault tree, for braking system, is shown in figure 5.7.

The main objective of the fault tree qualitative analysis is to find the minimal cut set (MCS), the potential failures and their importance that may leads to an undesired event [Su and Lei, 2011, P. 899]. The minimal cut sets are identified and shown in table 5.1. The MCSs shows if a set of failure occurs, the undesired event,

which is braking system dysfunction will happen. For example, the cut set (Basic 6, Basic 9) means, if both rear and front hydraulic system have a small amount of the air, the vehicle stop too late which make the TOP event.

According the FTA 5.7, the TOP event occurs if one of its underneath unwanted event (B2, B3, or B4) is occurred. The event B2, which leads to stop the vehicle too early is considered as a braking dysfunction, although the system is safe in this situation. Only one of basic events 1-4 is enough to make event B2. Event B3 that leads to stop the vehicle too late is more critical than B2. In order to make B3 event, at least one basic event in both rear and front braking subsystem must occur. The event B4 is more critical than B2 and B3, as it result the vehicle not to stop. The severity of this failure is catastrophic as it may leads to significant damage to the vehicle or driver. The event B4 is divided by AND-gate to two events B9 and B10. This shows at least one basic failure in B9 and B10 must be occurred to induce not stopping the vehicle.

Numbers	MCS	Numbers	MCS
1	Basic 6,Basic 9	10	Basic 12,Basic 15
2	Basic 6,Basic 10	11	Basic 12,Basic 16
3	Basic 6,Basic 8	12	Basic 12,Basic 14
4	Basic 7,Basic 9	13	Basic 13,Basic 15
5	Basic 7,Basic 10	14	Basic 13,Basic 16
6	Basic 7,Basic 8	15	Basic 13,Basic 14
7	Basic 5,Basic 9	16	Basic 11,Basic 15
8	Basic 5,Basic 10	17	Basic 11,Basic 16
9	Basic 5,Basic 8	18	Basic 11,Basic 14

TABLE 5.1: Minimal Cut Sets from FTA

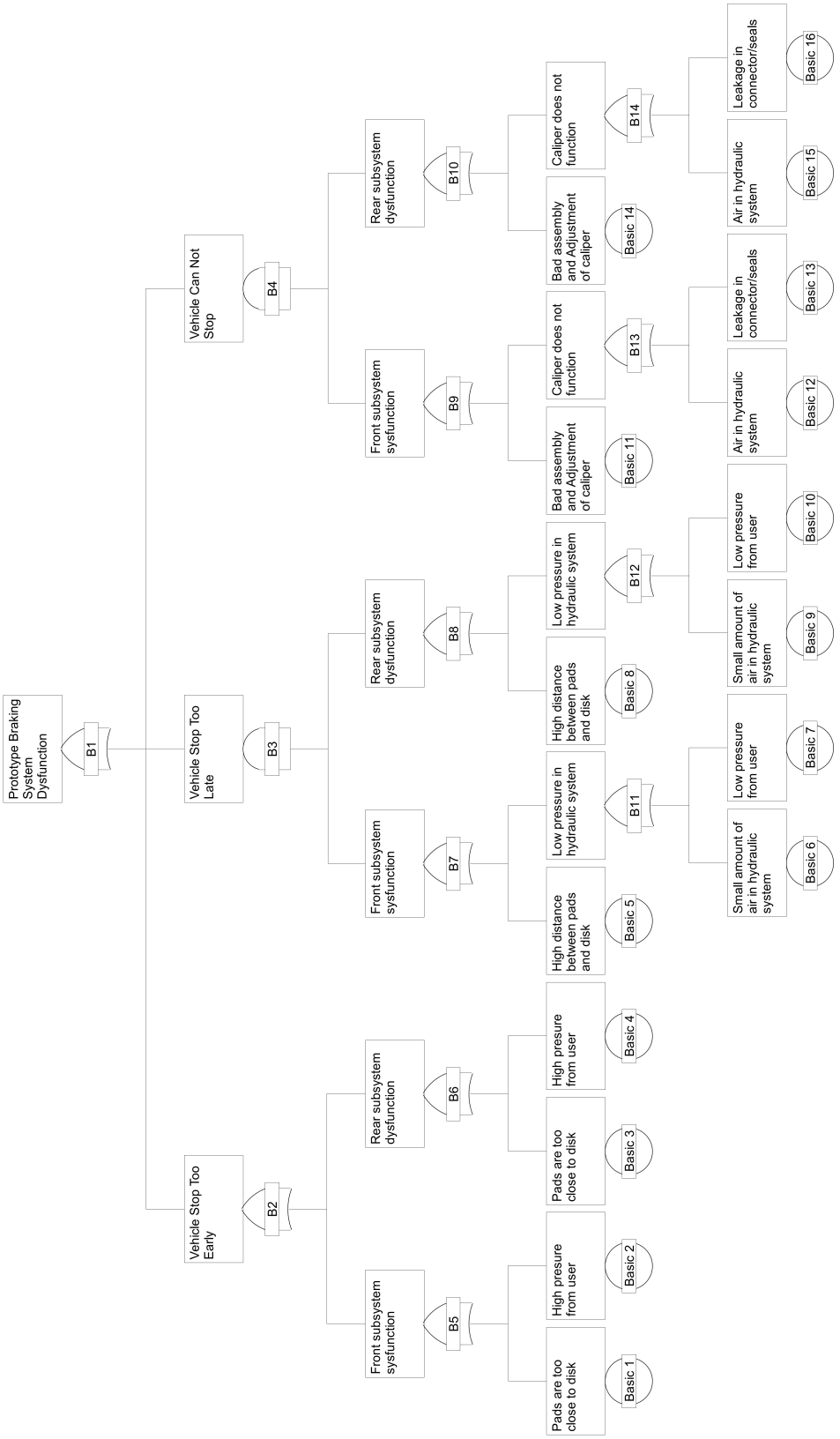


FIGURE 5.7: Fault Tree Analysis (FTA) for braking system

Chapter 6

Discussion

In the previous DNVGLFF project 2014, the former team was faced with problems in the braking system of the prototype vehicle. This study was conducted based on empirical and theoretical research method to identify possible solutions to the mentioned problem. As such, this study began by implementing systems and reliability engineering principles on the prototype system, specifically on its braking system. In order to do so, a number of research questions were formulated. This section will address the research questions and discuss how the results answer each question.

Q.1: how reliability engineering can be valuable for DNVGLFF project?

Implementation of reliability engineering in DNVGLFF 2015 was productive of good results. First, reliability modeling of the prototype system and specifically braking subsystem enabled the author to visualize the system for the members to understand better how system and subsystems are functioning. In addition, employing reliability modeling has revealed that how the subsystems and components are structured dependently or independently. This can be useful to recognize the most critical subsystems and components that any failure to them leads to the whole system failure. Also, from braking system RBD the reliability equation of the braking system is gained. The reliability of the braking system might be

attained by replacing the proper reliability data from each subsystem in the following equation. The result, from braking system reliability, might be useful to be compared with the reliability result of the various available braking system to gain an excellent overview of current system's status.

$$\boxed{R_{BrSys} = R_{FB} + R_{RB} - R_{FB}R_{RB}}$$

Another gained advantage by reliability engineering was to find potential failures of braking system through conducting FMECA. The results from FMECA (figure 5.5) implies that occurring failures in braking system seems to be probable. Also, the experience of the previous team in braking system shows that these potential failures should not be ignored. In order to mitigate the risks of potential failures, the author proposed a reliability checklist in which all necessary tasks with accordance to reduce the risks of potential failures are mentioned. The checklist is shown in figure 5.6. The developed reliability checklist including items that show an instruction must be followed by using the vehicle. It is expected by following this checklist the risks of the potential failures will be reduced.

FTA, also as a partial reliability assessment of the braking system revealed the minimal cut sets that lead to dysfunction in braking system. According to FTA (figure 5.7), the primary concern of the assigned system engineer was to prevent the event B4 as it might be leaded to not stop the vehicle. The result from FTA shows the basic events that contribute to B4 occurs are 11-13 and 14-16. These basic events show that bad assembly and adjustment of the components mostly results in failure in braking system, leakage in connectors, fasteners and seals, and aeration in the hydraulic system. These result from FTA not only has raised the awareness of the team about potential failures they might be faced with, but also reveals the weaknesses of the used braking system.

Limitation The reliability study performed in DNVGLFF was qualitative. Although the author believes that the results are satisfactory for analyzing the reliability of the braking system, however, quantitative reliability also analyzing could

be carried out to better shows the reliability status of the braking system. The reason, for not performing quantitative analysis, was the lack of reliability information of braking system (e.g., $\lambda, MTTF, R$ etc.,). The results from quantitative analysis must be compared with standards, handbooks, or results from real testing of the system, to better show the reliability status of the system.

Q.2: how the Prototype braking system can be designed to be reliable?

Figure 5.4, shows an excellent view of braking system architecture. The architecture design of the braking system seems to be proper as the every wheel has its caliper to stop the wheel's motion. Since the prototype system has three wheels, allocating one caliper to each wheel was a wise decision. Although designing a redundancy caliper with an independent handbrake might result in increasing the safety of the vehicle, this decision with accordance to the limited time and budget was not made.

Q.3: to what extent the potential failures can be tolerable?

The RBD shown in figure 5.4 indicates that the braking system is made by two independent braking subsystems for front wheels and the rear one. Also, the result of FTA suggest that at least one basic event (figure 5.7) must occur in front and rear braking system to prevent vehicle from stopping. As a result, if the risks of potential failures shown in FMECA (figure 5.5) are mitigated by the suggested solutions into the checklist (figure 5.6), at least during the competition it seems remote to have a failures in both rear and front braking subsystem at the same time. For this reason, even in the worst scenario if one braking subsystem (rear or front) fails, the vehicle is still safe.

Chapter 7

Conclusion

This study was set out to implement reliability systems engineering in DNVGLFF 2015 project with the aim of the design for reliability to increase the reliability of the system. The study has also sought to apply reliability analysis specifically on braking system as a critical safety subsystem. The theoretical literature on the subject of braking system reliability specially the one used in this project is not extensive. For this reason, the author has reviewed the proper literature to propose best possible solutions within the scope of this thesis.

The author has pursued two goals concurrently. These goals were applying systems engineering practices including requirements specification, system architecture, and requirements allocation in parallel with implementing reliability engineering methods encompasses reliability block diagrams (RBD), failure mode effect and criticality analysis (FMECA), and fault tree analysis(FTA). The author used V-diagram as the system life cycle with the focus on left-side of this model. As the literature suggests, the reliability engineering incorporated into system life cycle. The process of reliability systems engineering applied in this project is explained in section 5.1.

The main theoretical findings regarding systems and reliability engineering are discussed in chapters 3 and 4 respectively. Also, the results, from implementing the

systems and reliability engineering, are described in chapter 5. The author has analyzed the requirements and made a standard requirement specification document. He also based on specified requirements has designed the high-level architecture of the system of interest. This document can be seen as appendix C. In parallel, as a partial reliability assessment of system he has started to reliability model the braking system by using RBD. The conducted RBD has shown an excellent scheme of braking system structure that was useful to identify dependent and independent components. Also, FMECA was carried out to identify the potential failures in braking system. The outcomes from FMECA made the author able to find proper solutions to mitigate the potential failure's risks. These solutions were proposed in the form of the reliability checklist shown in figure 5.6. Finally, FTA has been employed to recognize the minimal cut sets by which the unwanted events occur. In the FTA, the basic events that cause undesired events revealed how the braking can fail, and how to prevent the system from failure.

The empirical results show that although the braking system is safe, the occurrences of failures is not improbable. The theoretical literature, as a result, suggest conducting reliability study as early as possible to find potential failures and the solutions for mitigating them.

Future Work In spite the results of this study seem to be appropriate for reliability engineering of the braking system with respect to its complexity, it is only one interpretation of the reliability engineering. The scale of this study is extensive even at the subsystem level. As a result, the following items can be used for future research:

- Quantitative reliability analysis on braking system is required to be compared with standards, handbooks, and its counterparts to achieve conclusive results.
- The reliability systems engineering can be performed for both left and right sides of V-diagram to see how reliability engineering can be integrated into production and testing stages of the system life-cycle.

References

(1987). Ieee guide for general principles of reliability analysis of nuclear power generating station safety systems. *ANSI-IEEE Std 352-1987*.

(1998). Ieee standard reliability program for the development and production of electronic systems and equipment. *IEEE Std 1332-1998*.

(2014). Shell eco-marathon. http://www.shell.com/global/environment-society/ecomarathon.html.

(2015). Shell eco-marathon 2015 official rules chapter 1. http://www.shell.com/global/environment-society/ecomarathon/for-participants/general-information/rules.html.

60050-191, I. (1990). Dependability and quality of service. Technical report, International Electrotechnical Commission.

Al-Garni, A. Z., Sahin, A. Z., and Al-Farayedhi, A. A. (1997). A reliability study of fokker f-27 airplane brakes. *Reliability Engineering & System Safety*, 56(2):143–150.

AlmasBerg, I. (2010). Design for reliability applied to develop of subsea process. Master's thesis, Norwegian University of Science and Technology.

Avontuur, G. and van der Werff, K. (2001). An implementation of reliability analysis in the conceptual design phase of drive trains. *Reliability Engineering And System Safety*, 73(2):155 – 165.

Bahr, N. (2000). System safety engineering and risk assessment. *International Encyclopedia of Ergonomics and Human Factors*, 2:1604.

Birolini, A. (2007). *Reliability engineering*, volume 5. Springer.

Blanchard, B. S. and Fabrycky, W. J. (1990). *Systems engineering and analysis*, volume 4. Prentice Hall, Englewood Cliffs, New Jersey.

Boniardi, M., D'Errico, F., Tagliabue, C., Gotti, G., and Perricone, G. (2006). Failure analysis of a motorcycle brake disc. *Engineering Failure Analysis*, 13(6):933–945.

Bronwyn Becker, Patrick Dawson, K. D. C. H. S. H. J. L. D. M. C. T. and Palmquist, M. ((1994 - 2012)). Research methodology: Case studies. http://writing.colostate.edu/guides/guide.cfm?

CARDEROCKDIV, N.-. (2010). Handbook of reliability prediction procedure for mechanical equipment. Technical report, NAVAL Surface Warfare Center.

Carlson, C. (2012). *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis*, volume 1. John Wiley & Sons.

Cepin, M. (2011). Reliability block diagram. In *Assessment of Power System Reliability*, pages 119–123. Springer London.

Cheng, Z., Wang, X., Tian, C., and Wang, F. (2009). Mission reliability simulation of high-speed emu service braking system. In *Reliability, Maintainability and Safety, 2009. ICRMS 2009. 8th International Conference on*, pages 253–256. IEEE.

Clausing, D. and Frey, D. D. (2005). Improving system reliability by failure-mode avoidance including four concept design strategies. *Systems Engineering*, 8(3):245–261.

Crowe, D. and Feinberg, A. (2010). *Design for reliability*. CRC press.

Eisner, H. (2008). *Essentials of project and systems engineering management*. John Wiley & Sons.

Engel, A. (2010). *Verification, Validation, and Testing of Engineered Systems*, volume 84. John Wiley and Sons, Inc.

Filippi, S. and Cristofolini, I. (2009). *The design guidelines collaborative framework: a design for Multi-X method for product development.* Springer.

Fohn, S., Greef, A., Young, R., and O'Grady, P. (1995). Concurrent engineering. In *Information Management in Computer Integrated Manufacturing*, volume 973 of *Lecture Notes in Computer Science*, pages 493–505. Springer Berlin Heidelberg.

Gonzalez, P. J. (2002). Building quality intelligent transportation systems through systems engineering. Technical report, Federal Highway Administration.

Grady, J. O. (2014). 1 - introduction. In Grady, J. O., editor, *System Requirements Analysis (Second Edition)*, pages 1 – 92. Elsevier, Oxford, second edition edition.

Harkins, W. (1999). Public lessons learned entry 0757. http://www.nasa.gov/offices/oce/llis/0757.html.

Haskins, C. (2010). *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities.*

Holt, R. and Barnes, C. (2010). Towards an integrated approach to design for x: an agenda for decision-based dfx research. *Research in Engineering Design*, 21(2):123–136.

Johannes Aalberg, Mats Bovre, M. K. I. O. S. N. (2014). Dnv gl fuel fighter. Thesis.

Jung, W., Kim, G., and Ismail, A. (2012). Reliability improvement of brake pads 2014; case study. In *Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012 International Conference on*, pages 7–11. IEEE.

Kamrani, A. K. and Azimi, M. (2012). *Systems Engineering Tools and Methods.* CRC Press.

Kececioglu, D. (2002). *Reliability engineering handbook*, volume 1. DEStech Publications, Inc.

Kohda, T. and Fujihara, H. (2008). Risk analysis of level crossing accidents based on systems control for safety. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 222(3):419–429.

Kossiakoff, A. and Sweet, W. N. (2003). *Systems Engineering; Principles and Practice*. John Wiley & Sons.

Kossiakoff, A., Sweet, W. N., Seymour, S., and Biemer, S. M. (2011). *Systems engineering principles and practice*, volume 83. John Wiley & Sons.

Kuo, T.-C., Huang, S. H., and Zhang, H.-C. (2001). Design for manufacture and design for x: concepts, applications, and perspectives. *Computers & Industrial Engineering*, 41(3):241–260.

Liu, Y. Rams engineering and management. Lecture notes.

Maskell, B. H. (1991). *Performance measurement for world class manufacturing: A model for American companies*. Productivity Press.

Min, L., Meng-lin, W., and Xiao-Yan, W. (2010). Study on reliability test for brake control execution unit of rail transit vehicle. In *E-Product E-Service and E-Entertainment (ICEEE), 2010 International Conference on*, pages 1–4. IEEE.

Mital, A., Desai, A., Subramanian, A., and Mital, A. (2014). Chapter 8 - designing for maintenance. In Mital, A. M. D. S., editor, *Product Development (Second Edition)*, pages 203 – 268. Elsevier, Oxford, second edition edition.

Moriarty, B. (2012). Integrating design for reliability with design for safety. *Design for Reliability*, pages 253–266.

Norman B, F. (2005). Developing reliability requirement. Technical report, Alion System Reliability Center.

O'Connor, P. and Kleyner, A. (2011). *Practical reliability engineering*. John Wiley & Sons.

Online, E. B. (2014). systems engineering. http://global.britannica.com/EBchecked/topic/579234/systems-engineering.

Pecht, M. and Dasgupta, A. (1995). Physics-of-failure: an approach to reliable product development. In *Integrated Reliability Workshop, 1995. Final Report., International*, pages 1–4. IEEE.

Pineda, R. L. and Kilicay-Ergin, N. (2012). System verification, validation, and testing. *Systems Engineering Tools and Methods*, page 81.

Popovic, P., Ivanovic, G., Mitrovic, R., and Subic, A. (2011). Design for reliability of a vehicle transmission system. *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, page 0954407011416175.

Pyster, A., Olwell, D., Hutchison, N., Enck, S., Anthony, J., Henry, D., and Squires, A. (2012). Guide to the systems engineering body of knowledge (sebok) version 1.0. hoboken, nj: The trustees of the stevens institute of technology© 2012.

Raheja, D. G. and Gullo, L. J. (2012). *Design for reliability*. John Wiley & Sons.

Rausand, M. (2014). *Failures and Failure Analysis*, pages 53–76. John Wiley & Sons, Inc.

Rausand, M. and Høyland, A. (2004). *System reliability theory: models, statistical methods, and applications*, volume 396. John Wiley & Sons.

Rechtin, E. and Maier, M. W. (2000). *The art of systems architecting*. CRC Press.

Sage, A. P. and Rouse, W. B. (2009). *Handbook of systems engineering and management*. John Wiley & Sons.

Sharvia, S. and Papadopoulos, Y. (2015). Integrating model checking with hiphops in model-based safety analysis. *Reliability Engineering & System Safety*, 135:64–80.

Sheard, S. A. (1996). Twelve systems engineering roles. volume 17, pages pp.481–488. Proc Sixth Annuual Int Symp INCOSE, Boston, USA.

Sinha, P. (2011). Architectural design and reliability analysis of a fail-operational brake-by-wire system from iso 26262 perspectives. *Reliability Engineering & System Safety*, 96(10):1349–1359.

Soleimani, M. and Pourgol-Mohammad, M. (2014). Design for reliability of complex system with limited failure data; case study of a horizontal drilling equipment. *Proceedings of the Probabilistic Safety Assessment and Management PSAM*, 12.

Stevens, Richard, P. B. K. J. and Arnold, S. (1998). *Systems engineering: coping with complexity*. Pearson Education.

Su, X. and Lei, Z. (2011). Methodology for visualized fault tree analysis. In *Electronics, Communications and Control (ICECC), 2011 International Conference on*, pages 898–901.

Tan, Q., Qi, H., Li, J., and Tian, Y. (2012). The reliability modeling and analysis on brake system of medium-low speed maglev train. In *Computer Distributed Control and Intelligent Environmental Monitoring (CDCIEM), 2012 International Conference on*, pages 772–777. IEEE.

Tanner, D., Walraven, J., Mani, S., and Swanson, S. (2002). Pin-joint design effect on the reliability of a polysilicon microengine. In *Reliability Physics Symposium Proceedings, 2002. 40th Annual*, pages 122–129.

Teller, A. (2014). The implementation of system modeling methods in safety engineering. In *Reliability and Maintainability Symposium (RAMS), 2014 Annual*, pages 1–5. IEEE.

Vatn, J. (2013). *Project Risk Analysis*. Norwegian University of Science and Technology.

W.S.Afleck, G. (2013). Milage marathons. http://www.byronwine.com/files/Shell%20P221.pdf.

Xie, X. (2003). Design for manufacture and assembly. *Utah: Dept. of Mechanical*.

Xing, L. and Amari, S. V. (2008). Fault tree analysis. In *Handbook of performability engineering*, pages 595–620. Springer.

Yang, G. (2007a). *Life cycle reliability engineering*. John Wiley & Sons.

Yang, G. (2007b). *Reliability Definition, Metrics, and Product Life Distributions*, pages 9–32. John Wiley & Sons, Inc.

Yin, R. K. (2014). *Case study research: Design and methods*. Sage publications.

Young, R. R. (2002). Recommended requirements gathering practices. *CrossTalk*, 15(4):9–12.

Young, R. R. (2006). *Project requirements: A guide to best practices*. Management Concepts Inc.

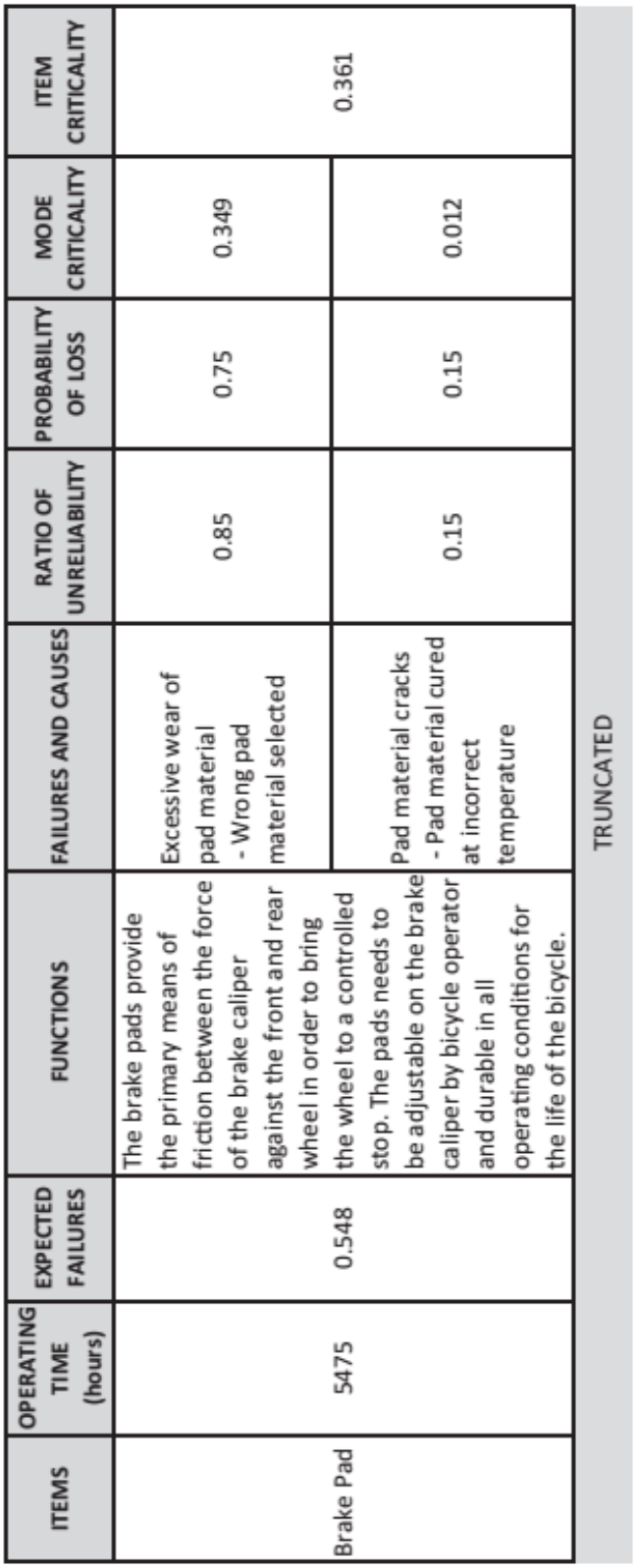
Zhang, Y. and Liu, Q. (2002). Reliability-based design of automobile components. *PROCEEDINGS OF THE INSTITUTION OF MECHANICAL ENGINEERS PART D-JOURNAL OF AUTOMOBILE ENGINEERING*, 216(D6):455–471.

Zhifa, Y., Wang, J., Xuefeng, S., Jinhai, Z., Yu, W., and Xu, Y. (2011). The brake system reliability evaluation of a type of jiefang truck based on go methodology. In *Transportation, Mechanical, and Electrical Engineering (TMEE), 2011 International Conference on*, pages 1224–1227. IEEE.

Appendix A

Quantitative FMECA

An example of quantitative FMECA for a bicycle braking pad:



ITEMS	OPERATING TIME (hours)	EXPECTED FAILURES	FUNCTIONS	FAILURES AND CAUSES	RATIO OF UNRELIABILITY	PROBABILITY OF LOSS	MODE CRITICALITY	ITEM CRITICALITY
Brake Pad	5475	0.548	The brake pads provide the primary means of friction between the force of the brake caliper against the front and rear wheel in order to bring the wheel to a controlled stop. The pads needs to be adjustable on the brake caliper by bicycle operator and durable in all operating conditions for the life of the bicycle.	Excessive wear of pad material - Wrong pad material selected	0.85	0.75	0.349	0.361
				Pad material cracks - Pad material cured at incorrect temperature	0.15	0.15	0.012	
TRUNCATED								

FIGURE A.1: A Example quantitative FMECA for a bicycle braking pad [Carlson, 2012]

Appendix B

Gantt Diagram

B.1 Improvement of Rims, Battery tray, and Safety

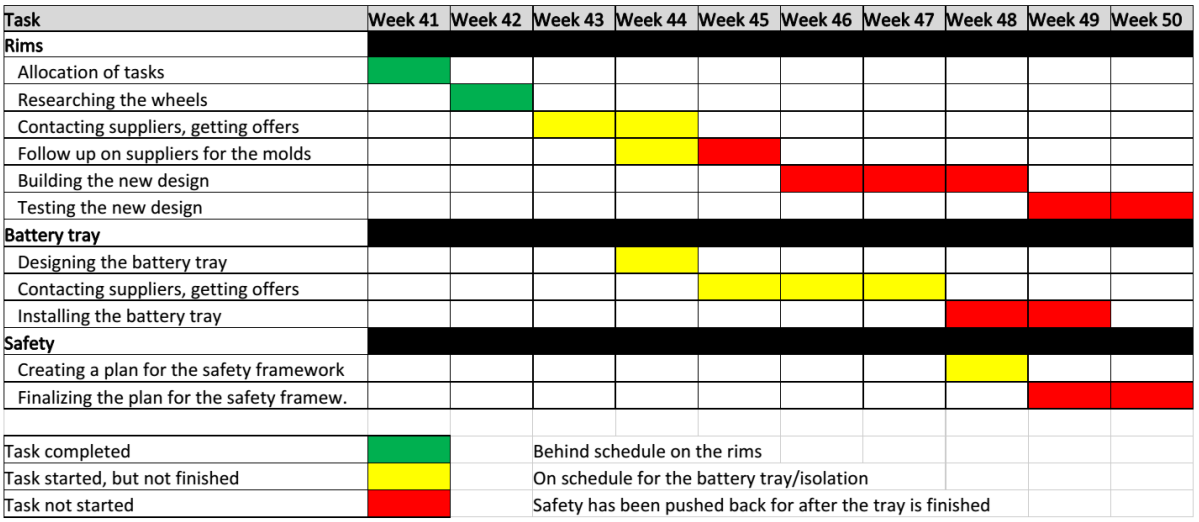


FIGURE B.1: Gantt chart for rims, battery tray, and safety improvement

B.2 Improvement of Transmission, Wheels, and Rear Suspension

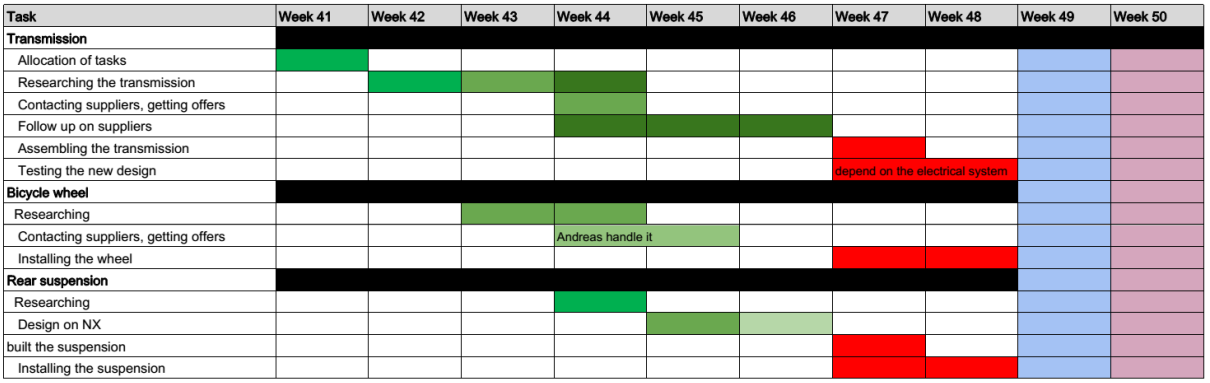


FIGURE B.2: Gantt chart for Transmission, Wheels, and Rear Suspension improvement

B.3 Improvement of Steering, Covers for the linkage, Display, and Dead-man-switch

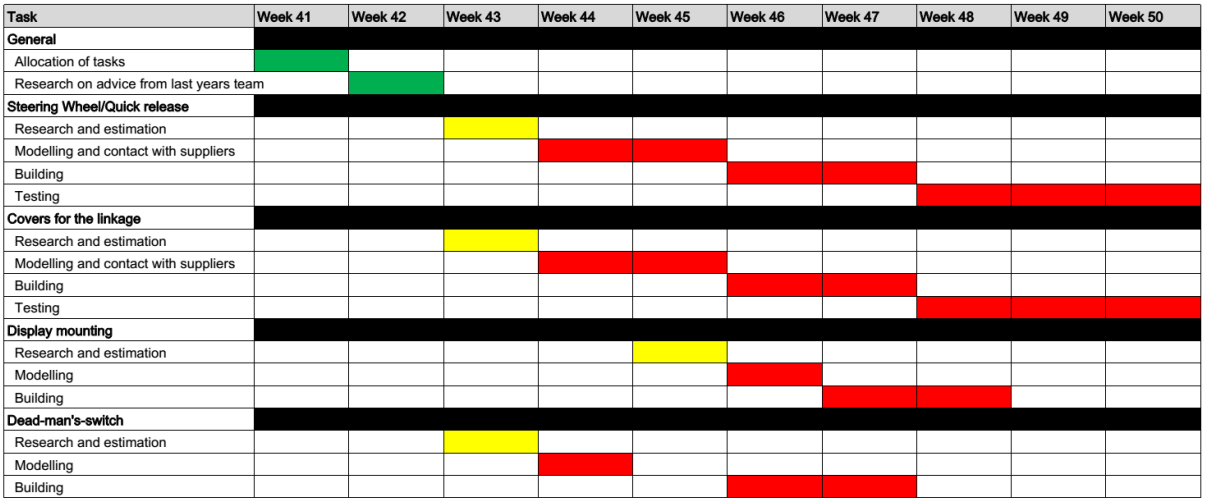


FIGURE B.3: Gantt chart for Steering, Covers for the linkage, Display, and Dead-man-switch improvement

B.4 Improvement of Propulsion system

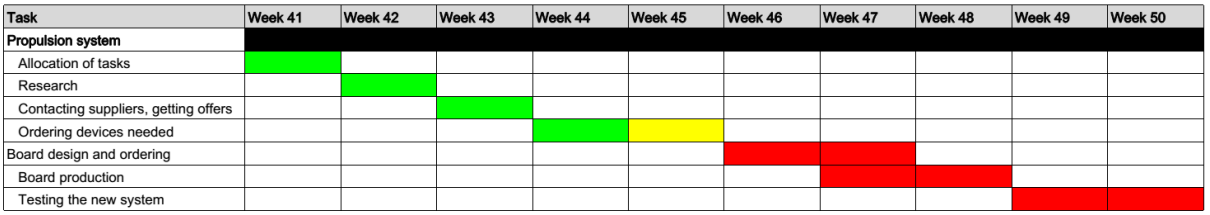


FIGURE B.4: Gantt chart for Propulsion system improvement

Appendix C

System Requirements Specification

SYSTEM REQUIREMENTS SPECIFICATION

for

DNV GL Prototype Vehicle Improvement

Release 1.0

Version 1.0approved

Prepared by Hossein Neizan Hosseini

C.1 Introduction

C.1.1 Purpose

The requirement specification document describes the functions and requirements specified for DNV GL prototype vehicle. The vehicle (system) is needed to participate in the Shell Eco-Marathon completion. This project is run voluntarily by some students from Norwegian University of Science and Technology.

C.1.2 Business Context

This project is carried out mainly under sponsorship of DNV GL with the purpose of reducing the amount of energy used in the next generation of the vehicles. Also, the companies SEGGER, Elprint Norge, and Wright are supporting this project.

C.1.3 Scope

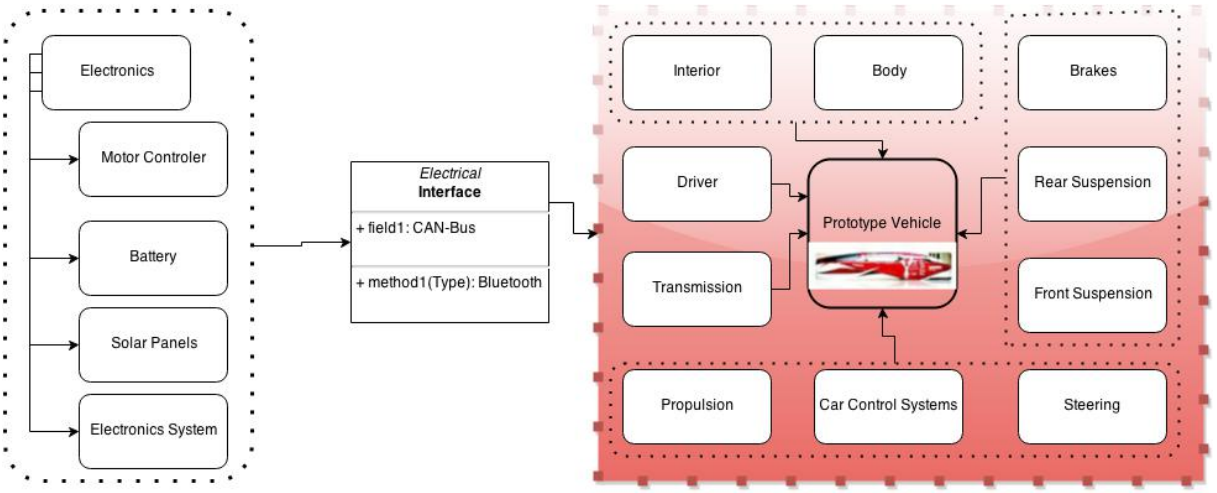
The purpose of this project is to improve and develop DNVGL Prototype 2014, in order to participate in the Shell Eco-marathon as one of the most energy efficient vehicles on the planet.

C.1.4 User Characteristics

As it mentioned before, this project is considered as one of the contest driven project, and it is not a commercial project for specific user. The prototype vehicle is an inspiration for next generation to make real transportation vehicles with very low usage of energy.

C.2 Overall Description

C.2.1 System Perspective



C.2.2 System Architecture

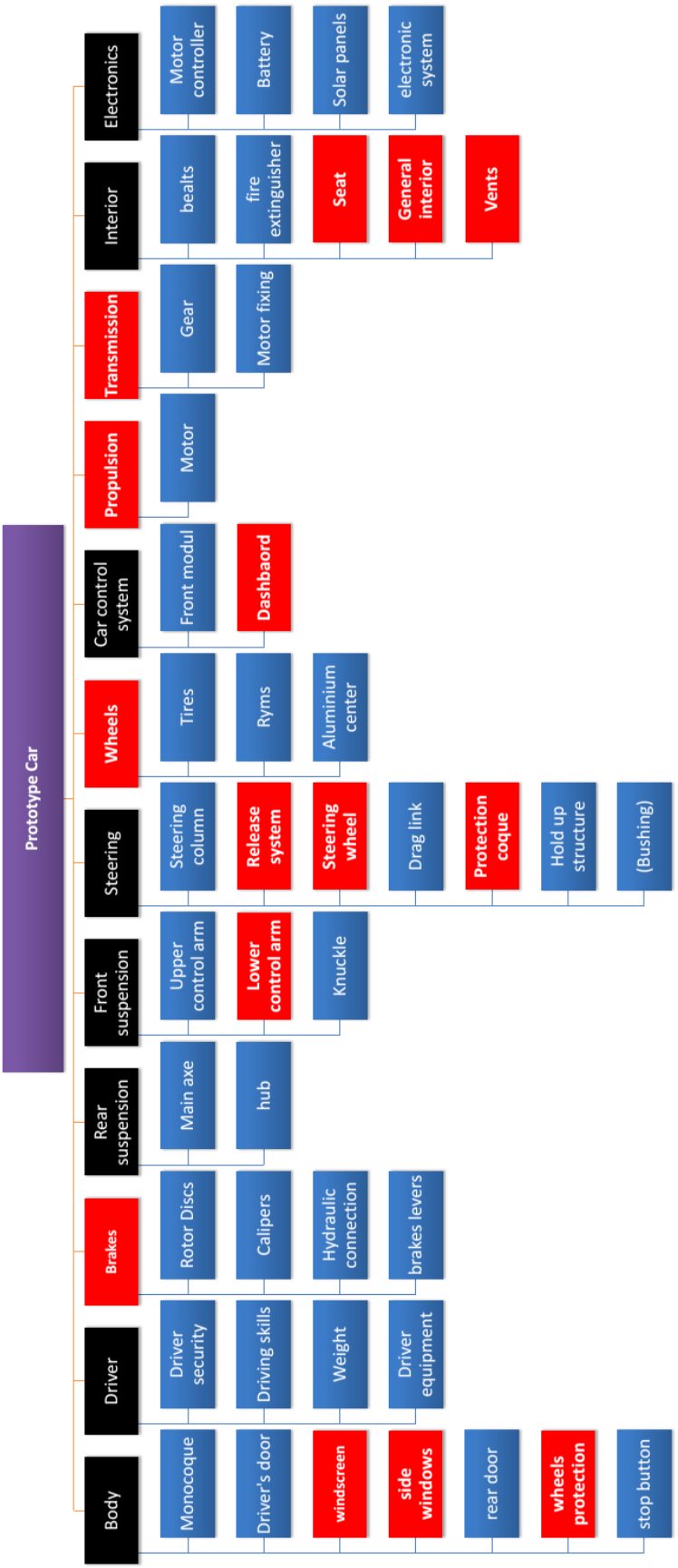
As it can be seen in the picture below, the red blocks are those components that need to be improved. The reasons for improvements are explained briefly as follow:

- It has suggested by the previous team to improve the windows and the panels as the solution of using tape wasn't satisfactory. The tape must be replaced with another solution as the windows and the panels that cover the front wheels seem vulnerable during the movement or the race.
- The installed hydraulic braking system was apparently satisfactory. However, its components in terms of reliability and durability must be improved.
- For the suspension, a new solution can be considered to fix the rear axle for easier mounting and detaching of the rear wheel.
- General performance of steering system was acceptable, however, some improvements are needed. For example, quick release mechanism, fixing the

cables, and new design of steering linkage cover are the areas of the improvement.

- The production of the rims are very important. As the previous team recommended, some test regarding the materials especially fiber needs to be taken.

- The interior part of the prototype must be more comfortable and luxury as it wasn't before. The messy appearance of the interior leads to damage cables that can be covered properly.


Prototype Car
Body
Monocoque
Driver's door
windscreen
side windows
rear door
wheels protection
stop button
Driver
Driver security
Driving skills
Weight
Driver equipment
Brakes
Rotor Discs
Calipers
Hydraulic connection
brakes levers
Rear suspension
Main axe
hub
Front suspension
Upper control arm
Lower control arm
Knuckle
Steering
Steering column
Release system
Steering wheel
Drag link
Protection coque
Hold up structure
(Bushing)
Wheels
Tires
Ryms
Aluminium center
Car control system
Front modul
Dashbaord
Propulsion
Motor
Transmission
Gear
Motor fixing
Interior
bealts
fire extinguisher
Seat
General interior
Vents
Electronics
Motor controller
Battery
Solar panels
electronic system

C.3 System Capabilities, Condition, and Constraints

C.3.1 Functional Requirements

New value is recognized from the Shell-Eco Marathon Rules for 2015.

Description	Old valve	New Value
Functional Requirements		
Turning Radius (NB: Only front wheel steering is allowed)	10 m	8 m
Brakes can hold the car still while in incline (with driver inside)	20 degree slope	20 degree slope
Difference in weight before and after an attempt	≤ 1 kg	≤ 1 kg
Running wheels	3-4	3-4
Sharp point radius	≥ 5 cm	≥ 5 cm
Distance between driver's helmet and roll bar	≥ 5 cm	≥ 5 cm
Arc of visibility on each side of the longitudinal axis of the vehicle	90 degrees	90 degrees
Surface area of the rear view mirror (one on each side of the vehicle)	> 25 cm2	> 25 cm2

C.3.2 Design Requirements

Design requirements	Old value	New Value
Height of car	< 100 cm	< 100 cm
Width of car	≤ 130 cm	≤ 130 cm
Distance between wheels (Front - Rear)	< 100 cm	< 100 cm
Track width	> 50 cm	> 50 cm
Length of car	< 350 cm	< 350 cm
Height of car/track width	< 1.25	< 1.25
Vehicle weight (excluding driver)	≤ 140 kg	≤ 140 kg

C.3.3 Safety Requirements

Safety	Old Value	New Value
ABC extinguisher capacity (NB: Needs to be never used and not expired)	≥ 1 kg	≥ 1 kg
Effective equipment to mitigate/control Lithium based battery fires during charging	None	See comment
Bulkhead height from highest point of propulsion/fuel system/drivers' shoulders (open design)	≥ 5 cm	≥ 5 cm
Static load applied vertical, horizontal and perpendicular to the roll bar	700 N	700 N
Topmost straps angle below the shoulder line	≥ 10 degrees	≥ 10 degrees
Weight the safety harness buckle must withstand	1,5 x drivers weight	1,5 x drivers weight
Evacuation time of fully harnessed driver	< 10 s	< 10 s
Dimensions of red arrow (showing the emergency shutdown actuator)	≥ 10 x 3 cm	≥ 10 x 3 cm
Must be equipped with automatic engine/motor shutdown in case of driver incapacitation	None	See comment
Voltage on board the vehicle at any time (max)	< 60 volts	< 60 volts
Voltage on board the vehicle at any time (nominal)	< 48 volts	< 48 volts
Lithium-batteries must be equipped with a metal tray, able to withstand a thermal runoff by the batteries	None	Needed
Mounting points for the driver's seat	≥ 5	≥ 5

C.3.4 Environment Requirements

Environmental requirements	Old Value	New value
Electric horn sound measured 4 meters horizontally from the vehicle	> 85 dBa	> 85 dBa
Pitch of horn	≥ 420 Hz	≥ 420 Hz
Sound levels of vehicle measured 4 meters away from the vehicle	< 90 dBa	< 90 dBa
Percentage of solar energy	≤ 20 %	≤ 20 %
Total combined surface area of solar cells (10 cells 5x5 inches or 7 cells 6x6 inches)	< 0,17 m2	< 0,17 m2

C.3.5 Standards Requirements

Standardization	Old Value	New Value
Shell logo on the front and each side (width x height)	20 x 20 cm	20 x 20 cm
Racing number on the front and each side (width x height)	20 x 26 cm	20 x 26 cm
Partner streamer on each side of the lower body (width x height)	90 x 6 cm	90 x 6 cm
Space on each side of the Shell logo	10 cm	10 cm
Total sponsor stickers space	400 cm2	400 cm2

Appendix D

FMECA failure rate and severity ranking tables

Failure Rate		
1	Very Unlikely	Once per 1000 years
2	Remote	Once per 100 years
3	Occasional	Once per 10 years
4	Probable	Once per year
5	Frequent	Once per month or more often

Severity Ranking		
10	Catastrophic	Failure results in major injury or death of personnel
7 \9	Critical	Failure results in minor injury to personnel, personnel exposure to harmful chemicals or radiation, or fire or a release of chemical to the environment
4\6	Major	Failure results in a low level of exposure to personnel, or activates facility alarm system
1\3	Minor	Failure results in minor system damage but does not cause injury to personnel, allow any kind of exposure to operational or service personnel or allow any release of chemicals into the environment

Appendix E

The process of braking system assembly

The figure E.1 shows how caliper engages the disk.

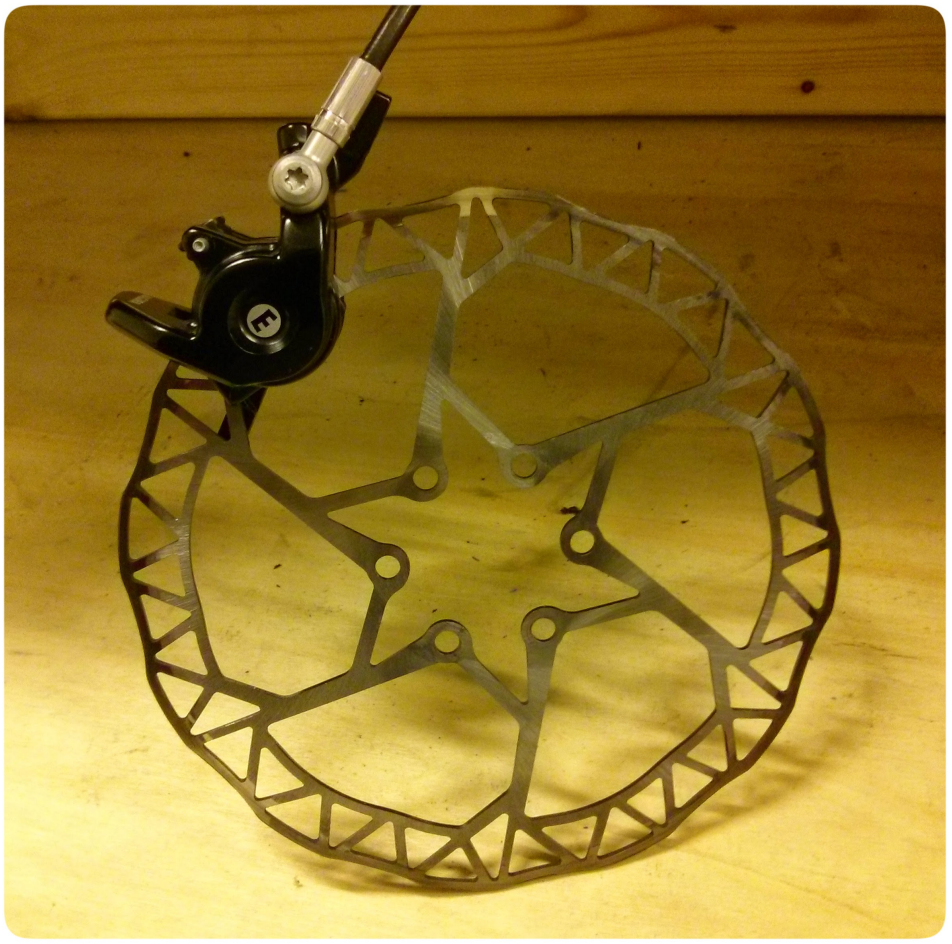


FIGURE E.1: engaging the caliper with disk

In the figure E.2, the colored arrow shows the proper distance between caliper and suspension. Inappropriate distance between caliper and suspension might leads to caliper dysfunction.

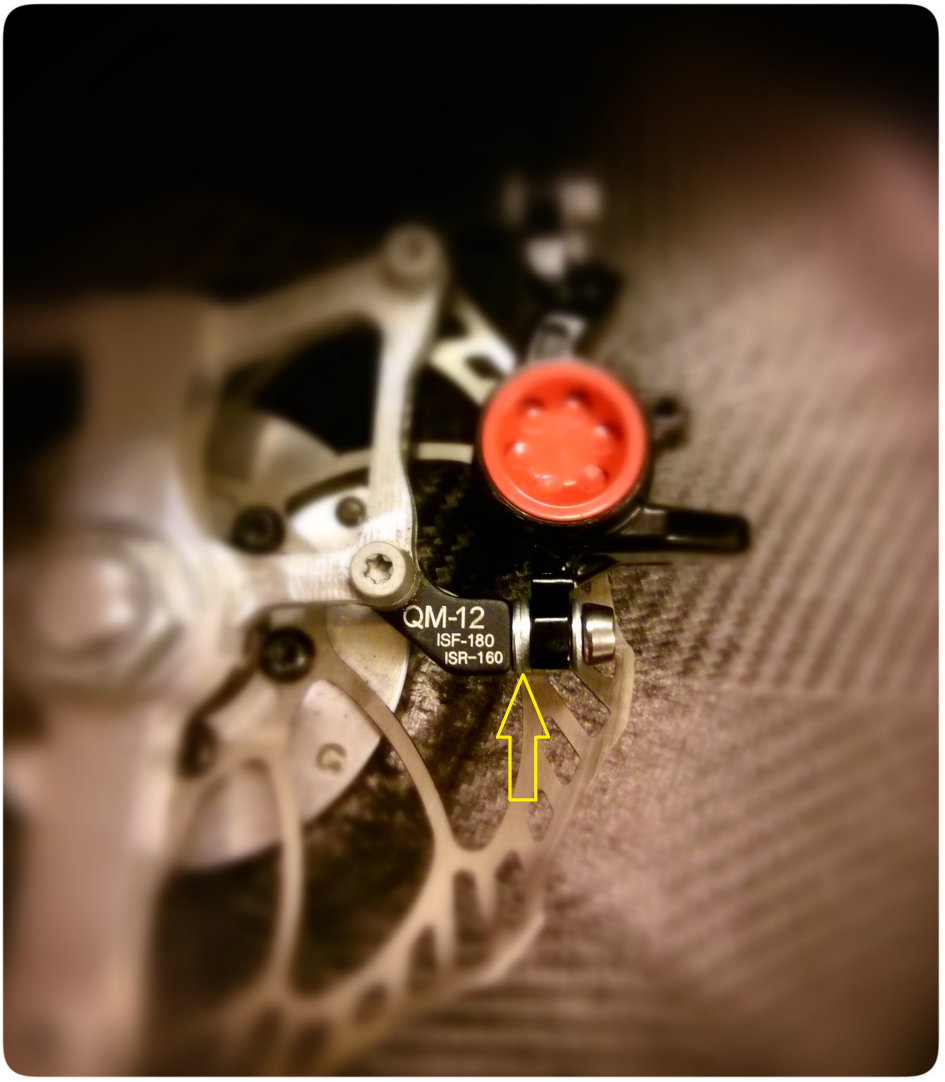


FIGURE E.2: The proper distance between caliper and suspension

The figure E.3 shows the process of filling the hydraulics system with particular liquid. This process also is carried out to bleed the hydraulic lines.

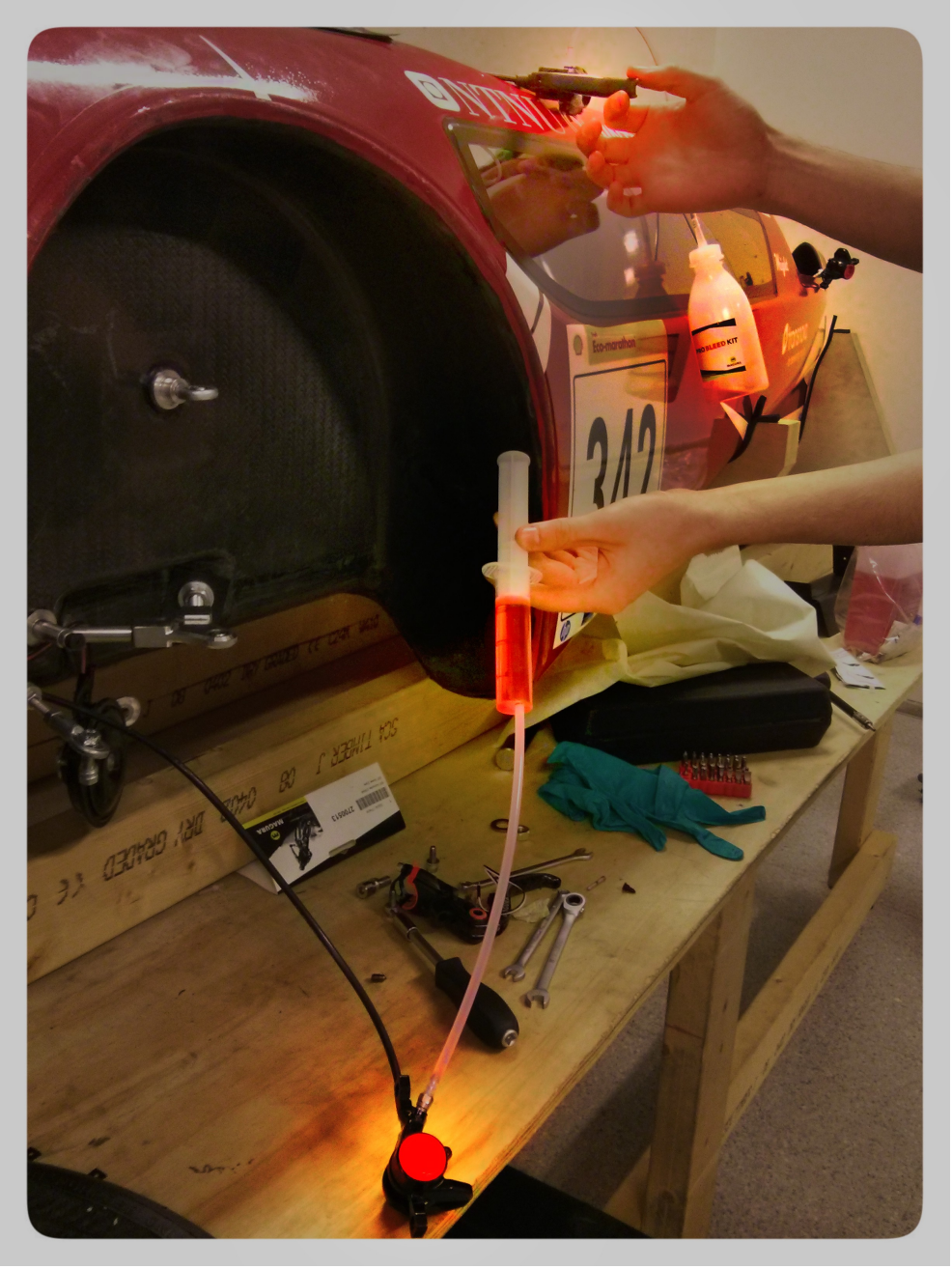


FIGURE E.3: The process of filling the hydraulic system with hydraulic liquid

In the figure E.4 the colored arrow shows the leakage around the lever bolt. The leakage might leads to reduce the pressure in the hydraulic lines.

FIGURE E.4: Leakage around the lever bolt