Linköping University | Division of Fluid and Mechatronic Systems
Master Thesis | Mechanical Engineering
Spring 2018 | LIU-IEI-TEK-A--18/03195–SE

Safety analysis on digital hydraulics
Redundancy study for aviation applications

Robert Pettersson

Supervisor:
Petter Krus, IEI, Linköping University

Co-advisors:
Victor Juliano De Negri, Federal University of Santa Catarina
Heitor Azuma Kagueiama, Federal University of Santa Catarina

Examiner:
Ingo Staack, IEI, Linköping University

Linköping University
SE-581 83 Linköping
013-28 10 00, www.liu.se

Upphovsrätt

Copyright

Abstract

Digital hydraulic actuators (DHA) are an interesting new technology that could replace todays system with inefficient proportional valves. By using an array of on/off valves the hydraulic pressures are discretised. This gives a fixed set of force outputs that can be used to control the actuator. DHA systems have been proven to drastically reduce the energy consumption at the cost of higher system complexity. More components and more advanced controllers are needed to maintain an equal system performance.

Previous research has been mentioning the fault tolerance of the DHA system without analysing the actual requirements to achieve it. In this thesis a safety analysis is made. One first approach of making an active fault tolerant system is presented and the effects of using this is analysed. In total, over four million failure modes are analysed and grouped into 2402 system outputs. The thesis is also the first within the research of DHA system to present a chamber wise analysis, where all four chambers are analysed independently.

The thesis also presents a method to calculate reliability for the system. The method is a new computational way of creating and reducing fault trees. From the fault trees the probability of system failure can be calculated.

The conclusion of this thesis is that DHA is not fault tolerant by default but can be if designed correctly. The thesis also concludes that if the components in the DHA system have the same reliability as the components used in today's system the reliability is similar.

Acknowledgments

The writing of this master thesis has been a fantastic journey. Not just a journey to another continent but also a journey of personal development. On the way I have meet a lot of people that deserve acknowledgements. First, my supervisor Petter Krus, director of hydraulic department FluMes (Linköping university), who enabled this trip. From the first email in June 2017 until the presentation a year later Petter was always a helping hand. My co-advisors also had a big part of this. Victor Juliano De Negri is the director of the hydraulic laboratory LASHIP (Federal University of Santa Catarina) where I had my desk during the work. He supervised me in the hydraulics parts. My other co-advisor Heitor Azuma Kagueiama, together with professor Acires Dias, thought me everything I know about reliability. Their help was crucial for this thesis.

Ingo Staack was the examiner of this thesis and gave me good advice along the way. Alessandro Dell'Amico is the project leader for the research project and my contact to SAAB. He was the one who wrote the thesis proposal and followed the work until it was finished. In the final part of the thesis Karin Gustafsson and Sofia Viklinder made huge effort proofreading the text.

Then of course we have all the other students working at LASHIP. They taught me both about hydraulics and other important things such as the ways to the best beaches in Florianópolis. Some special thanks also to my Brazilian room mate Henrique Raduenz and my study buddy Pablo Antunes for getting me through the first scary weeks in a foreign country.

Finally, I want to thank all the fantastic people I have met during my stay here - all Brazilian orienteers, the other students in the Portuguese class and in the samba class, all the exchange students I met and a lot of other people. Thank you all, you have been truly amazing.

Florianópolis, Brazil, May 2018

Robert Pettersson

Contents

Nomenclature

Common variables

$\emptyset$	Empty state	
κ	Rate of force	
λ	Constant failure rate	1/h
A_y	Area chamber y	m^2
C_x	Closed state valve x	
F^A	Force from actuator	N
N	Normal state	
n_{dist}	Number of force distributions	
O_x	Open state valve x	
$P(t)$	Probability function	
p_y	Pressure chamber y	Pa
p_{sx}	Pressure source x	Pa
S_y	State in chamber y	
t	Time	h
V_{xPy}	Valve that links p_{sx} and A_y	
x	Pressure index	
y	Chamber index	
z	Failure mode index	

Sets

$\mathbb{A}_{index}$	Set of chamber indices
$\mathbb{F}$	Set of forces

$\mathbb{P}_y$	Set of pressures in chamber y
$\mathbb{P}_{index}$	Set of pressure indices
$\mathbb{S}$	Set of chamber states
$\mathbb{V}$	Set of all on/off valves

Chapter 1

Introduction

1.1 Background

Fluid power is used all over the world to transfer energy and create motion. Estimations show that over 2% of the total power consumption in the United States come from fluid power systems. With an average energy efficiency of 21% there are a lot of possible energy savings to be made. [24]

Most of the hydraulics on the market today uses throttling valves to control the hydraulic flow, this leads to substantial energy losses. In a research project between SAAB AB (SAAB), Linköpings University (LiU) and Federal University of Santa Catarina (UFSC), digital hydraulics for aircraft applications is studied [25]. Digital hydraulics is one research branch aiming to reduce the losses created by throttling, by replacing throttling valves with discrete on/off valves. Previous research in the area shows a reduced energy consumption by 80% but to a cost of precision [5]. Other research with a hybrid design combining accuracy of conventional system with the energy efficiency of digital hydraulics shows promising results of with over 30% reduced energy consumption and withheld precision [26].

The aviation industry has strict regulation for security and redundancy [8]. For the hydraulics in aircraft applications the redundancy requirement is fulfilled with multiple separate systems [20] or tandem configurations, where two independent hydraulic systems work on the same actuator [5].

1.2 Purpose

This master thesis is part of an ongoing research project on digital hydraulics for aircraft applications run by SAAB, LiU and UFSC [25]. The purpose of this thesis is to investigate security and redundancy of the digital hydraulic system proposed by the project.

1.3 Objectives

Objectives for this master thesis are to investigate if a Digital Hydraulic Actuator (DHA) can be a *fault-tolerant* [7] system and to present a method for reliability calculations on a DHA system.

Questions considered in this thesis are:

1. Is it possible to design a controller that makes DHA *active fault-tolerant* [7]?
2. What system parameters affect the fault tolerance?
3. Is DHA an appropriate choice, in terms of safety, for aviation applications?

1.4 Method

Since no previous studies has been made on safety for DHA systems an iterative process were used to investigate the possibilities of the system. Ideas were tested, rejected and refined until the theories and methods used in this thesis were discovered.

The result was to use a Fault Tree Analysis (FTA) as a main method to investigate the effects of component failures. However, the conventional logical, top-down, method for constructing fault trees [10] is not applicable straight off. The system complexity makes it impossible see the result of a component error without using calculations. Therefore, a uniquely designed computational FTA method is used in an initial part. This computational algorithm is described in detail in this thesis. After this initial part conventional FTA is used.

Simulation is used to identify appropriate inputs for the computational algorithm. For simulation the hydraulic simulation tool HOPSAN [18] is used.

1.5 Delimitations

The following delimitations have been made:

- In this thesis fixed wing aircraft will be studied.
- The current failure mode for every component: *normal operation/ closed failure/ open failure* etc. is considered to be known. Fault detection and diagnose are disclosed.
- Only one manoeuvre will be simulated, a change in altitude. This means that only the pitch angle will be affected. Therefore, only the control surfaces responsible for pitch motion will be analysed.
- Pressure line failures are not included in reliability calculations due to lack of data.
- Time-independent/constant fault rate of the components is assumed.

1.6 Outline

This thesis starts with **2. Literature study** containing relevant background to understand the thesis. In next chapter, **3. Theoretical studies**, the studied system is presented along with notations and equations. Some of the notations differ from previous research in the field of digital hydraulics, these are especially explained. After the system is described a methodology for doing **Fault Tree Analysis** is presented in chapter 4. This methodology differ from conventional fault tree methodologies. In chapter **5. Simulations** the simulation environment is described. The used simulation model is from previous research [26] and therefore only changes are presented. After all methodologies are explained these are applied and shown in **6. Results**. In this chapter some probability calculations are presented. Many assumptions are made for these calculations. Assumptions are presented along with the results. Chapter **7. Discussion** includes a discussion about the whole thesis. As a final chapter **8. Conclusion** answers the objectives of the thesis and makes some suggestions for further works within the subject.

Chapter 2

Literature study

2.1 Aviation

There are many types, configurations and sizes of aircraft. Two main categories are lighter/heavier than air. Lighter than air aircraft are for example airships and hot air balloons. These creates the lift by having their average density lower than air. Heavier than air aircraft create lift by forcing air downwards. This is made by the shape of the wing called airfoil, see figure 2.1. The airfoil creates a differentiation in pressure between the top and lower side of the wing, that creates lifting force. The shape of the airfoil and the angle of attack is crucial for its function. In rotary-wing aircraft, such as a helicopter, the airfoil often has a fixed shape while in fixed-wing aircraft, such as an airplane, a control surface is often used to change the shape during flight. See figure 2.1. [12]

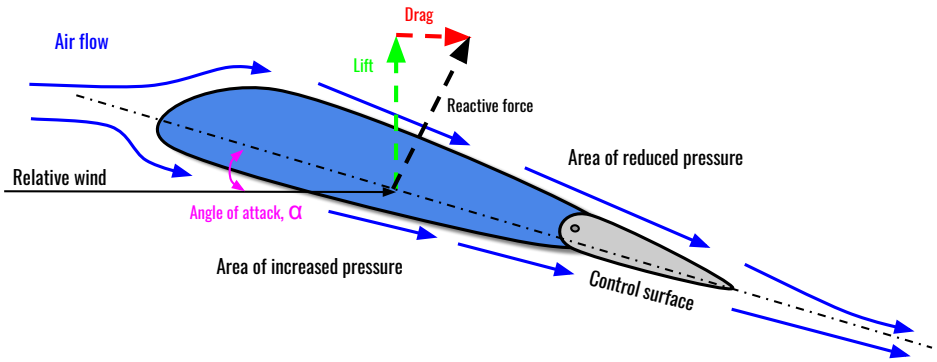


Figure 2.1: An aircraft wing with a control surface. The airfoil shape makes a pressure difference over the wing which creates lift and drag force.

The simulation model used in this thesis simulates four control surfaces, *rudder, elveon, flapperon and aileron.* These are shown in figure 2.2 along with the aircraft

principal axes for aviation; *yaw, pitch and roll*.

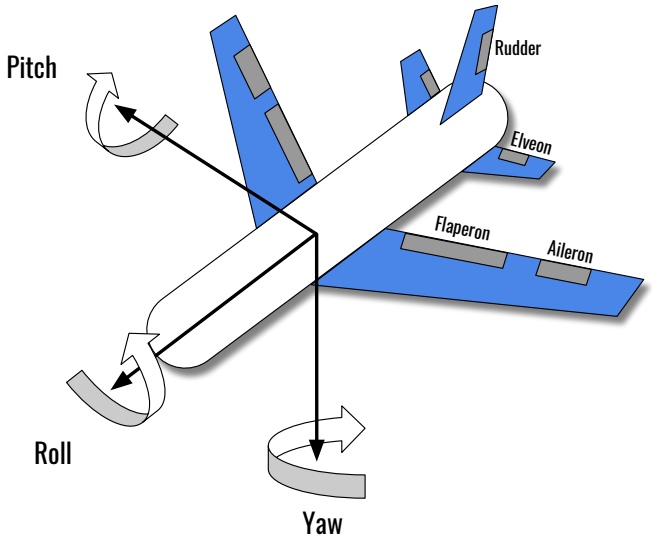


Figure 2.2: Illustration of axis definitions and main control surfaces.

2.2 Flight hydraulics

There are several ways in aviation to control the control surfaces. Hydraulic systems are commonly used. These hydraulic systems can be designed in numerous ways. All systems designs have in common that one single component must not be responsible for the functionality of the system. [5, 20]

In the research project run by LiU, UFSC and SAAB [25] the simplified hydraulic system, shown in figure 2.3, is used as a reference system. This system has two parallel hydraulic subsystems, both working on same tandem cylinder. If one subsystem fails, the bypass valve set it into free floating mode and the other subsystem control the actuator. This system setup is precise, redundant and reliable. [5]

H. Belan et al. (2015) [5] presents table 2.1 of force levels need for different types of flight manoeuvres.

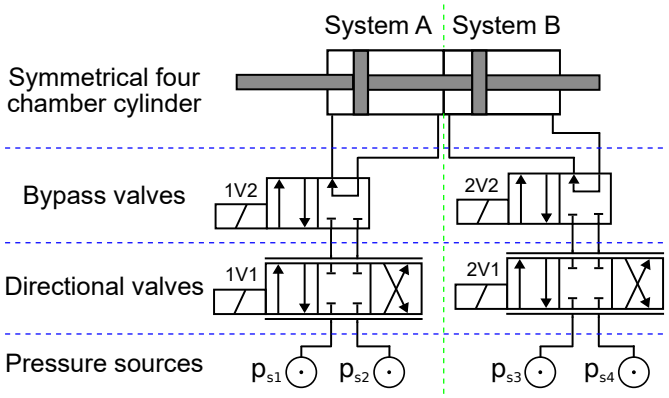


Figure 2.3: Reference system considered in this project.

Table 2.1: Typical force levels compared to the maximum available force [5]. *= Yaw actuators are dimensioned to manage cross-wind landings.

	Action	Takeoff/ landing	Cruise	Dogfight/ turbulent flying
Military aircraft	Pitch	20%	10%	60-100%
	Roll	20%	10%	60-100%
	Yaw	10%	5%	60-100%
Civilian aircraft	Pitch	40%	20%	60-100%
	Roll	40%	20%	60-100%
	Yaw	10%*	10%	60-100%

2.3 Aviation safety regulations

2.3.1 14 CFR 25.671 - General.

The following text is a quote from Code of Federal Regulations Title 14, part 25, section 671. This law regulates control systems for civil aircraft. The safety regulations for civil aircraft are stricter than for military aircraft where ejection seats is available as a last resort.

(a) *Each control and control system must operate with the ease, smoothness, and positiveness appropriate to its function.*

(b) *Each element of each flight control system must be designed, or distinctively and permanently marked, to minimize the probability of incorrect assembly that could result in the malfunctioning of the system.*

(c) *The airplane must be shown by analysis, tests, or both, to be capable of continued safe flight and landing after any of the following failures or jamming in the flight control system and surfaces (including trim, lift, drag, and feel systems), within the normal flight*

envelope, without requiring exceptional piloting skill or strength. ***Probable malfunctions must have only minor effects on control system*** *operation and must be capable of being readily counteracted by the pilot.*

(1) ***Any single failure****, excluding jamming (for example, disconnection or failure of mechanical elements, or structural failure of hydraulic components, such as actuators, control spool housing, and valves).*

(2) ***Any combination of failures not shown to be extremely improbable****, excluding jamming (for example, dual electrical or hydraulic system failures, or any single failure in combination with any probable hydraulic or electrical failure).*

(3) *Any jam in a control position normally encountered during takeoff, climb, cruise, normal turns, descent, and landing unless the jam is shown to be extremely improbable, or can be alleviated. A runaway of a flight control to an adverse position and jam must be accounted for if such runaway and subsequent jamming is not extremely improbable.*

(d) *The airplane must be designed so that it is controllable if all engines fail. Compliance with this requirement may be shown by analysis where that method has been shown to be reliable.*

-14 CFR 25.671 - General [8]

2.4 Fault-tolerant

No system or component is perfect, over time failures will always appear in a system. In a safety-critical system such as an aircraft it is of highest importance that a single fault cannot cause a complete system failure. A system that can achieve this is called a *fault-tolerant* system [7]. Blanke et al. (2006) [7] define some terminology related to the area.

Failure mode *Particular way in which a failure can occur.*

Fault *Unpermitted deviation of at least one characteristic property or parameter of a system from its acceptable/usual/standard condition. A fault is the occurrence of a failure mode.*

Fault accommodation *The action of changing the control law in response to fault, without switching off any system component. In fault accommodation, faulty components are still kept in operation thanks to an adapted control law.*

Fault-operational *The ability to sustain any single point failure.*

Fault-tolerant system *A system where a fault is recovered with or without performance degradation, but a single fault dose not develop into a failure on subsystem or system level*

> ***Passive fault-tolerant*** *A fault-tolerant system where faults are not explicitly detected and accommodated, but the controller is designed to be insensitive to a certain restricted set of faults. Contary to an active fault-tolerat system.*
>
> ***Active fault-tolerant*** *A fault-tolerant system where faults are explicitly detected and accommodated. Opposite of a passive fault-tolerant system.*
>
> Blanke et al. (2006) [7]

Figure 2.4 shows a general design of an active fault-tolerant system presented by Blanke et al. (2006) [7]. In this figure the diagnosis is considered ideal. The diagnosis block result (f) is identical to the fault (f) on the plant. In a real application this is generally not the case due to disturbance (d) on the system. Then the result from the diagnosis block is an estimated fault ($\hat{f}$).

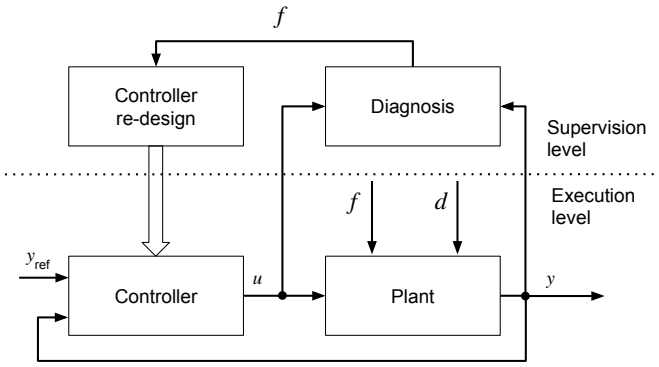


Figure 2.4: General design of an active fault-tolerant system.

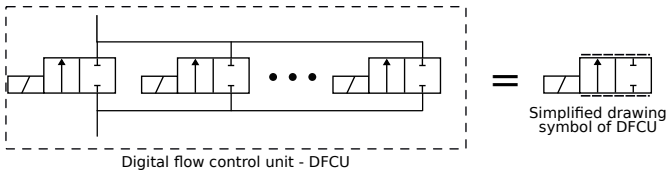
2.5 Digital hydraulics

> *"Digital Fluid Power means hydraulic and pneumatic systems having discrete valued component(s) actively controlling system output."*
>
> - Matti Linjama, 2011 [13]

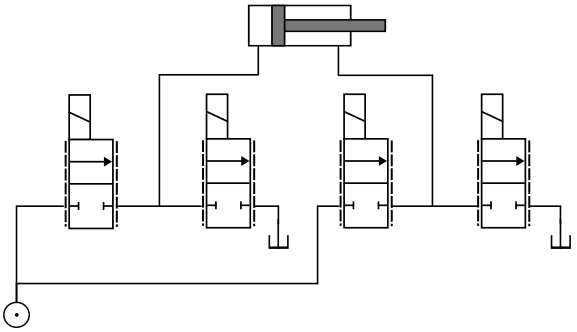
There are a lot of hydraulic system that falls within Matti Linjamas definition of digital fluid power systems. Two systems that have been in focus for a lot of research is Digital Flow Control Unit (DFCU) [11, 13, 14, 22, 23] and Digital Hydraulic Actuator (DHA) [3, 4, 5, 15, 25].

2.5.1 Digital Flow Control Unit - DFCU

In figure 2.5 a DFCU system can be seen along with the common way to draw them. A DFCU has parallel on/off valves that generates a discrete flow output [13]. A DFCU reduce the energy consumption in comparison to a traditional proportional valve, but also demands a complex controller and a lot of computational power [14].



(a) DFCU is commonly drawn with following symbol.



(b) DFCUs connected for control of a cylinder.

Figure 2.5: Digital flow control unit-DFCU is one type of digital hydraulics.

2.5.2 Digital Hydraulic Actuator - DHA

Digital Hydraulic Actuators (DHA) was initially proposed by Linjama et al. (2009) [15]. DHA is also the subject for the research project this thesis is part of [25]. The studied DHA system has three pressure levels, a four-chamber cylinder and twelve on/off valves connecting the chambers to the pressures [5], see figure 3.1.

The DHA system setup replaces the need of a proportional valve. The proportional valves have substantial energy losses due to their throttling. The on/off valves are in comparison with the proportional valves loss free and do not throttle the hydraulic flow at all. [9]

The drawback of this design is the loss of control precision where the proportional valve has endless amount of positions and outputs whereas the on/off valve only has two position and two outputs. By combining positions of the on/off valves different force levels can be achieved. The controller for this system calculated the desired actuator force and configures the valves accordingly. Sometimes DHA is referred to as a digital force control system. [15]

2.5.3 Fault detection and diagnose

In section 1.5 Delimitations, it is stated that fault detection and diagnose are disclosed. The literature study does not include any previous research where this is made on a DHA system. In contrarily research have been made on DFCU systems, without adding extra sensors. Both on-line, during operation [11] and off-line, as a functionality test before start [22]. Therefore, it is reasonable to believe that the same result can be achieved with a DHA system.

2.5.4 Fault accommodation

H. Belan et al. (2015 and 2016) [4, 5] briefly mentions a control strategy for fault accommodation on DHA systems. Just a few sentences, stating that it is plausible without any deeper analytics. L. Siivonen et al. (2009) [23] on the other hand presents a fault accommodation that makes a DFCU system active fault-tolerant.

2.6 HOPSAN

HOPSAN [18] is the simulation tool used in this thesis. HOPSAN is a multi-domain simulating tool that handles fluid power, mechanics and electronics. It uses Transmission Line Modelling (TLM) and has a graphical interface (see figure 2.6) which also can make animations. The tool is developed under an open license at Linköping University. [19]

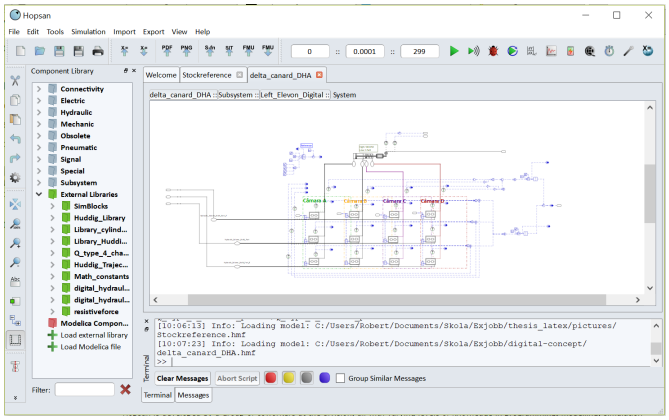


Figure 2.6: HOPSAN GUI, graphical user interface.

2.7 Mathematical notation

For explaining the theoretical parts in this thesis some standard mathematical notation is used. These are explained below.

Set theory

Sets are collections of numbers or objects. In this thesis a set is denoted with a blackboard bold font. $\mathbb{A} = \{1, 2, 3\}$ is the notation for set $\mathbb{A}$ that includes number 1, 2 and 3. In table 2.2, notation and operators are presented.

Table 2.2: Standard set theory notation used in this thesis. [17]

Notation	Name	Meaning	Example
$\{\}$	Set	A collection of elements	$\mathbb{A} = \{1, 2, 3\}$
$\|$	Such that	So that	$\mathbb{A} = \{x \| x \text{ is blue }\}$
$\mathbb{A} \cap \mathbb{B}$	Intersection	Elements that belong to both set $\mathbb{A}$ and set $\mathbb{B}$	$\mathbb{A} = \{1, 2, 3\}$, $\mathbb{B} = \{2, 3, 4\}$, $\mathbb{A} \cap \mathbb{B} = \{2, 3\}$
$\mathbb{A} \subseteq \mathbb{B}$	Subset	All elements in $\mathbb{A}$ are included in $\mathbb{B}$.	$\mathbb{A} = \{1, 2\}$, $\mathbb{B} = \{1, 2, 3\}$, $\mathbb{A} \subseteq \mathbb{B}$
$\mathbb{A}^c$	Complement	All the objects that do not belong to set $\mathbb{A}$	
$\mathbb{A} - \mathbb{B}$	Relative complement	Objects that belong to A and not to B	$\mathbb{A} = \{1, 2, 3\}$, $\mathbb{B} = \{2, 3, 4\}$, $\mathbb{A} - \mathbb{B} = \{1\}$
$x \in \mathbb{A}$	Member of	x is a member of $\mathbb{A}$	$\mathbb{A} = \{1, 2, 3\}$, $2 \in \mathbb{A}$
$\|\mathbb{A}\|$	Cardinality	The number of elements in $\mathbb{A}$	$\mathbb{A} = \{1, 2, 3\}$, $\|\mathbb{A}\| = 3$

Logical operators

For logical reasoning some standard mathematical notation is used. This can be found in table 2.3.

Table 2.3: Standard logical notation used in this thesis. [16]

Notation	Name	Meaning
$A \wedge B$	Logical conjunction	A and B
$A \cdot B$	Logical conjunction	A and B
$A \Rightarrow B$	Implies	If A is true then B is true.
$\neg A$	Negation	Not A
$\forall x = 1$	For all	For all $x = 1$

Boolean algebra

Some laws of boolean algebra used in the thesis [10].

Distributive Law:

$$X(Y + Z) = XY + XZ$$

$$X + YZ = (X + Y)(X + Z)$$

Abortion Law:

$$X + (XY) = X$$

$$X(X + Y) = X$$

Idempotent Law:

$$XX = X$$

$$X + X = X$$

2.8 Fault Tree Analysis

Fault Tree Analysis (FTA) is a common way to evaluate the safety in engineering systems. The method was developed in the early 1960s by H.A Watson. The method is a logical presentation of causes to an undesirable event, the *top event*. By combining logical gates OR, AND, etc. a tree structure is created. [10] In figure 2.7 all symbols used in this thesis are shown.

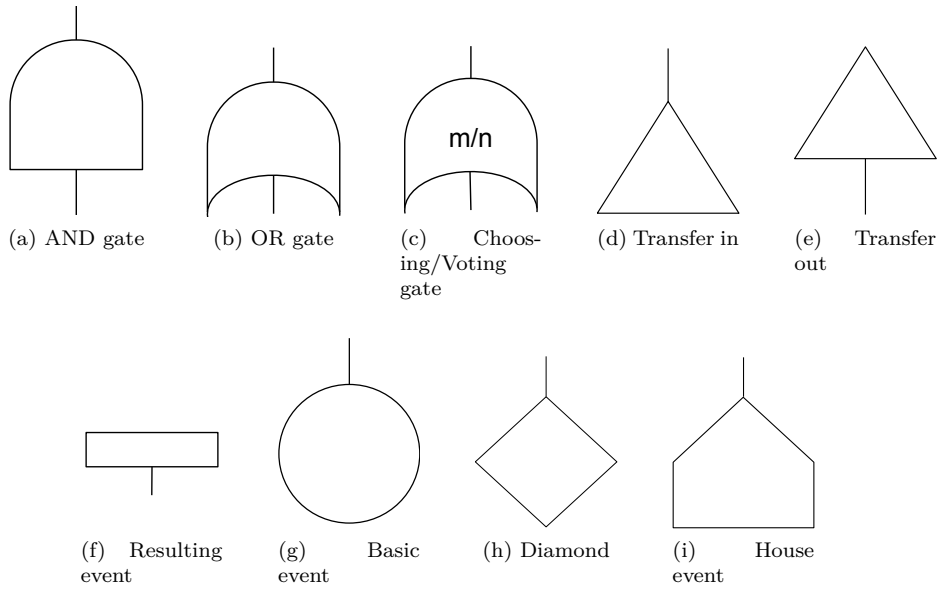


Figure 2.7: Commonly used fault tree symbols.

- AND gate, 2.7a, the output fault event occurs if all connected events occur.
- OR gate, 2.7b, the output fault event occurs if one or more of the connected events occur.
- Choosing/Voting gate, 2.7c, the output fault event occurs if m out of n connected events occur.

- Transfer in, 2.7d, is used to connect sub trees to avoid lengthy or complex trees.
- Transfer out, 2.7e, is used to connect sub trees to avoid lengthy or complex trees.
- Resulting event, 2.7f, a resulting event of combinations of more basic events.
- Basic event, 2.7g, the most basic fault event.
- Diamond, 2.7h, denotes an event that is not fully developed due to lack of information or interest.
- House event, 2.7i, is an expected event, often with probability 1 or 0.

Fault trees can be translated to Boolean expressions. The fault tree in figure 2.8 have the expression 2.1.

$$\begin{aligned} E1 &= A \cdot B \\ E2 &= A \cdot C \\ E3 &= C \cdot D \\ E4 &= E1 + E2 + E3 \end{aligned} \tag{2.1}$$

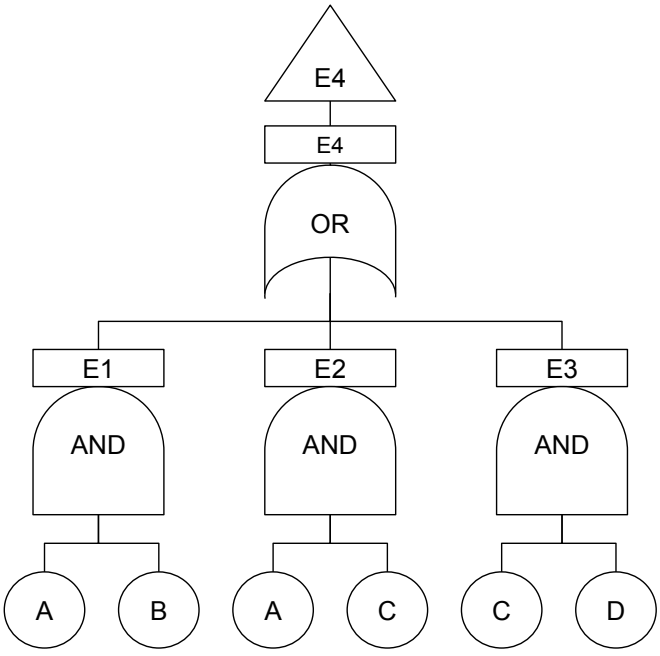


Figure 2.8: An example of a fault tree.

Sometimes it is possible to reduce the fault tree using Boolean algebra. This is only possible if the probabilities of the fault events have similar values. A fully reduced fault tree is called a minimal cut set. [10]

Example: The fault tree in figure 2.9 can be reduced according to expression 2.2 using the abortion law.

$$E2 = A \cdot B + A = A \tag{2.2}$$

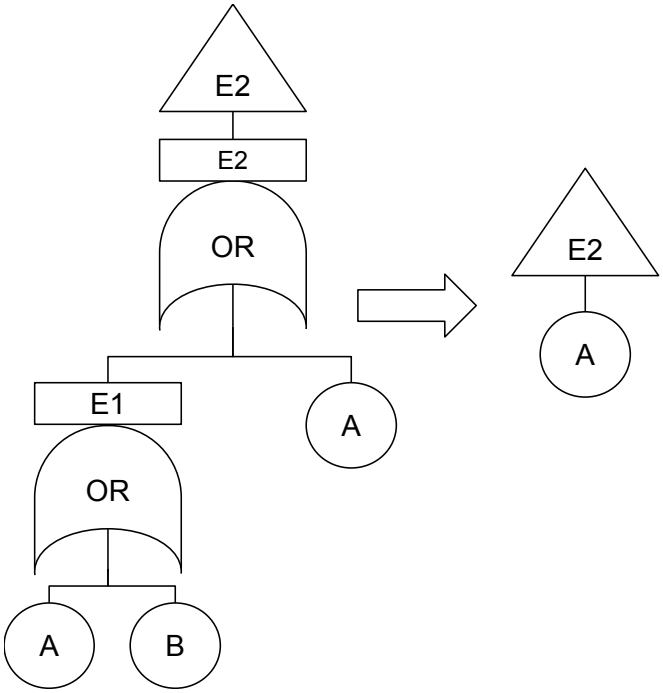


Figure 2.9: The fault tree to the left can be reduced to the fault tree to the right.

2.8.1 Calculate probabilities

To correctly calculate the probability of the top event a minimal cut set is needed. The probability of an OR gate is calculated with equation 2.3. For small probabilities, $P(X_i) < 0.1$, it can be approximated to the sum of the individual probabilities, see equation 2.4. [10]

$$P(X_0) = 1 - \prod_{i=1}^{m} \{1 - P(X_i)\} \tag{2.3}$$

$$P(X_0) \approx \sum_{i=1}^{m} P(X_i) \tag{2.4}$$

AND gates are calculated as the product of the individual probabilities, equation 2.5 [10].

$$P(X_0) = \prod_{i=1}^{k} P(X_i) \tag{2.5}$$

2.9 Probability

There are numerous ways of calculating probabilities for individual components. One of the easiest probabilities that are widely used is exponential distribution. An exponential distribution assumes a constant failure rate during the components life time. The probability is calculated with equation 2.6 where λ is the constant failure rate and t is the time for the calculation. [10]

$$P(t) = 1 - e^{-\lambda t} \tag{2.6}$$

Chapter 3

Theoretical studies

3.1 System setup

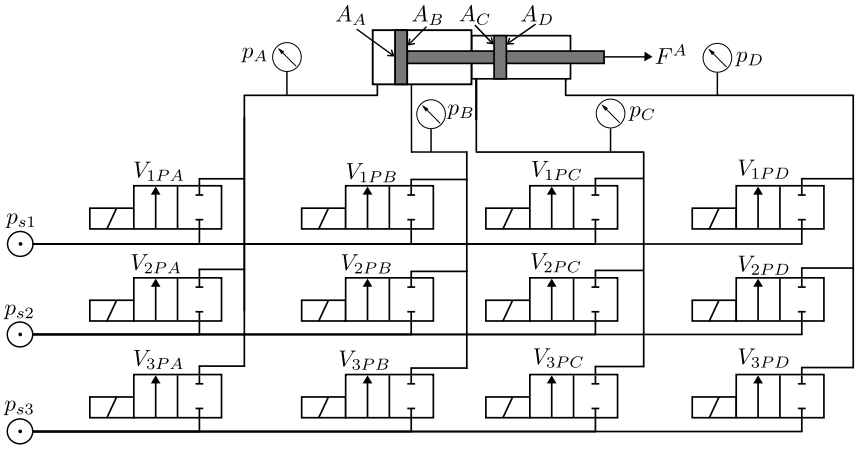


Figure 3.1: System setup for the digital actuation system.

The system considered in this research project run by SAAB, USCF and LiU [25], and its notation, is shown in figure 3.1. The system has three pressure sources ($p_{sx}, x \in \mathbb{P}_{index}$), a cylinder with four chamber areas ($A_y, y \in \mathbb{A}_{index}$) and 12 on/off valves ($\mathbb{V}$) that connects all pressure sources to all chambers.

Definitions are made in equation 3.1-3.3. The notation V_{xPy} is used for the valve connecting pressure source p_{sx} to chamber area A_y. The function $\gamma(V_{xPy})$ gives the current valve position, open or close, see equation 3.4. The total force from the cylinder (F^A) is calculated with equation 3.5. [3]

$$\mathbb{P}_{index} = \{1, 2, 3\} \tag{3.1}$$

$$\mathbb{A}_{index} = \{A, B, C, D\} \tag{3.2}$$

$$\mathbb{V} = \{V_{xPy} | x \in \mathbb{P}_{index} \wedge y \in \mathbb{A}_{index}\} \tag{3.3}$$

$$\begin{cases} \gamma(V_{xPy}) = 0, & V_{xPy} \text{ is closed} \\ \gamma(V_{xPy}) = 1, & V_{xPy} \text{ is open} \end{cases} \tag{3.4}$$

$$F^A = A_A p_A - A_B p_B + A_C p_C - A_D p_D \tag{3.5}$$

3.1.1 Short circuit

The pressure in every chamber ($p_y, y \in \mathbb{A}_{index}$) is given by equation 3.6. This is under the assumption that the pressure drop over on/off valves is negligible. [15] At a given time only one valve can be open to the same chamber. This is to prevent what is refereed to as a *short circuit*. A short circuit means an uncontrolled hydraulic flow between two pressure sources where there are no restrictions limiting the flow. A short circuit leads to substantial energy loss and is therefore avoided. Equation 3.7 mathematically describe the relationship. [3]

$$p_y \approx \begin{cases} p_{s1}, & \text{if } \boldsymbol{\gamma(V_{1Py}) = 1} \text{ and } \gamma(V_{2Py}) = 0 \text{ and } \gamma(V_{3Py}) = 0 \\ p_{s2}, & \text{if } \gamma(V_{1Py}) = 0 \text{ and } \boldsymbol{\gamma(V_{2Py}) = 1} \text{ and } \gamma(V_{3Py}) = 0 \\ p_{s3}, & \text{if } \gamma(V_{1Py}) = 0 \text{ and } \gamma(V_{2Py}) = 0 \text{ and } \boldsymbol{\gamma(V_{3Py}) = 1} \end{cases} \tag{3.6}$$

$$\text{if } j, k \in \mathbb{A}_{index} \wedge x \in \mathbb{P}_{index}, \text{ then } \gamma(V_{xPj}) \implies \neg\gamma(V_{xPk}) \forall j \neq k \tag{3.7}$$

3.1.2 Forces

By combining valve positions different forces can be achieved. For analyse of failures a notation for unique forces is added. A unique force is named F^A_{abcd} ($a, b, c, d \in \mathbb{P}_{index}$) where *abcd* refers to the pressure in each chamber for the given forces, see equation 3.8. A notation $\mu(V_{xPy}, F^A_{abcd})$ is added to define the relationship between a specific force and a specific valve, see equation 3.9.

$$F^A_{abcd} = A_A p_{sa} - A_B p_{sb} + A_C p_{sc} - A_D p_{sd} \tag{3.8}$$

$$\mu(V_{xPy}, F^A_{abcd}) = 1 \text{ if } \begin{cases} \gamma(V_{aPA}) = 1 \\ \gamma(V_{bPB}) = 1 \\ \gamma(V_{cPC}) = 1 \\ \gamma(V_{dPD}) = 1 \end{cases} \quad \text{else } \mu(V_{xPy}, F^A_{abcd}) = 0 \tag{3.9}$$

The set $\mathbb{F}_{normal}$, equation 3.10, is a set with all possible forces for the system in normal function.

$$\mathbb{F}_{normal} = \{F_{abcd} | a, b, c, d \in \mathbb{P}_{index}\} \tag{3.10}$$

Every chamber can have three different pressures and there are four different chambers. This gives $3^4 = 81$ number of forces in the system in normal condition

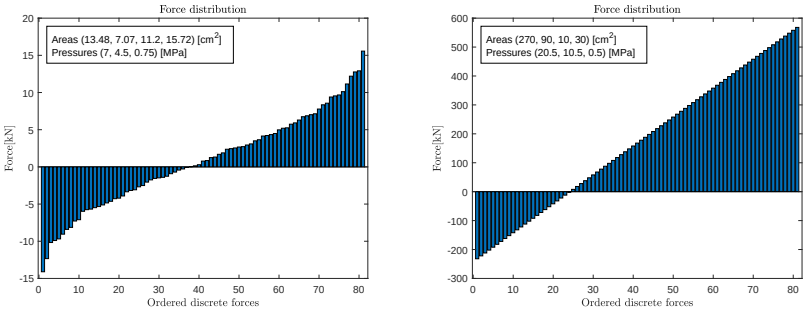
[9]. This can be described more generally with equation 3.11. This equation is essentially the same equation presented by H. Belan el at. (2015) [5] for calculating the number of discrete forces. However, equation 3.11 uses the set notation applied in this thesis.

$$|\mathbb{F}_{normal}| = |\mathbb{P}_{index}|^{|\mathbb{A}_{index}|} \tag{3.11}$$

The combinations of areas and pressures affect the set of discrete forces in the system. In table 3.1 an abstract of the forces for the test rig at LASHIP [3] can be seen. The full force distribution is presented in figure 3.2a. Figure 3.2b is a different area-pressure combination presented by H. Belan et al. (2015) [5]. The area-pressure combination has a relative area relation of 27:9:1:3 and equally spaced pressures. This gives an evenly distributed force spectra, with same distance between every force.

Table 3.1: An abstract from the force table for a the test rig at LASHIP with pressures = [7, 4.5, 0.75]MPa and areas = [13.48, 7.07, 11.2, 15.72]cm^2

abcd	F^A_{abcd} $[N]$	$\mu(V_{1PA}, F^A_{abcd})$	$\mu(V_{2PA}, F^A_{abcd})$	$\mu(V_{3PA}, F^A_{abcd})$	$\mu(V_{1PB}, F^A_{abcd})$	$\mu(V_{2PB}, F^A_{abcd})$	$\mu(V_{3PB}, F^A_{abcd})$	$\mu(V_{1PC,}, F^A_{abcd})$	$\mu(V_{2PC,}, F^A_{abcd})$	$\mu(V_{3PC,}, F^A_{abcd})$	$\mu(V_{1PD}, F^A_{abcd})$	$\mu(V_{2PD}, F^A_{abcd})$	$\mu(V_{3PD}, F^A_{abcd})$
3131	-14102	0	0	1	1	0	0	0	0	1	1	0	0
3231	-12335	0	0	1	0	1	0	0	0	1	1	0	0
3132	-10172	0	0	1	1	0	0	0	0	1	0	1	0
3121	-9902	0	0	1	1	0	0	0	1	0	1	0	0
3331	-9683	0	0	1	0	0	1	0	0	1	1	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1213	12916	1	0	0	0	1	0	1	0	0	0	0	1
1313	15567	1	0	0	0	0	1	1	0	0	0	0	1



(a) Test rig LASHIP (b) Evenly spread forces

Figure 3.2: Depending on the combination of areas and pressures the force distribution changes. Every force represents a unique combination of valve positions.

3.2 Failures

3.2.1 Fault accommodation, previous studies

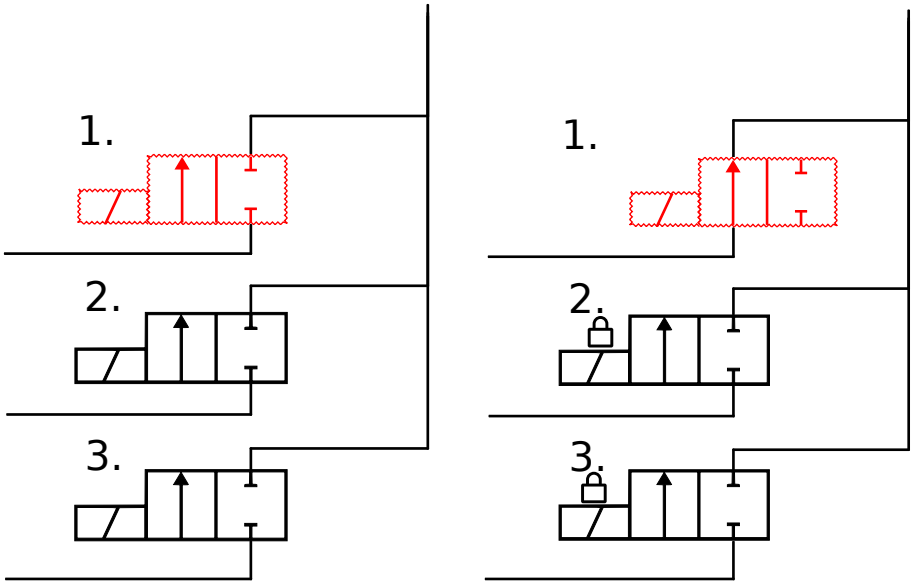
H. Belan et al. (2015 and 2016) [4, 5] briefly mentions a control strategy for fault accommodation on DHA systems. The approach is to use fault diagnostics to identify failures then re-design the controller to only use discrete forces with the valves in the failing positions. For an single open failure the controller only uses forces where this valve is open. This narrows the original 81 discrete forces down to 27 [5]. The same applies for closed failures. For a single closed failure the controller only uses forces where this valve is closed. This gives 54 discrete forces [5]. The purpose of this fault accommodation is to prevent short circuits in the system.

Furthermore, in case of a pressure line failure the pressure in the pressure line is unknown. The controller can therefore not predict the force output. The fault accommodation to this fault, suggested by H. Belan et al. (2015) [5], is therefore to close all valves connected to this line. This leads to 16 remaining discrete forces in the system [5].

With these fault accommodations the system can continue its work with a reduced amount of force levels. In figure 3.3a, 3.3b and 3.4 visualisations of the fault accommodations are presented.

3.2.2 Fault accommodation, general description

The fault accommodations earlier presented for DHA system handle only single valve failures. To have a more general description this thesis adds some notation. $\mathbb{P}_y$ ($y \in \mathbb{A}_{index}$) is the set of pressures currently available in chamber y. In normal



(a) Zigzag indicates a closed failure at valve 1, valve 2 and 3 can still work as normal, creating two available pressures for the chamber.

(b) Zigzag indicates an open failure at valve 1, valve 2 and 3 are locked in closed position, preventing short circuit, creating one available pressure level for the chamber.

Figure 3.3: The two failure states that can appear after single valve failure.

condition equation 3.12 applies.

$$\begin{aligned} \mathbb{P}_{A,normal} &= \{p_{s1}, p_{s2}, p_{s3}\} \\ \mathbb{P}_{B,normal} &= \{p_{s1}, p_{s2}, p_{s3}\} \\ \mathbb{P}_{C,normal} &= \{p_{s1}, p_{s2}, p_{s3}\} \\ \mathbb{P}_{D,normal} &= \{p_{s1}, p_{s2}, p_{s3}\} \end{aligned} \tag{3.12}$$

Equation 3.5 is extended with this definition in equation 3.13.

$$F^A = A_A p_A - A_B p_B + A_C p_C - A_D p_D \quad p_A \in \mathbb{P}_A, p_B \in \mathbb{P}_B, p_C \in \mathbb{P}_C, p_D \in \mathbb{P}_D \tag{3.13}$$

The total amount of forces can be calculated with equation 3.14. This equation gives the same results as previously presented equations for systems in normal condition [5] but also handles failures.

$$|\mathbb{F}| = |\mathbb{P}_A| \cdot |\mathbb{P}_B| \cdot |\mathbb{P}_C| \cdot |\mathbb{P}_D| \tag{3.14}$$

Closed failure

The fault accommodation for a closed failure on valve V_{xPy} is described with equation 3.15 where $\mathbb{P}_{y,i}$ indicates the pressures set before the failure and $\mathbb{P}_{y,i+1}$ indicates after the fault accommodation.

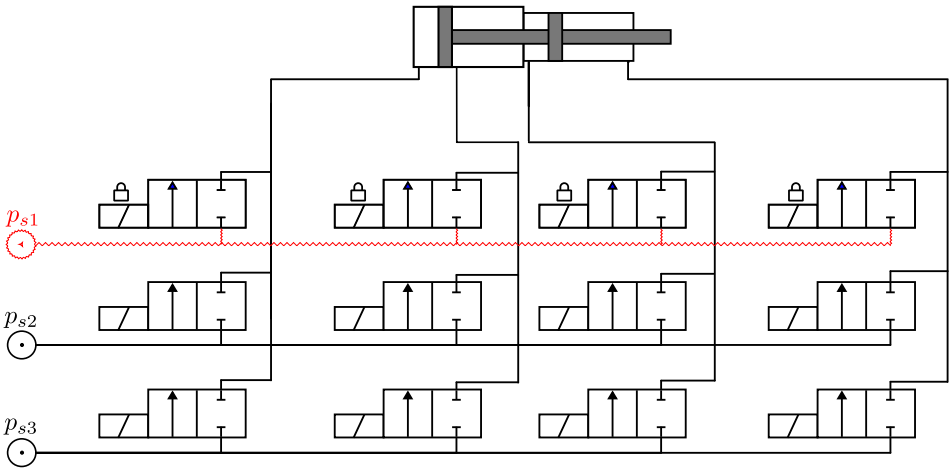


Figure 3.4: Zigzag line indicates a pressure line failure, all valves connected to the pressure line are locked to closed position to prevent failing pressures in the system.

$$\mathbb{P}_{y,i+1} = \mathbb{P}_{y,i} - \{p_{sx}\} \tag{3.15}$$

Example: If chamber A is in normal condition ($\mathbb{P}_{A,normal} = \{p_{s1}, p_{s2}, p_{s3}\}$) and a **closed failure** appears at valve V_{1PA}, $\mathbb{P}_A = \{p_{s1}, p_{s2}, p_{s3}\} - \{p_{s1}\} = \{p_{s2}, p_{s3}\}$.

Open failure

The fault accommodation for an open failure on valve V_{xPy} is described with equation 3.16. The notation $\{p_{sx}\}^c$ means complement, so the equation removes all pressures except p_{sx}.

$$\mathbb{P}_{y,i+1} = \mathbb{P}_{y,i} - \{p_{sx}\}^c \tag{3.16}$$

Example: If chamber A is in normal condition ($\mathbb{P}_{A,normal} = \{p_{s1}, p_{s2}, p_{s3}\}$) and an **open failure** appears at valve V_{1PA}, $\mathbb{P}_A = \{p_{s1}, p_{s2}, p_{s3}\} - \{p_{s1}\}^c = \{p_{s1}\}$.

Pressure line failure

The fault accommodation for a pressure line failure on pressure line p_{sx} is described with equation 3.17. This is identical to four closed failures on valves $V_{xPA}, V_{xPB}, V_{xPC}$ and V_{xPD}.

$$\begin{aligned}\mathbb{P}_{A,i+1} &= \mathbb{P}_{A,i} - \{p_{sx}\} \\ \mathbb{P}_{B,i+1} &= \mathbb{P}_{B,i} - \{p_{sx}\} \\ \mathbb{P}_{C,i+1} &= \mathbb{P}_{C,i} - \{p_{sx}\} \\ \mathbb{P}_{D,i+1} &= \mathbb{P}_{D,i} - \{p_{sx}\}\end{aligned} \tag{3.17}$$

3.2.3 Chamber combinatorics

This thesis considers three working modes for every valve; *Normal(N), closed failure(C), open failure(O)*. In a chamber there are three valves, this leads to $3^3 = 27$ combinations of valve working modes in every chamber. In table 3.2 all 27 failures are presented and ordered accordingly to $\mathbb{P}_y$. Every unique set of $\mathbb{P}_y$ is called a *chamber state*. The naming convention for chamber states is presented in table 3.2. Chamber states are named after the single valve failure creating this set of pressures.

If pressure line failures also are considered there would be even more combinations ($3^3 \cdot 2^3 = 216$), but since the failure accommodation for a pressure line failure is to close connected valves, a "C" in table 3.2 can be considered as closed failure and/or pressure line failure to reduce the amount of combinations.

Table 3.2: Chamber states for chamber y, with notation; N=normal condition, C=closed failure and/or pressure line failure, O=open failure. **Example:** OCN means that valve 1 has open failure, valve 2 has closed and/or pressure line failure, valve 3 is in normal condition.

State	$\mathbb{P}_y$	Combinations of working modes
N	$\{p_{s1}, p_{s2}, p_{s3}\}$	NNN
C_1	$\{p_{s2}, p_{s3}\}$	CNN
C_2	$\{p_{s1}, p_{s3}\}$	NCN
C_3	$\{p_{s1}, p_{s2}\}$	NNC
O_1	$\{p_{s1}\}$	ONN, OCN, ONC, NCC, OCC
O_2	$\{p_{s2}\}$	NON, CON, NOC, CNC, COC
O_3	$\{p_{s3}\}$	NNO, CNO, NCO, CCN, CCO
$\emptyset$	$\{\}$	OON, ONO, NOO, OOC, OCO, COO, OOO, CCC

$\mathbb{S}$ is defined as the set of working states that the system can work with. $\emptyset$ is not included since the system cannot work without defined pressures in one chamber.

$$\mathbb{S} = \{N, C_1, C_2, C_3, O_1, O_2, O_3\} \tag{3.18}$$

3.2.4 System combinatorics

In this thesis three working modes are considered for all 12 valves and two working modes for the three pressure lines (working/not working). This gives a total of $3^{12} \cdot 2^3 = 4\,251\,528$ failure combinations. Many of these combinations leads to

the same chamber states and thereby the same force distributions. Therefore, the combinations of chamber states are more interesting to investigate. To calculate the number of unique force distributions equation 3.19 is used.

$$n_{dist} = |\mathbb{S}|^{|\mathbb{A}_{index}|} + 1 \tag{3.19}$$

In equation 3.19, $|\mathbb{S}|$ is the number of working states in the system. $|\mathbb{A}_{index}|$ is the number of chambers in the system. $+1$ is to add the case where one or more chambers have the chamber state $\emptyset$. For the system considered in this thesis $n_{dist} = 7^4 + 1 = 2402$, considerably smaller than 4 251 528.

3.2.5 Failure, a subset of forces

A force distribution is denoted as $\mathbb{F}_{S_A S_B S_C S_D}$ where $S_A S_B S_C S_D$ denotes the chamber states. S_y is the state in chamber y. The force distribution for the normal condition $\mathbb{F}_{normal} = \mathbb{F}_{NNNN}$. If one or more chambers are in state $\emptyset$ there are no forces in the system at all, according to equation 3.14. This is denoted with only one index $\mathbb{F}_\emptyset$ since the other chambers' states are irrelevant.

Example: $\mathbb{F}_{O_1NNN}$ is the set of forces where chamber A is in state O_1 and chamber B, C and D is in normal state. This force distribution includes the forces in $\mathbb{F}_{normal}$ that have V_{1PA} open according to the failure accommodation. This also means that $\mathbb{F}_{O_1NNN}$ is a subset of $\mathbb{F}_{normal}$, $\mathbb{F}_{O_1NNN} \subseteq \mathbb{F}_{normal}$. This is valid for all force distributions, see equation 3.20

$$\mathbb{F}_{S_A S_B S_C S_D} \subseteq \mathbb{F}_{normal}, \quad S_A, S_B, S_C, S_D \in \mathbb{S} \tag{3.20}$$

A combination of chamber states results in a intersection of the force distributions.

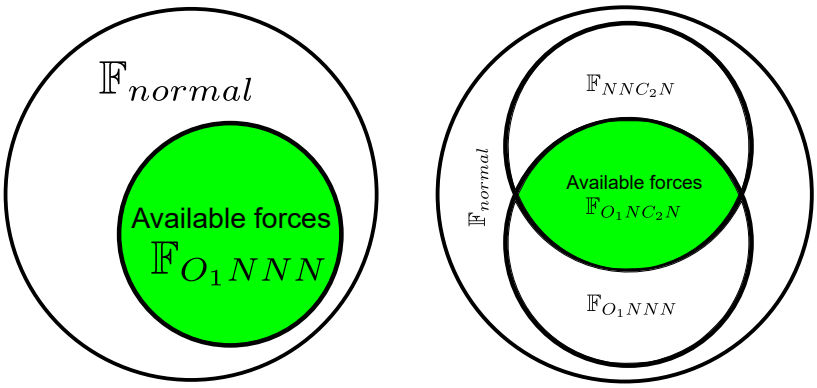
Example: State O_1 on chamber A in combination with state C_2 on chamber C, (B and D in state N), gives:

$$\mathbb{F}_{O_1NC_2N} = \mathbb{F}_{O_1NNN} \cap \mathbb{F}_{NNC_2N}$$

Generally this can be described with equation 3.21.

$$\mathbb{F}_{S_A S_B S_C S_D} = \mathbb{F}_A \cap \mathbb{F}_B \cap \mathbb{F}_C \cap \mathbb{F}_D$$
$$\text{where } \mathbb{F}_y = \begin{cases} \mathbb{F}_{normal} & \text{if } S_y = N \\ \{F^A_{abcd} | \mu(V_{xPy}, F^A_{abcd}) = 1\} & \text{if } S_y = O_x \\ \{F^A_{abcd} | \mu(V_{xPy}, F^A_{abcd}) = 0\} & \text{if } S_y = C_x \end{cases} \quad y \in \mathbb{A}_{index} \tag{3.21}$$

Figure 3.5 visualises the set theories and figure 3.6 shows an example of two failures combined into a combined force distribution. The area-pressure combination used is from LASHIP test rig [3].



(a) Every failure case is a subset of the total force distribution.

(b) A combination of failures results in an intersection between individual failure subsets.

Figure 3.5: The force distribution in case of a failure can be described with subsets.

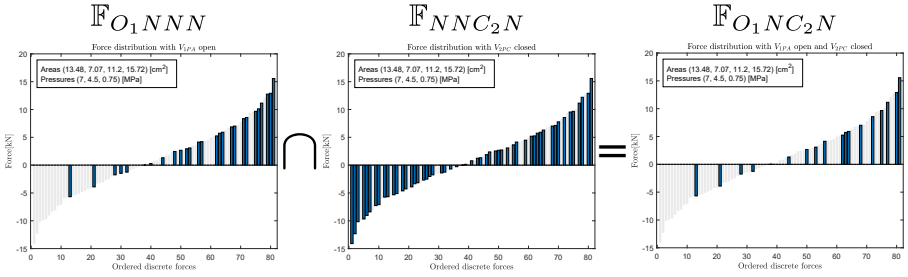


Figure 3.6: The force distribution $\mathbb{F}_{O_1NNN}$, caused by an open failure on V_{1PA} and the force distribution $\mathbb{F}_{NNC_2N}$, caused by a closed failure on V_{2PC} are combined into the force distribution $\mathbb{F}_{O_1NC_2N}$. The grey bars represent the forces in normal condition, $\mathbb{F}_{normal}$, not included in the subsets.

3.3 Percentage of force

There are many statistical properties of a force distribution. For the traditional system a common way is to talk about percentage of force in the system. This is intuitive since the system is symmetrical regarding positive and negative force. For digital hydraulics this is not the case and therefore κ is defined as the rate of force compared to the forces in normal condition ($\mathbb{F}_{normal}$). κ is defined as with equation 3.22-3.24. An example is shown in figure 3.7

$$\kappa_{pos} = \begin{cases} \frac{\max \mathbb{F}}{\max \mathbb{F}_{normal}} & \text{if } \max \mathbb{F} > 0 \\ 0 & \text{otherwise} \end{cases} \tag{3.22}$$

$$\kappa_{neg} = \begin{cases} \frac{\min \mathbb{F}}{\min \mathbb{F}_{normal}} & \text{if } \min \mathbb{F} < 0 \\ 0 & \text{otherwise} \end{cases} \tag{3.23}$$

$$\kappa_{min} = \min(\kappa_{pos}, \kappa_{neg}) \tag{3.24}$$

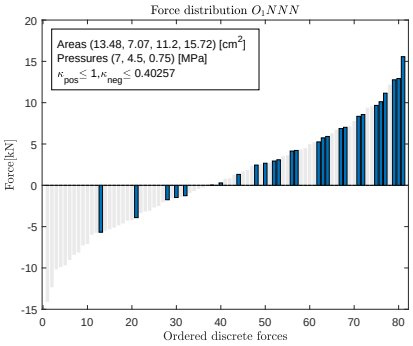


Figure 3.7: This system has $\kappa_{pos} = 1$ and $\kappa_{min} = \kappa_{neg} = 0.40257$. Therefore, the system is said to have $\sim$40% of force.

3.4 Max/min force

κ_{min} is directly dependent on the maximum and minimum force in the system. In this section a derivation of the max/min force is presented along with how failures affect it.

In order to maximize the output force (F^A_{abcd}) the pressures that give a positive contribution should be maximized ($\mathbb{P}_A$ and $\mathbb{P}_C$) and the pressures with negative contribution ($\mathbb{P}_B$ and $\mathbb{P}_D$) should be minimized. In order to minimizing the output force, the situation is the opposite and the positive contribution should be the minimized whereas the negative contribution should be maximized. Areas are constant and does not change during operation. Equation 3.25 and 3.26 defines the maximum and minimum forces of a force set.

$$\max \mathbb{F} = A_A \max \mathbb{P}_A - A_B \min \mathbb{P}_B + A_C \max \mathbb{P}_C - A_D \min \mathbb{P}_D \tag{3.25}$$

$$\min \mathbb{F} = A_A \min \mathbb{P}_A - A_B \max \mathbb{P}_B + A_C \min \mathbb{P}_C - A_D \max \mathbb{P}_D \tag{3.26}$$

By subtracting the minimum from the maximum the system range is defined, equation 3.27.

$$\begin{aligned} F^A_{range} = \max \mathbb{F} - \min \mathbb{F} = A_A(\max \mathbb{P}_A - \min \mathbb{P}_A) + A_B(\max \mathbb{P}_B - \min \mathbb{P}_B) \\ + A_C(\max \mathbb{P}_C - \min \mathbb{P}_C) + A_D(\max \mathbb{P}_D - \min \mathbb{P}_D) \end{aligned} \tag{3.27}$$

Every chamber therefore have a contribution of $A_y(\max \mathbb{P}_y - \min \mathbb{P}_y)$ to the range.

In normal condition ($\mathbb{F}_{normal}$) all chambers have the same pressures $\mathbb{P}_{y,normal} = \{p_{s1}, p_{s2}, p_{s3}\}$. Which gives $F^A_{range,normal}$, equation 3.28.

$$F^A_{range,normal} = (A_A + A_B + A_C + A_D)(\max \mathbb{P}_{y,normal} - \min \mathbb{P}_{y,normal}) \quad (3.28)$$

3.4.1 Range loss

Range loss is defined as ΔF^A_{range}, equation 3.29.

$$\Delta F^A_{range} = F^A_{range,normal} - F^A_{range} \quad (3.29)$$

If there is a **single closed** failure on a chamber there are two available pressures, $|\mathbb{P}_{y,closed}| = 2$. If the pressures are not equal to each other, $p_{s1} \neq p_{s2} \neq p_{s3}$, equation 3.30 applies.

$$\max \mathbb{P}_{y,closed} - \min \mathbb{P}_{y,closed} > 0 \quad (3.30)$$

In case of a **single open** failure on a chamber there are only one pressure available, $|\mathbb{P}_{y,open}| = 1$. This gives equation 3.31.

$$\max \mathbb{P}_{y,open} - \min \mathbb{P}_{y,open} = 0 \quad (3.31)$$

By comparing equation 3.30 and 3.31 the conclusion is made that open failures gives larger range losses. The range loss for an open failure is found in equation 3.32.

$$\begin{aligned} \Delta F^A_{range,open} = F^A_{range,normal} - F^A_{range,open} = \\ A_y(\max \mathbb{P}_{y,normal} - \min \mathbb{P}_{y,normal}) \end{aligned} \quad (3.32)$$

In equation 3.33 this loss is compared to $F^A_{range,normal}$.

$$\begin{aligned} \frac{\Delta F^A_{range,open}}{F^A_{range,normal}} = \\ \frac{A_y(\max \mathbb{P}_{y,normal} - \min \mathbb{P}_{y,normal})}{(A_A + A_B + A_C + A_D)(\max \mathbb{P}_{y,normal} - \min \mathbb{P}_{y,normal})} = \\ \frac{A_y}{A_A + A_B + A_C + A_D} \end{aligned} \quad (3.33)$$

Equation 3.33 shows that the range loss for an open failure is directly proportional to the size of the chamber area.

Example: If area A_y is 40% of the total chamber area $(A_A + A_B + A_C + A_D)$ the range loss will be 40% of the total range in case of an open failure.

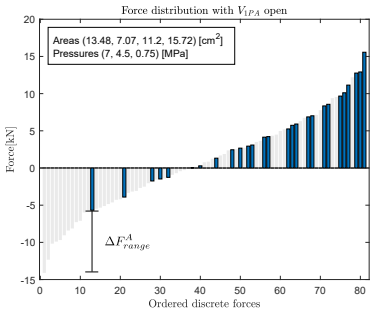
3.4.2 Position of force loss

Depending on which valves that are failing the loss of force comes from either the positive, negative or both sides of the force spectra. Under the assumption that the pressures are ordered $p_{s1} > p_{s2} > p_{s3}$ the following applies.

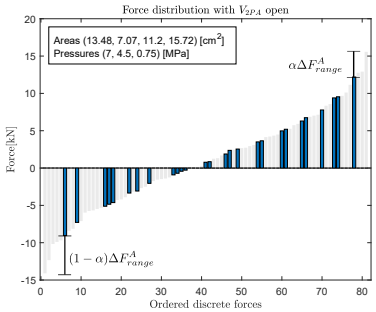
For valves used open for the system maximum force ($\max \mathbb{F}_{normal}$) the range loss for an open failure is only form the negative side, since the maximum force is still available. $\max \mathbb{F}_{normal} = F^A_{1313} \Rightarrow \{V_{1PA}, V_{3PB}, V_{1PC}, V_{3PD}, \}$.

The opposite appear for the valves used open for the minimum force. $\min \mathbb{F}_{normal} = F^A_{3131} \Rightarrow \{V_{3PA}, V_{1PB}, V_{3PC}, V_{1PD}\}$. If they have an open failure the range loss is exclusively from the positive side.

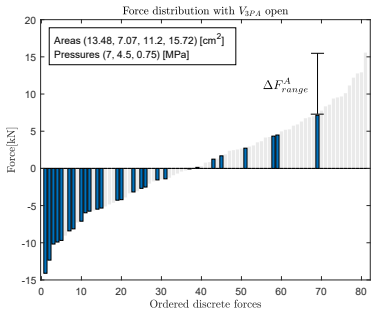
If one of the middle valves, V_{2Py}, have an open failure both the maximum and minimum force is reduced. But in all cases the total amount of range loss is the same within the chamber as shown in equation 3.33. Figure 3.8 shows all open failure cases for chamber A on the test rig at LASHIP [3].



(a) Open failure V_{1PA}



(b) Open failure V_{2PA}, where α is a constant.



(c) Open failure V_{3PA}

Figure 3.8: The force range is equal for all three cases.

3.4.3 Most critical failure

Since the range loss is directly proportional to the chamber area (equation 3.33) the biggest range loss will appear at the biggest area. The biggest area on a four-chamber cylinder will always be 25% or more of the total area. This means that the biggest range loss, for single failures, always will be 25% or more of the total range.

This loss can appear from positive, negative or both sides of the force spectra depending on failing valve, see section 3.4.2. If this is translated into κ-values, an open failure, on the biggest chamber on the smallest side gives the smallest κ_{min}.

Symmetrical system

To spread the influence from every chamber a symmetrical system can be used, see figure 3.9. On a symmetrical cylinder the areas are 25% each and the sides are 50% each. Thereby the smallest $\kappa_{min} = 0.5$ for a single failure, see equation 3.34 where all values are relative to $F^A_{range,normal}$.

$$\kappa_{min,symetrical} = \frac{\max \mathbb{F}_{normal} - \Delta F^A_{range,open}}{\mathbb{F}_{normal}} = \frac{0.5 - 0.25}{0.5} = 0.5 \tag{3.34}$$

Many of the discrete forces in a symmetrical system have the same values. These systems are harder to control in normal condition since there are less unique values to choose from.

Example: The wanted force is 4kN. The six closest forces for the symmetrical system are [3, 3, 3, 4.5, 4.5, 4.5]kN. The controller will then choose on of the combinations giving 4.5kN, which is 0.5kN form the wanted force. For another evenly spread system the six closest forces are [3.3, 3.6, 3.9, 4.2, 4.5, 4.8]kN. Here the controller chooses 3.9kN which is 0.1kN from the wanted force. A smaller difference and thereby a better control.

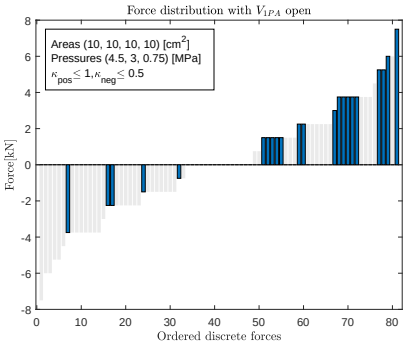


Figure 3.9: Force distribution of a symmetrical system with an open failure on V_{1PA}, the most critical failure.

Unsymmetrical system

If the cylinder is unsymmetrical the biggest area is greater than 25% and the smaller side is smaller than 50%. This leads to a conclusion that the most critical single failure has $\kappa_{min} \leq 0.5$ for all area-pressure combinations. In the reference system the most critical single failure has $\kappa_{min} = 0.5$.

Example: An extrem case of this is an open failure on valve V_{1PA} on the evenly spread system presented by H. Belan et al. (2015) [5]. In this system A_A is 67.5% of the total area and thereby the system will have a 67.5% loss of the force range in case of an open failure on chamber A, according to equation 3.33. This is seen in figure 3.10. A force distribution like this will cause a failing system since it only can extract the cylinder and not retract it.

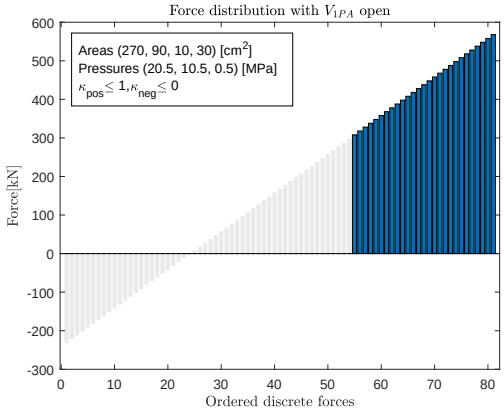


Figure 3.10: An even force distribution with an open failure on valve V_{1PA}.

A trade-of between reliability and controllability is found here. The evenly spread force distribution have the best controllability over the whole force spectra but is not fault tolerant. The symmetrical system have a high fault tolerance but a poor controllability. A good compromise can be a *semi-symmetrical* cylinder as the test rig at LASHIP [3] or the one used by S. Ward [26].

3.4.4 Dual failures

Chambers work independently, therefore a double open failure results in equation 3.35.

$$\Delta F^A_{range} = \frac{A_{y1} + A_{y2}}{A_A + A_B + A_C + A_D}(p_{s1} - p_{s3}) \tag{3.35}$$

On an unsymmetrical cylinder the combined area of the two biggest chambers will be greater than 50%. This means that the combination of two open failures on the two biggest chambers on the smaller side of the force spectra will always result in $\kappa_{min} = 0$. This is the same as for the reference system where double failure also results in $\kappa_{min} = 0$. $\kappa_{min} = 0$ means that either the positive or the

negative force is zero, the cylinder cannot extract or it cannot retract. Therefore, it is an uncontrollable system.

Chapter 4

Fault Tree Analysis

4.1 Chamber states

To get a better understanding of the probability, fault trees are produced for every chamber state. Table 3.2 is used to find all fault events that creates a specific chamber state. A failure event for a valve is denoted xPy, z where xPy correlates with valve V_{xPy} and $z \in \{O, C\}$ for open or closed failures. The event of a pressure line failure is denoted p_{sx} in the fault trees.

4.1.1 Closed state

As mentioned for table 3.2, a "C" equals a closed and/or a pressure line failure. In the fault trees this corresponds to an OR gate with failure event xPy, C and failure event p_{sx}. The fault tree for closed state can be seen in figure 4.1, equation 4.1 shows the Boolean expression.

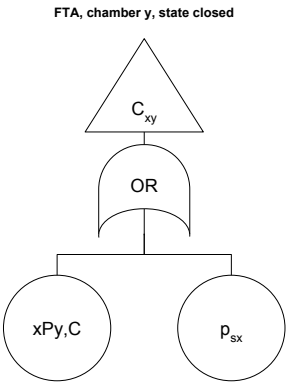


Figure 4.1: The fault tree for state C_{xy}

$$C_{xy} = xPy, C + p_{sx} \tag{4.1}$$

4.1.2 Open state

Chamber state open, O_{x1y} on chamber y can be achieved in five different ways according to table 3.2. This is represented in the fault tree in figure 4.2, transfer in symbols is used to add closed states in the fault tree. The Boolean expression is found in equation 4.2.

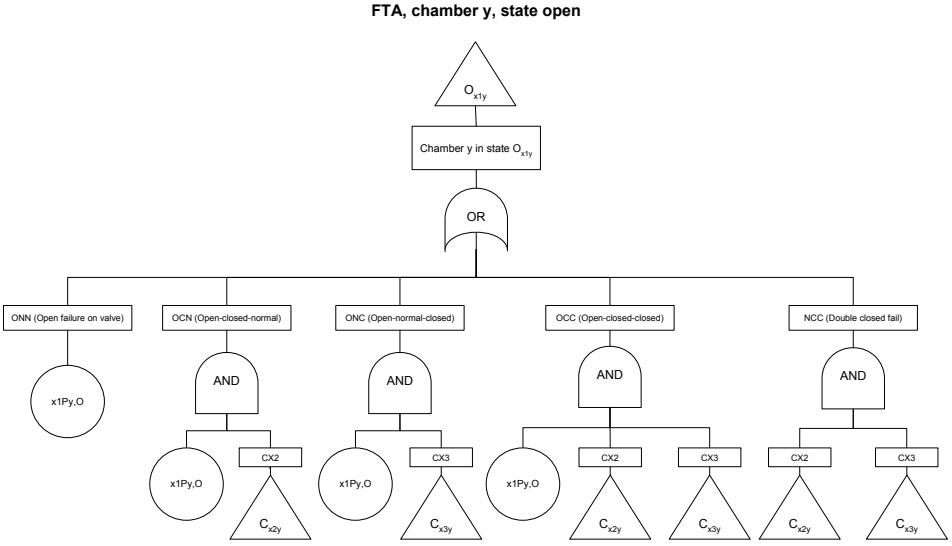


Figure 4.2: Fault tree for chamber y state O_{x1y} before reduction.

$$x1Py, O + x1Py, O \cdot CX2 + x1Py, O \cdot CX3 + x1Py, O \cdot CX2 \cdot CX3 + CX2 \cdot CX3 \tag{4.2}$$

Equation 4.2 can be reduced using the abortion law:

$$x1Py, O\big(x1Py, O \cdot CX2 + x1Py, O \cdot CX3 + x1Py, O \cdot CX2 \cdot CX3\big) + CX2 \cdot CX3 =$$

$$x1Py, O + CX2 \cdot CX3$$

By inserting equation 4.1 the full expression 4.3 is derived. The reduced fault tree is shown in figure 4.3.

$$O_{x1y} = x1Py, O + (x2Py, C + p_{sx2})(x3Py, C + p_{sx3}) \tag{4.3}$$

Where $x1, x2, x3 \in \{1, 2, 3\}$ and $x1 \neq x2, x1 \neq x3, x2 \neq x3$.

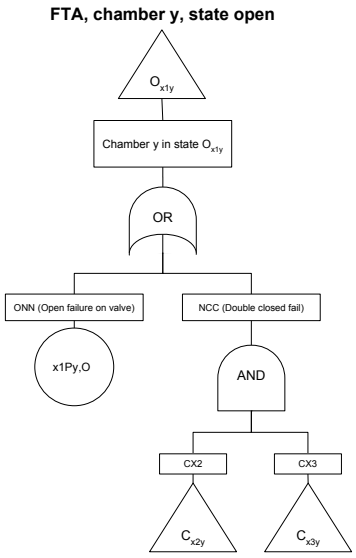


Figure 4.3: Fault tree for chamber y state O_{x1y} after reduction.

4.1.3 Normal state

Since normal chamber state is not a failure the probability for this state is 1, always true. Equation 4.4, figure 4.4.

$$P(N) = 1 \tag{4.4}$$

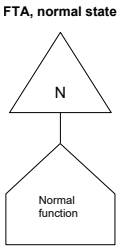


Figure 4.4: Fault tree for normal state. $P(N) = 1$

4.1.4 Chamber state $\emptyset$

The state $\emptyset$ has three main categories. In figure 4.5 the sub fault tree for the different situation is constructed and assembled into one, with figure 4.6. The case showed in figure 4.5c is not present in table 3.2 since a valve can not have two failures at the same time. The figure represents the failure where a pressure line

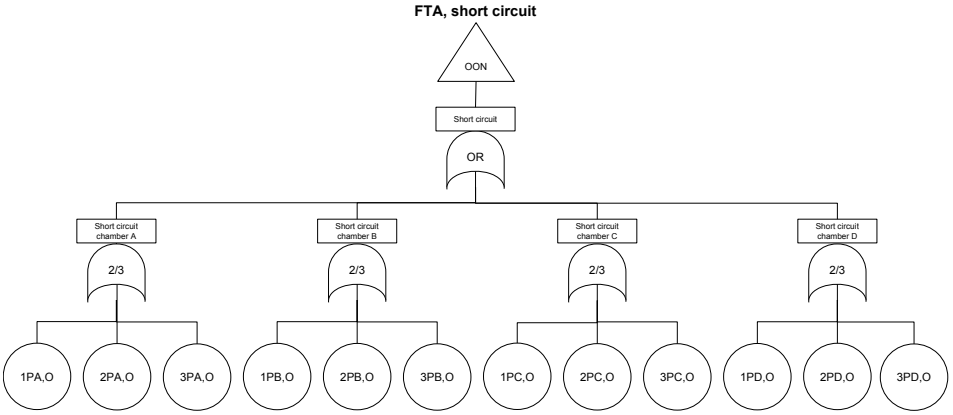
fails in combination with an open failure on the same pressure line which gives zero pressures in the chamber. Equation 4.5-4.8 shows the Boolean expressions.

$$\begin{aligned} OON = {} & 1PA, O \cdot 2PA, O + 1PA, O \cdot 3PA, O + 2PA, O \cdot 3PA, O + \\ & 1PB, O \cdot 2PB, O + 1PB, O \cdot 3PB, O + 2PB, O \cdot 3PB, O + \\ & 1PC, O \cdot 2PC, O + 1PC, O \cdot 3PC, O + 2PC, O \cdot 3PC, O + \\ & 1PD, O \cdot 2PD, O + 1PD, O \cdot 3PD, O + 2PD, O \cdot 3PD, O \end{aligned} \tag{4.5}$$

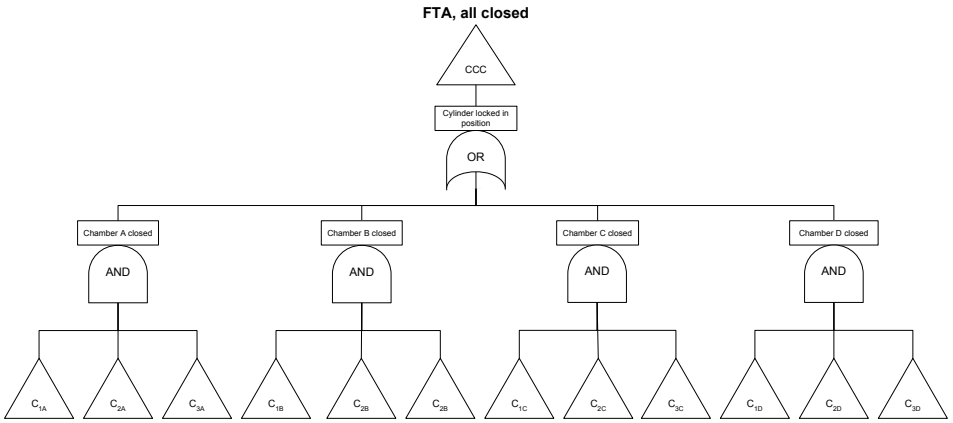
$$\begin{aligned} CCC = {} & C_{1A} \cdot C_{2A} \cdot C_{3A} + C_{1B} \cdot C_{2B} \cdot C_{3B} + \\ & C_{1C} \cdot C_{2C} \cdot C_{3C} + C_{1D} \cdot C_{2D} \cdot C_{3D} \end{aligned} \tag{4.6}$$

$$\begin{aligned} Op = {} & p_{s1}(O_{1A} + O_{1B} + O_{1C} + O_{1D}) + \\ & p_{s2}(O_{2A} + O_{2B} + O_{2C} + O_{2D}) + \\ & p_{s3}(O_{3A} + O_{3B} + O_{3C} + O_{3D}) \end{aligned} \tag{4.7}$$

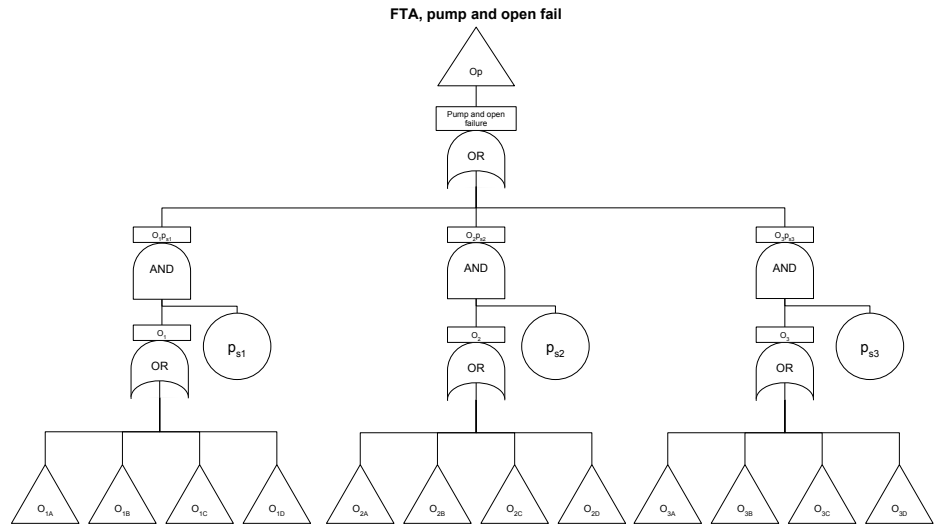
$$\emptyset = ONN + CCC + Op \tag{4.8}$$



(a) FTA for short circuits in the system. The 2/3 gates are *choosing gates*, 2 out of 3 must fail for the gate to fail.



(b) FTA for all valves on the same chamber closed.



(c) FTA for combination of pump failure and open failure on same pressure line.

Figure 4.5: Fault trees for sub cases to $\emptyset$.

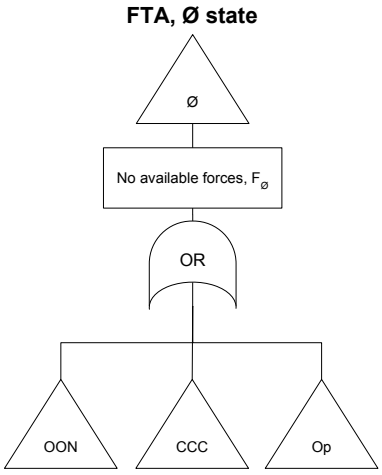


Figure 4.6: This tree shows all cases that creates ∅. This by combining 4.5a, 4.5b and 4.5c into one tree.

4.2 Force distributions

Every unique force distribution can be calculated by combining the four chamber states. This is achieved by an AND gate, see figure 4.7 and equation 4.9.

$$S_a S_b S_c S_d = S_{aA} \cdot S_{bB} \cdot S_{cC} \cdot S_{dD} \tag{4.9}$$

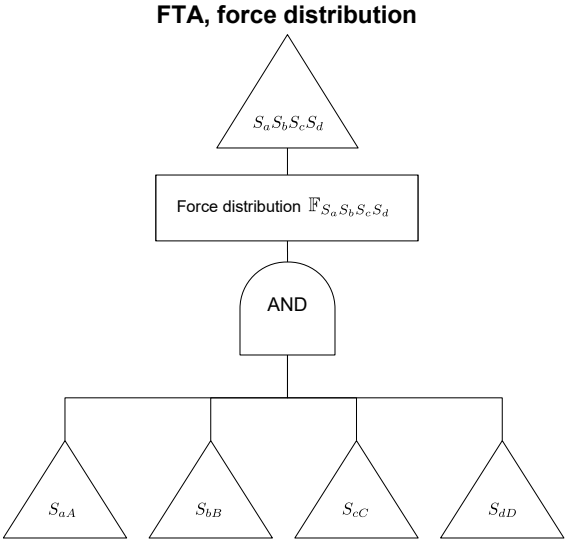


Figure 4.7: With an AND gate the four chamber states get assembled into a specific force distribution.

4.3 Assembling complete fault tree

To assemble a complete fault tree a top event must be chosen. There are several possible choices for a top event; positive/negative force, resolution, number of forces etc. or a combination of these. This is dependent on the system requirements. Figure 4.8 and equation 4.10 show the general look of a complete fault tree.

$$\text{Top event} = S_{a1} S_{b1} S_{c1} S_{d1} + S_{a2} S_{b2} S_{c2} S_{d2} + \cdots + S_{an} S_{bn} S_{cn} S_{dn} + \emptyset \tag{4.10}$$

4.3.1 Algorithm

To create and reduce the fault tree the following algorithm is used.

1. Calculate all 2401 unique force distributions, remove the ones not causing the top event.

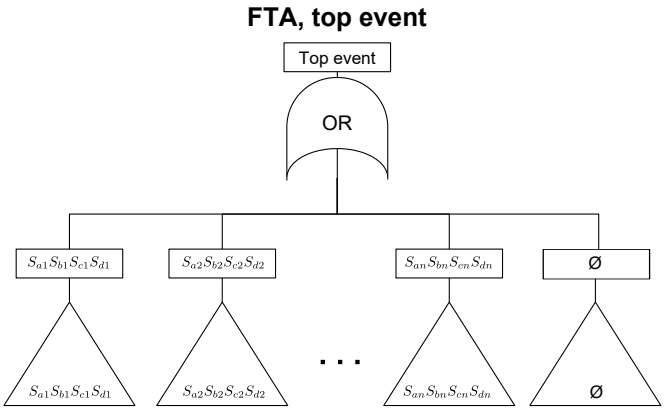


Figure 4.8: The top fault tree.

2. Calculate the Boolean expression for all distributions using equation 4.1, 4.3, 4.4 and 4.9. Reduce the Boolean expressions with the idempotent law. (A double closed state can for example give $p_{s1} \cdot p_{s1} \rightarrow p_{s1}$ this should be placed in the single table, not double.) Add the result to Boolean tables (figure 4.9).

3. Add state $\emptyset$, with equation 4.5-4.8, to the tables if these are considered to cause the top event.

4. Reduce the tables, a true value sets false in all higher dimensions (the abortion law), see figure 4.10.

5. Combinations that still are true after the reduction is the minimal cut set for the top event.

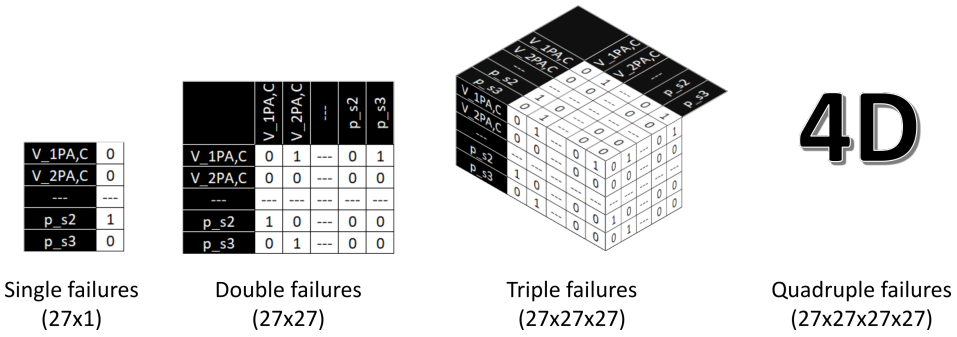


Figure 4.9: The combinations are placed in Boolean tables. Where for example triple(V_1PA,C, V_1PB,C, V_1PC,C) = true means that the combination of $V_{1PA,C} \cdot V_{1PB,C} \cdot V_{1PC,C}$ causes the investigated top event.

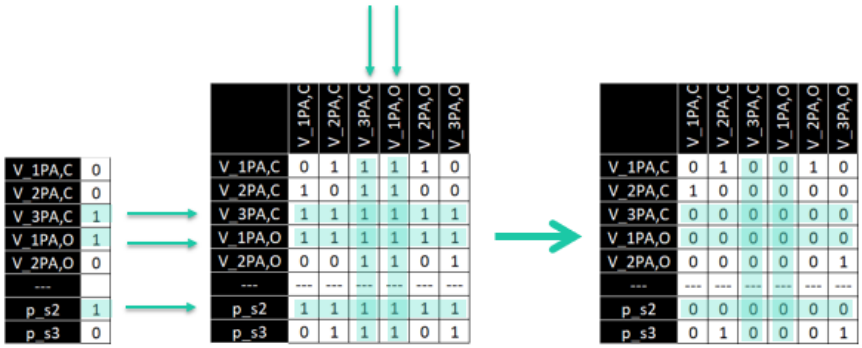


Figure 4.10: Reduction of the Boolean tables. A true value in first dimension sets false in higher dimensions.

4.3.2 Example: $\kappa_{min} \leq 0.8$, LASHIP

To show how the algorithm explained in section 4.3.1 works an example is presented below. This example uses $\kappa_{min} \leq 0.8$ as top event. The definition of κ_{min} is found in equation 3.22-3.24. $\kappa_{min} \leq 0.8$ could be translated to 80% force or less in the system.

1. Of the 2401 force distributions, 2349 have a $\kappa_{min} \leq 0.8$.
2. Totally 8677 combinations are added to the Boolean tables.
3. Another 64 combinations are added to the Boolean tables.
4. The tables are reduced into 27 combinations, 18 single and 9 double combinations, these are represented in a fault tree in figure 4.11.
5. -

4.3.3 Example: $\kappa_{min} \leq 0.2$, LASHIP

Another example with $\kappa_{min} \leq 0.2$ as top event.

1. Of the 2401 force distributions, 1245 have a $\kappa_{min} \leq 0.2$.
2. Totally 5786 combinations are added to the Boolean tables.
3. Another 64 combinations are added to the Boolean tables.
4. The tables are reduced into 283 combinations, 70 double, 161 triple and 52 quadruple, these can be seen in figure 4.12. Notable that there are no single fault events.
5. -

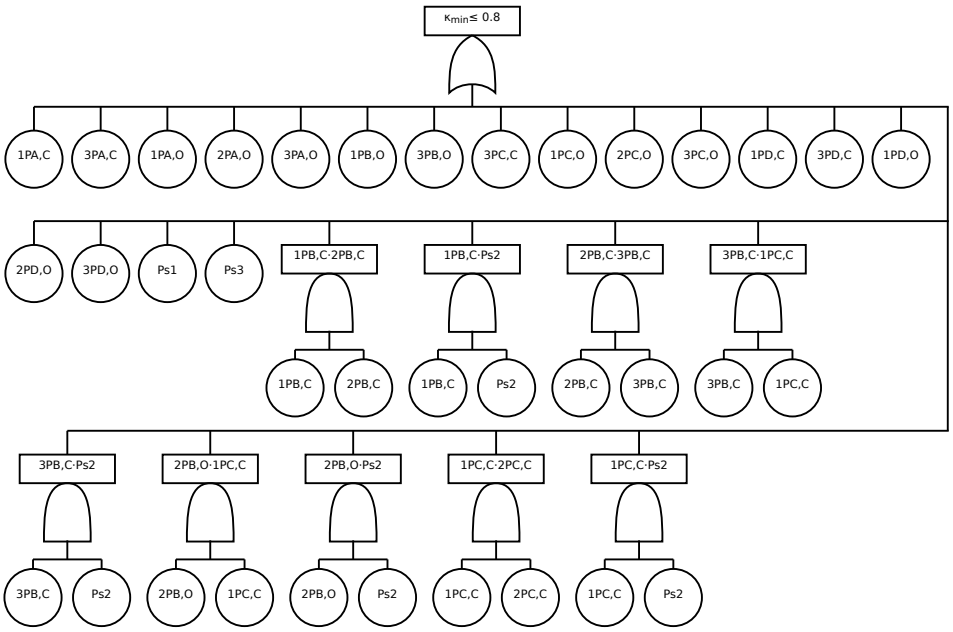


Figure 4.11: Complete fault tree for $\kappa_{min} < 0.8$, test rig LASHIP.

4.3.4 Implementation of algorithm

The used implementation of this algorithm only calculates up to quadruple failures. In section 3.4 is proven that it will always exist double failures causing $\kappa_{min} = 0$. Therefore, combinations of five or more failures are negligible in terms of probability and not considered. Also, all unique force distributions can be found using only four or less failing valves since there are four chambers and all chamber states are obtainable with one failing valve. In figure 4.12 this is seen by the occurrence of a diamond symbol, this is to mark that it can exist failure combinations with five or more failures.

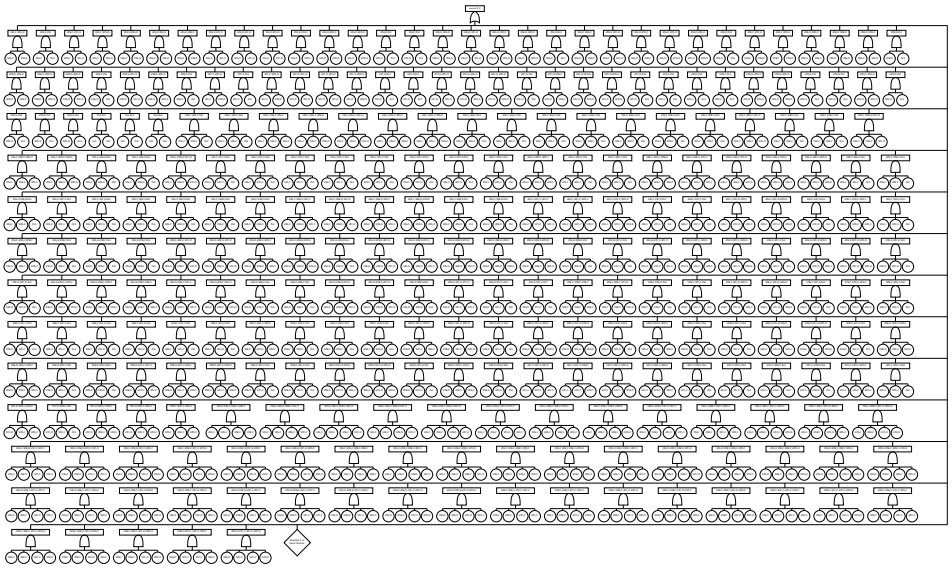


Figure 4.12: Complete fault tree for $\kappa_{min} < 0.2$, test rig LASHIP.

4.4 Reference system

To make a comparison between the DHA system and the reference system seen in figure 2.3, a fault tree analysis is performed on the reference system. This analysis is made with only logical reasoning about the hydraulics. The fault accommodation for the reference system is to close the bypass valves setting the subsystem into free floating mode [5].

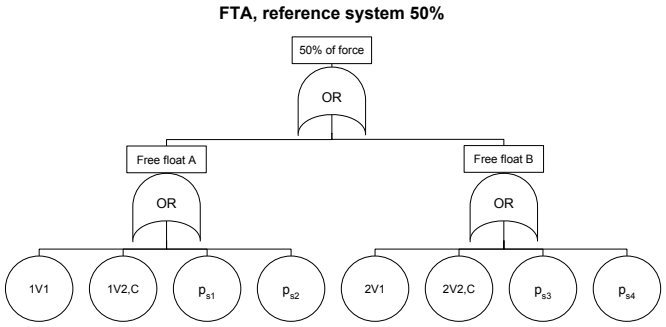


Figure 4.13: Fault tree for 50% force on the reference system.

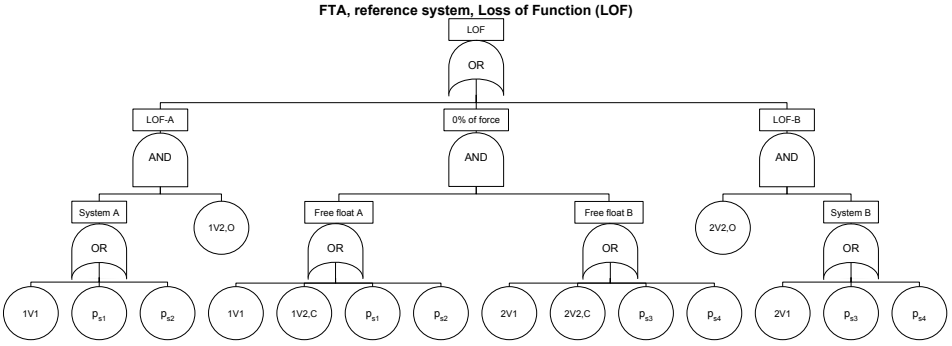


Figure 4.14: Fault tree for Loss of Function(LOF) on the reference system.

Chapter 5

Simulations

The simulation model used in this theses is a modified version of the F16 model used by S. Ward (2017) [26]. The DHA system has chamber areas [12.1, 10.6, 10.0, 10.1] cm^2 and the pressures are [28, 7.6, 0.75] MPa. Figure 5.1-5.4 shows some screenshots of the model. The model uses the AeroAircraft6DOFSS component included in the standard libary of HOPSAN [19]. This component is an air plane with six degrees of freedom. The model allows to model the hydraulic actuators separately.

In the used model right and left evelon have a DHA system implemented (figure 5.3 and 5.4) while the other control surfaces uses the reference system (figure 2.3).

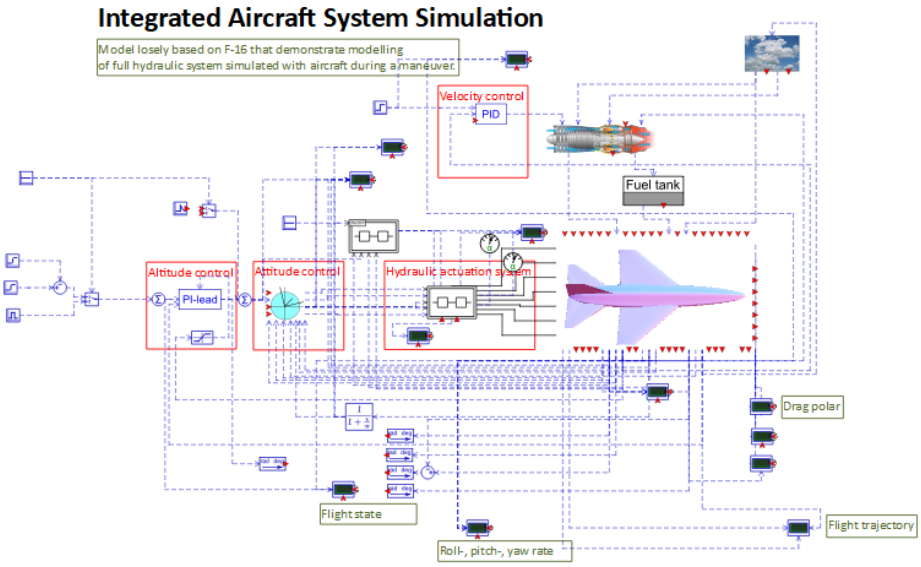


Figure 5.1: Complete simulation model.

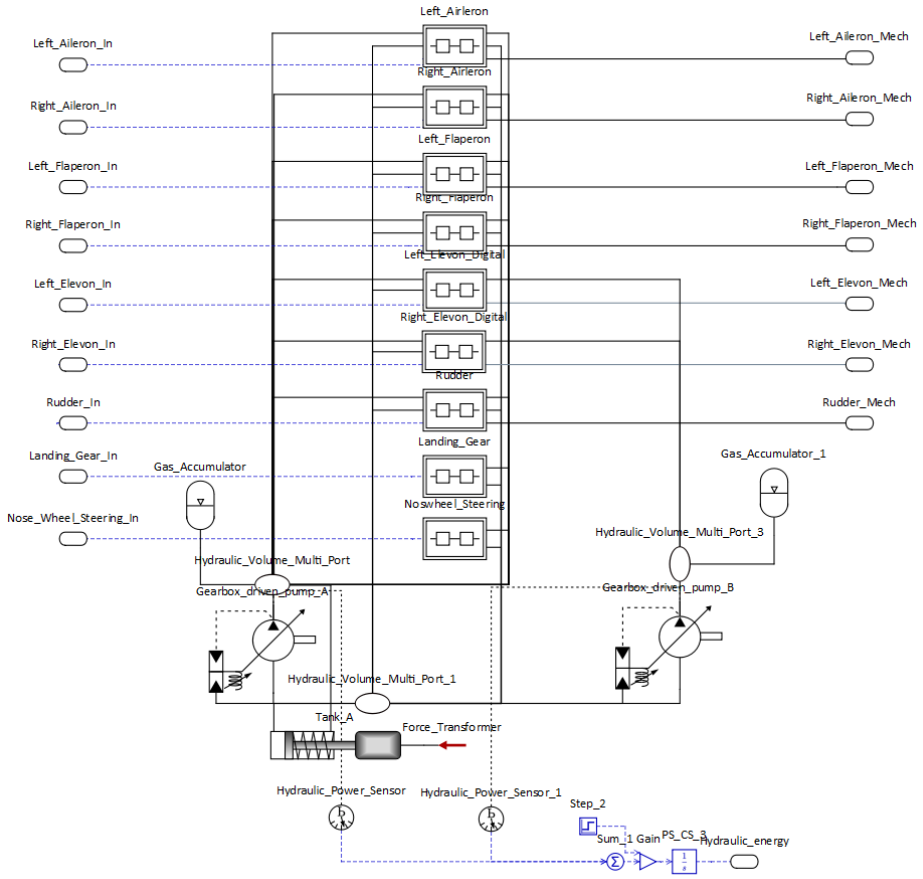


Figure 5.2: Sub models of the hydraulic system.

Changes made to the model, in comparison to S. Ward's simulations, are listed below.

1. The digital hydraulic quantisation block has been changed to implement fault accommodations suggested in this thesis.

2. According to advices from H. Belan the digital hydraulic quantisation block is changed to recalculate the discrete forces in every timestep. This change means that the block uses current pressure line pressures and not reference pressures in its calculations. This gives a more stable behaviour. H. Belan implemented this the same way in his PhD thesis [3]. A low-pass filter with $\tau = 1$ rad/s is used to filter the signal from the pressure sensor.

The flight manoeuvre used in the simulation is a steady flight at one kilometre above ground. After 50 seconds a step response is made in the reference altitude to two kilometres above ground. After another 50 seconds the reference steps back

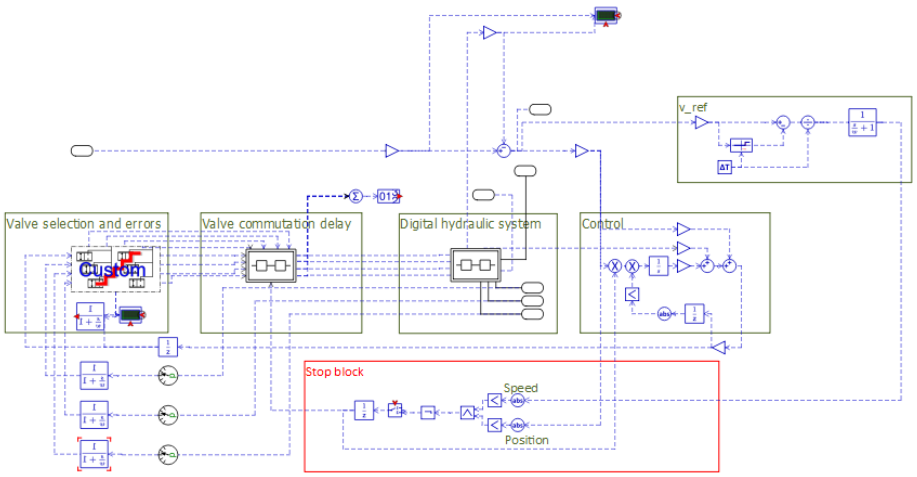


Figure 5.3: DHA-controller on left evelon.

to one kilometre. The simulations are analysed in a Boolean manner, no crash (figure 5.5a), or crash (figure 5.5b - 5.5d). All successful flight missions achieves the reference altitude after some time. The appearance of all the successfully missions are roughly the same on 150 second scale. A crash is defined as a simulation where the aircraft altitude reaches zero meter. Crashes appear in three main categories:

- Unable to maintain steady state flight, figure 5.5b.
- Unable to perform positive flank of the reference, figure 5.5c.
- Unable to perform negative flank of the reference, figure 5.5d.

These three situations are treated as the same.

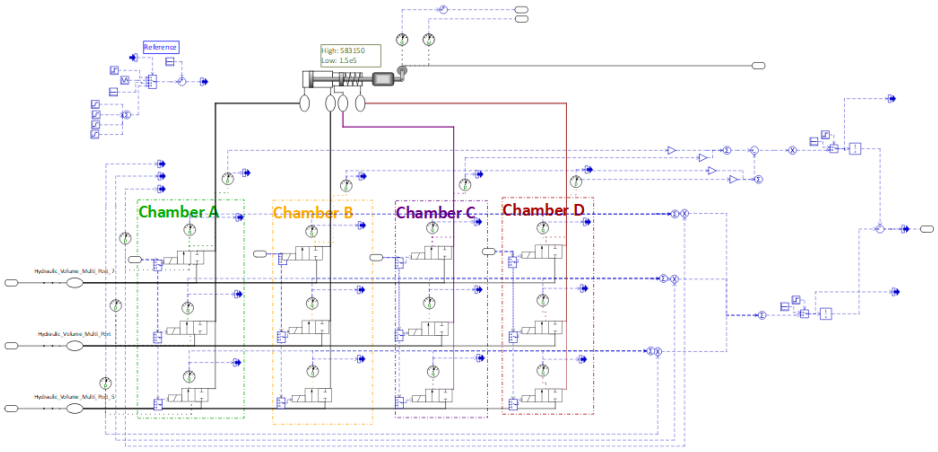
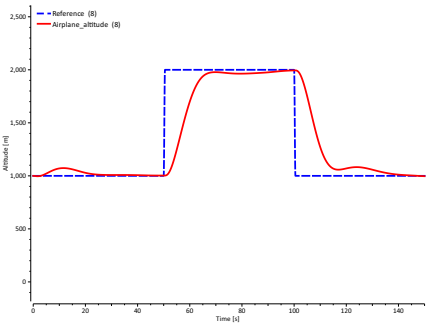
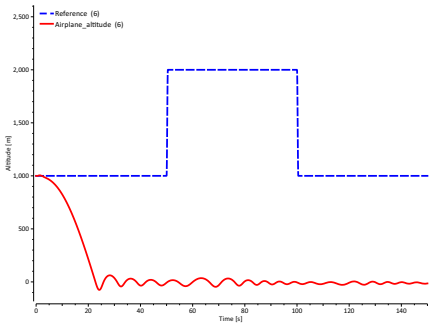


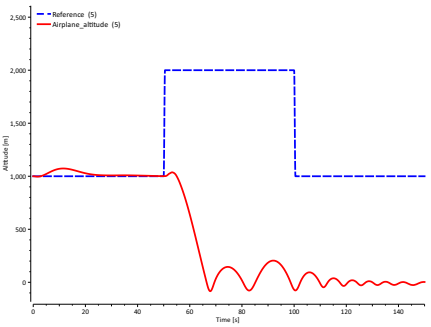
Figure 5.4: DHA system on left evelon.



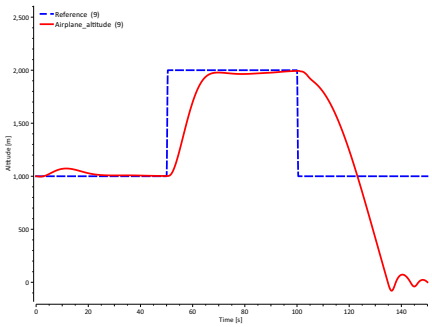
(a) A successful simulation, without crash.



(b) A crashing aircraft, unable to maintain steady state flight.



(c) A crashing aircraft, unable to perform positive flank of the reference.

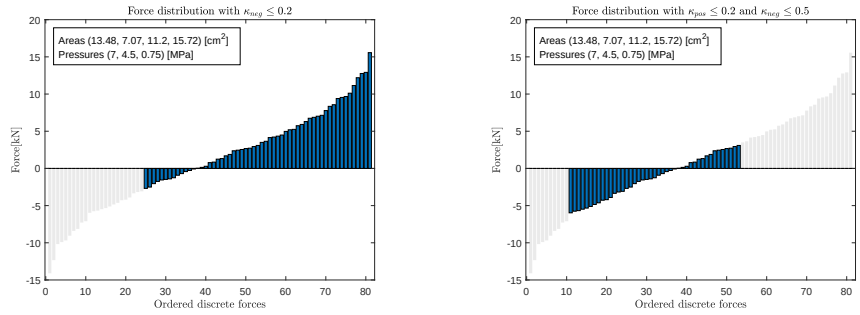


(d) A crashing aircraft, unable to perform negative flank of the reference.

Figure 5.5: There are four types of simulation results. Red line is the aircraft altitude. The dashed blue line is the reference altitude.

5.1 Statistical property

The quantisation block allows simulation of force distributions with a specific κ. These force distributions are unrealistic as a failure case since all valves and pressure lines are used, but are interesting for analysis. In figure 5.6 two examples of these types of force distributions are shown.



(a) A force distribution with $\kappa_{neg} \leq 0.2$.

(b) A force distribution with $\kappa_{pos} \leq 0.2$ and $\kappa_{neg} \leq 0.5$.

Figure 5.6: Two types of force distributions limited by κ-values.

Chapter 6

Results

6.1 Types of error

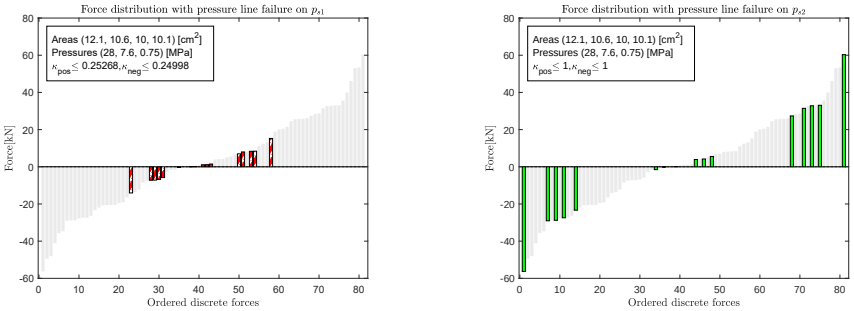
In table 6.1 a selection of κ_{min} on LASHIP test rig [3] is shown. The remaining fault events, after the fault tree is reduced, are grouped into types. Open and pressure line failures have, in comparison to closed failures, a larger impact and are therefore represented for lower κ-values.

Table 6.1: Table of types of errors, in reduced fault trees, for different κ_{min} on LASHIP test rig. C=closed failure, O=open failure, P=Pressure line failure. CC means a combination of two closed failures. CO is an open-closed combination etc.

$\vee\vert$ κ_{min}	C	O	P	$\sum$ Single	CC	CO	CP	OO	OP	PP	$\sum$ Double	$\sum$ Triple	$\sum$ Quadruple
0.0	0	0	0	0	0	1	0	19	12	3	35	166	141
0.1	0	0	0	0	0	3	1	24	13	3	44	197	87
0.2	0	0	0	0	0	11	5	34	17	3	70	161	52
0.3	0	0	0	0	0	15	12	39	24	3	93	153	6
0.4	0	2	1	3	4	19	8	32	12	1	76	72	4
0.5	0	4	1	5	10	23	12	23	12	1	81	26	0
0.6	0	6	2	8	15	24	6	15	4	0	64	9	0
0.7	2	9	2	13	11	10	5	3	2	0	31	0	0
0.8	5	11	2	18	4	1	3	0	1	0	9	0	0
0.9	8	12	2	22	0	0	0	0	0	0	0	0	0
1.0	12	12	3	27	0	0	0	0	0	0	0	0	0

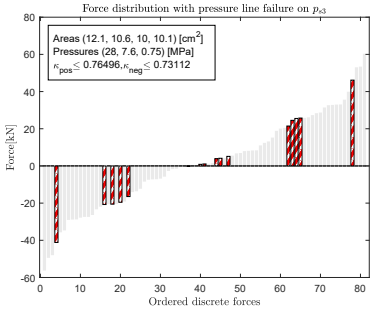
6.2 Simulation results

In figure 6.2 some results from the simulations are shown. Force distributions with a green solid fill are from successful flights and force distributions with a striped fill are from unsuccessful flights.



(a)

(b)



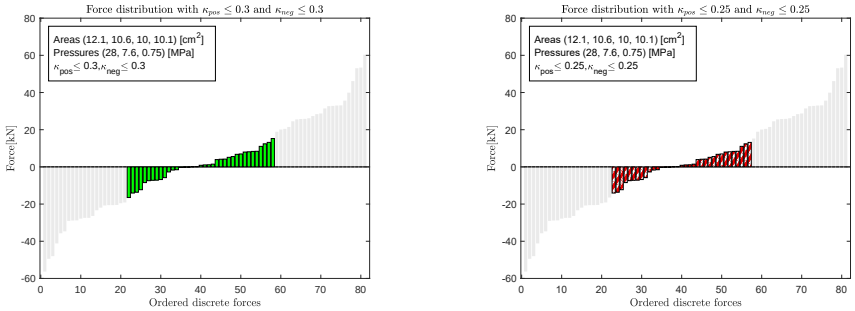
(c)

Figure 6.1: Simulation result pressure line failures, green bars means successful flight, red means crash.

6.2.1 Inconsistent results

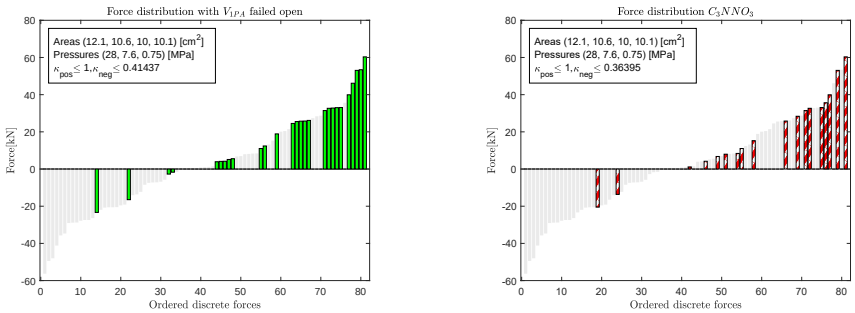
The simulation of pressure line failure on p_{s3} stands out since it have a high κ_{min} ($\kappa_{min} = 0.73$) and still fails (figure 6.1c). After further investigation of the simulation an answer to this is found in the pressure line itself and not the DHA system.

Pressure line p_{s3} is the normal system drain, but in that case it is closed. Therefore, the majority of the returning flow goes through p_{s2} which cannot handle this higher flow. p_{s2} has a reference pressure of 7.6 MPa but the pressure in this simulation has an average of 18MPa, before the crash after 100 sec, see figure 6.3. A redrawn force distribution with the new pressure is presented in figure 6.4. This is more similar the other failing distributions.



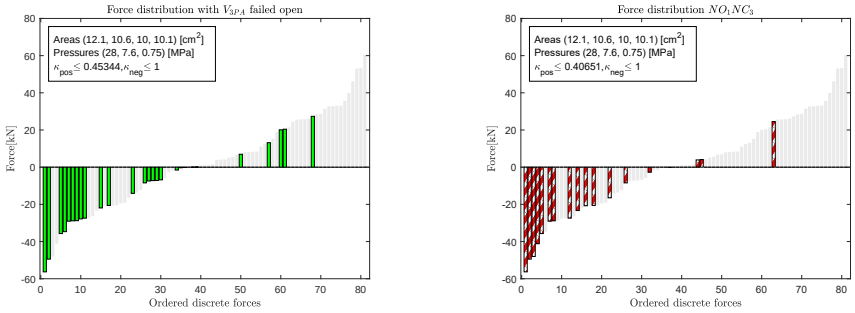
(a)

(b)



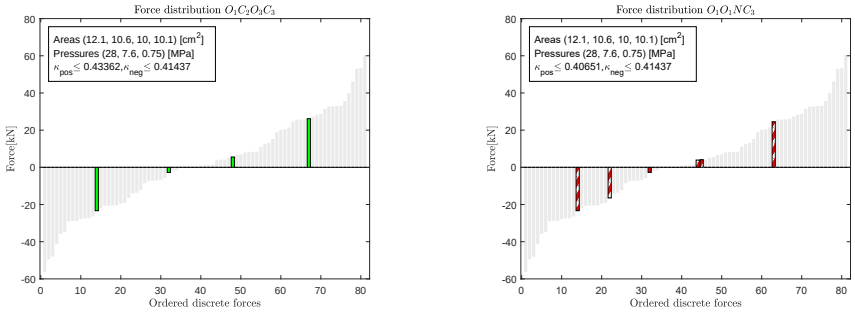
(c) Force distribution O_1NNN

(d)



(e) Force distribution O_3NNN

(f)



(g)

(h)

Figure 6.2: Simulation result valve failures, green bars means successful flight, red means crash.

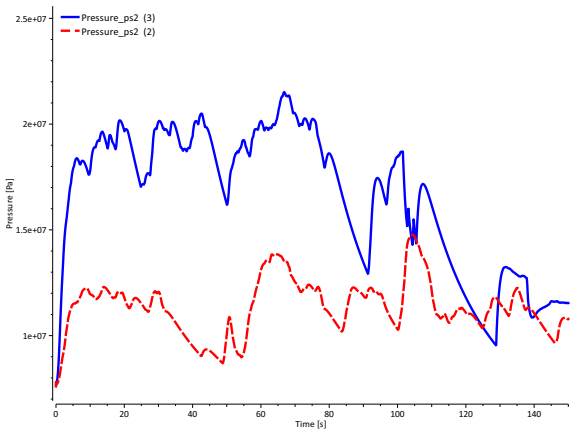


Figure 6.3: The blue line is p_{s2} when p_{s3} is failing. The plane crashes after 100 sec. The red dashed line is p_{s2} from a flight in normal condition. Both pressures are filtered with a 1 rad/s low pass filter.

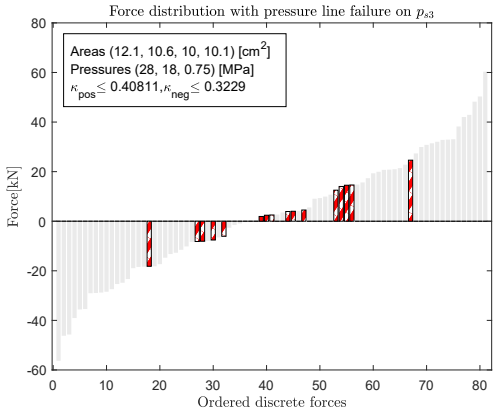


Figure 6.4: Force distribution for pressure line failure on line p_{p3} with changed pressure for p_{s2}.

6.3 Probability calculations

When calculating probabilities the pressure lines are excluded. Pressure lines are not just a single component, but another complex hydraulic system. This hydraulic system is not analysed in this thesis and consequently not included in the calculations. However, the pressure lines are assumed to be equivalent as in the reference system and thereby the difference should be small in terms of probabilities.

6.3.1 Assumptions

All components are assumed to have a constant failure rate. Therefore, an exponential probability distribution is used to calculate individual failure probabilities, see section 2.8.1.

The type of fast switching on/off valves needed for digital hydraulics are not commonly used on the market today [21]. Therefore, there are only a few reliability studies on this type of valves. J. Barg (2011) [2] calculates a theoretical failure rate of 25-100 dangerous failures/10^9h over a 1920h period for a PWM system with four fast switching on/off valves in an indoor environment. These are promising results but it might be unrealistic to use them for calculations on military aircraft.

The proportional valves used in the reference system are more commonly used. Therefore, an assumption is made that an on/off valve has the same failure rate as these valves. Half their failure rate for closed failures and the other half for open failures. This makes the total failure rate equal, see equation 6.1 and 6.2. The same assumption is made for the bypass valve in the reference system.

$$\lambda_{prop} = \lambda_{on/off,closed} + \lambda_{on/off,open} \tag{6.1}$$

$$\lambda_{on/off,closed} = \lambda_{on/off,open} \tag{6.2}$$

In the book *Nonelectronic parts reliability data* (1981) [1] reliability data is found for hydraulic valves used in uninhabited areas on an airborne fighters. An uninhabited area is an area where extreme condition exists such as big pressure or temperature differences, like a wing placement. The failure rate for this valve is $\lambda_{prop} = 17.309$ failures/10^6h. This value is used in the calculations.

The flight time (t in equation 2.6) is the number of hours the plane is used before the valves are replaced in scheduled maintenance, regardless if they work or not. In this thesis a flight time of 1000 hours is used, which corresponds to roughly three hours use per day for a year.

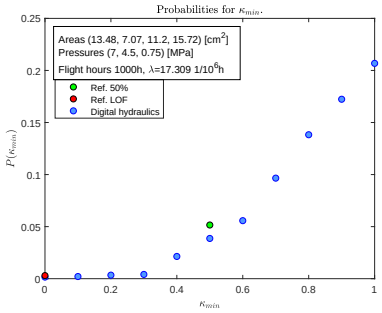
6.3.2 Probability results

In figure 6.5 calculations for three area-pressures combinations are shown. To the left are plots of the calculations and to the right corresponding force distributions. Figure 6.5a and 6.5b show the test rig at LASHIP [3]. Figure 6.5c and 6.5d show an evenly spread system presented by H. Belan et al (2015) [5]. Figure 6.5e and 6.5f is a system with a symmetrical four-chamber cylinder. A symmetrical system has

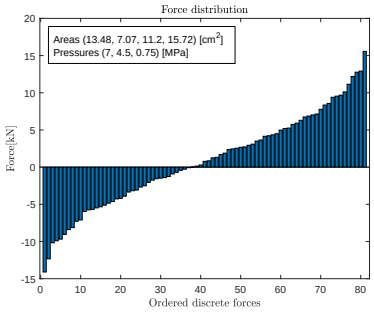
equal influence from all chambers which gives the highest κ_{min} for single failures. This is explained in section 3.4.

6.3.3 Sensitivity analysis

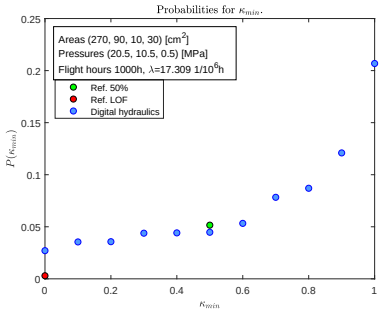
To see how the parameters affects the calculations, a sensitivity analysis is made. The λ-value and the flight hours are changed to large and small values. In figure 6.6 the result of this analysis is shown. All tests are done on test rig LASHIP and should be compared with figure 6.5a. In the calculations same changes of λ-value and flight hours are made for both the digital system and the reference system.



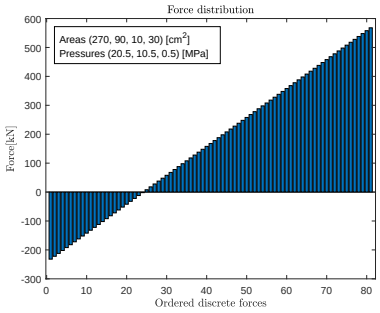
(a) Single failures for $\kappa_{min} \geq 0.4$.



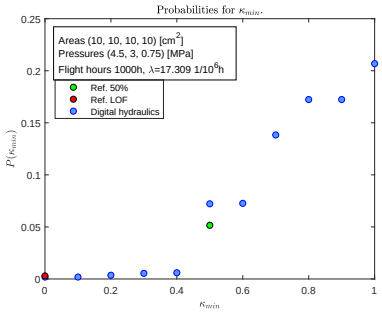
(b) Test rig LASHIP



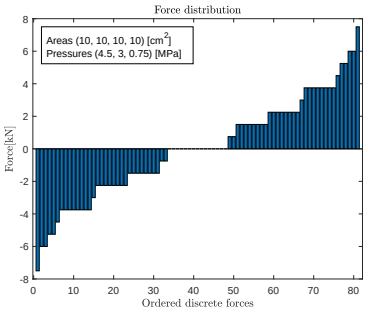
(c) Single failures for all κ_{min}.



(d) Evenly spread

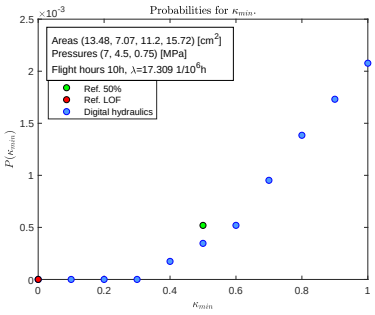


(e) Single failures for $\kappa_{min} \geq 0.5$.

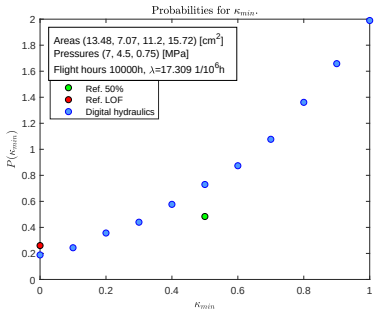


(f) Symmetrical cylinder

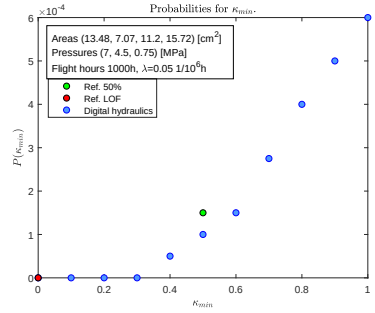
Figure 6.5: Probability calculations for three different area-pressure combinations. Force distributions for same systems are shown to the right.



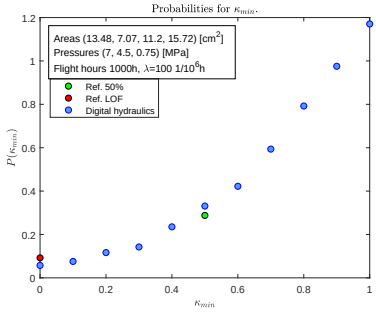
(a) LASHIP test rig with a short flight mission, 10h.



(b) LASHIP test rig with a long flight mission, 10 000h.



(c) LASHIP test rig with a small failure rate, $\lambda = 0.05\ 1/10^6$h.



(d) LASHIP test rig with a big failure rate, $\lambda = 100\ 1/10^6$h.

Figure 6.6: Sensitivity analysis of probability calculations.

Chapter 7

Discussion

A major part of this thesis have been in new research areas on a relatively new system. Therefore, many assumptions have been made and the analysis still has many inadequacies. In this chapter some of these inadequacies are presented.

7.1 Fault tolerant system

The most critical single failures according to section 3.4.3 are simulated in both negative (figure 6.2c) and in positive direction (figure 6.2e), both with successful results. Therefore, the conclusion is that the simulated system is fault tolerant for valve failures.

This conclusion is not true for all area-pressure combinations though. In figure 3.10 the even force distribution presented by H. Belan et al. (2015) [5] is shown with one open failure. This force distribution has no negative forces. Thereby it will not be able to retract the cylinder and consequently the system will fail. Therefore, the evenly spread area-pressure combination is not fault tolerant.

The probability calculations give the same result. The evenly spread system (figure 6.5c) has a much higher probability for $\kappa_{min} \leq 0$ in comparison to the other two systems, that require double faults for $\kappa_{min} \leq 0$. Everything relates to that area A_A on the evenly spread system is 67.5% of the total area and thereby the system will have a 67.5% loss of the force range in case of an open failure, according to equation 3.33.

7.1.1 Tolerance of pressure line failures

In the simulation results two out of three pressure line failures are causing system failure (figure 6.1). Therefore, the system is not fault tolerant to these failures. As already discussed in section 6.3, pressure lines are often a more complex setups than just one component. These setups are fault tolerant to their own component failures. This means that several components within the pressure line have to fail before it affects the DHA and its fault accommodation has to take place. Therefore, these results are not stopping our whole system form being fault tolerant.

7.2 Correct top event

As seen in the simulation results (figure 6.1 and 6.2) κ_{min} is not the only factor that makes the system fail or not even though it seems to be a key factor. Future studies need to be done to correctly decide a top event for use in the Fault Tree Analysis.

The implementation used in simulation that restricts κ_{neg} and κ_{pos} (figure 6.2a and 6.2b) recalculates the discrete forces to current pressure level at every time step. The fault accommodations used in the other simulations work with fixed set of valves. This means that the κ-values presented for the other simulations are only valid when the pressure lines have their reference pressures while the simulations in figure 6.2a and 6.2b always have $\kappa_{min} = 0.3$ and $\kappa_{min} = 0.25$. Therefore, these simulations are not fully comparable.

From the simulation in figure 6.2a and 6.2b the conclusion would be that $\sim 30\%$ of force is needed in both directions. The other simulations give $\sim 43\%$ in positive and $\sim 41\%$ in negative direction, except simulation 6.1c which is discussed in section 6.2.1.

The simulation 6.1c tells us that to just calculate κ_{min} of the reference pressure is not sufficient to find all system failures. Therefore, further studies is needed to find correct system requirements and top events.

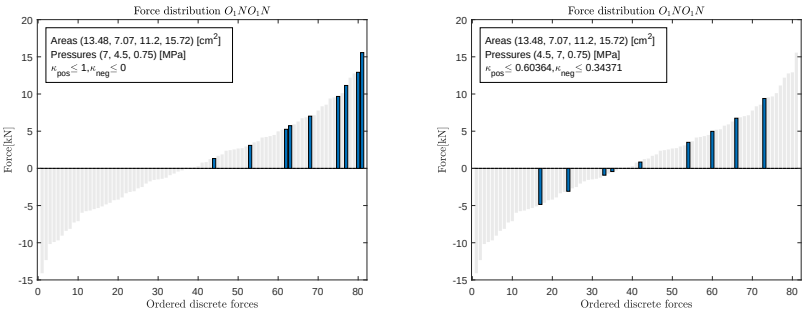
The values from table 2.1 (10% at Military Aircraft, Cruise, Pitch) are a bit lower than for the failing systems in this thesis. These values represent the typical forces while the percentages in this thesis are maximum forces. Therefore, the results are reasonable, a typical value should be lower than a maximum value.

7.3 More complex fault accommodations

Pressure lines in DHA-systems are considered to be variable and able to change pressure level. This opens up for another kind of fault accommodations where pressure levels change according to failures. An example is found in figure 7.1 where p_{s1} and p_{s2} switch values at a specific failure mode. By doing this more failure modes could be controlled.

7.3.1 Adding components

Another approach to control more failures could be to add more components. In figure 7.2 a system setup with a *mid-bypass* is shown. This would help in case of some failure modes, see the comparison in figure 7.3. The extra valve creates a bypass that gives pressure p_{s2} in the chamber, this center the range loss in the force spectra according to section 3.4.2. Compared to the solution of changing the reference pressures, this leaves the other chambers unaffected. Figure 7.3 shows an example where a mid-bypass is made. For this failure combination same easy pressure switch as shown in figure 7.1 cannot be made since two pressure lines are affected.



(a) With default pressures.

(b) p_{s1} and p_{s2} switched.

Figure 7.1: Both figures show open failures on V_{1PA} and V_{1PC}. In figure 7.1b, p_{s2} and p_{s3} have switched values.

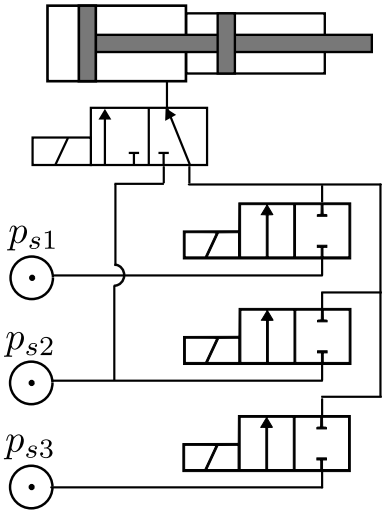
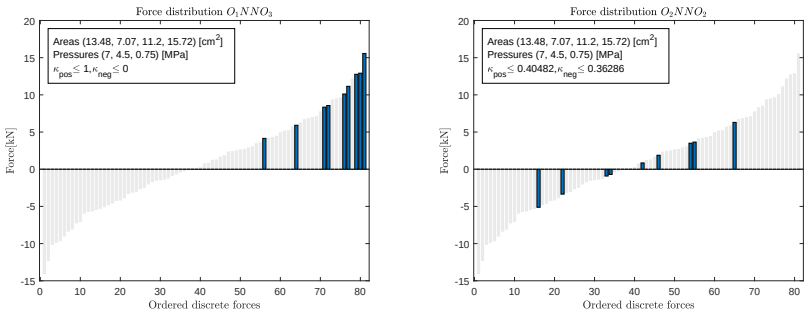


Figure 7.2: By adding a bypass valve to all chambers more failure modes can be handled.



(a) Without mid-bypass (b) With mid-bypass

Figure 7.3: The effect of using a mid-bypass for open failure on V_{1PA} and V_{3PD}.

7.4 State ∅

In this thesis short circuits (figure 4.5a) and combinations of pressure line failures and open failures (figure 4.5c) are considered as a direct cause of failure. This since the used fault accommodations gives zero forces. But with other fault accommodations, were the system works with other pressures than the reference pressures, it is possible that the system could maintain control in these cases. This is explained more in the following sub chapters.

7.4.1 Short circuit

For the short circuit (figure 4.5a) two pressure sources are connected without restrictions. Over time this will lead to a common pressure for the pressure lines, a basic hydraulic law. This will reduce the pressures in the whole system to two. The chamber with the short circuit will have a constant pressure, the common pressure, and the other three chambers will be able to alternate among these two pressures. Therefore, eight discrete forces could be available in the system (equation 3.14). As seen in figure 6.2g only four forces were enough to keep the plane stable, so this could be a successful flight. But to do so another type of fault accomondation is needed.

7.4.2 Open and pressure line failure

For the combination of pressure line and open failure (figure 4.5c) the failing chamber will have the same pressure as the failing pressure line. The used controller already measures the pressures and could therefore use this new pressure only in this chamber. Yet again this would demand another type of fault accommodation not considered in this thesis.

A problem with this would be if the pressure line failed in a way that made it impossible to let flow throw. This would cause a closed hydraulic volume, which would lock the cylinder. This is the same as in the third sub case of state ∅, a triple closed chamber (figure 4.5b). This would also create a closed hydraulic volume and lock the cylinder.

7.5 Other failure modes

In this thesis only three types of failure modes have been considered; closed valve failure, open valve failure and pressure line failure. However, there are other failure modes that needs to be considered. Leakage of valves are one of the most common failure modes. N. Bender et al. (2017) [6] shows a study where within 5 years 100% of the fast switching valves have a small leakage (0.0005 l/min). One plausible fault accommodation for leakages is to handle them as open failures, but this have to be further investigated. Another problem with leakages are the fault diagnostics. The fault diagnostics presented in the literature study for DFCUs was only for open/closed failures.

7.6 Uncertainties in calculations

As seen in figure 6.6 the calculations are rather unaffected by changes in the parameters. But the assumption that on/off valves and proportional valves have the same failure rates has no background. If there is a big difference between in the failure rates the reliability will not be the similar either.

Another assumption made for the calculations is that on/off valves have the same failure rate for open and closed failures, this is probably not true either. The used on/off valves are of type *normally closed* on/off valves. A normally closed valve has a closed position as default. Thereby many failures, such as loss of control signal, would cause a closed failure and not an open. Most probably a normally closed valve have a lower failure rate for open failures compare to closed. A lower open failure rate would just improve the system reliability since open failures have bigger system impacts, see table 6.1.

Another aspect not considered with the failure rates is the tight relationship between failures and switching frequencies that J. Barg (2011) [2] points out. If the system is designed in a way that makes some valves switch more often, these valves will have a higher probability of failure.

7.7 Unrealistic simulation model

In the simulation model the closing and opening time for an on/off valve is set to 8ms. This time is based on an assumption H. Belan did 2015 [5] before he built test rig at LASHIP.

In the measurement H. Belan has done on the test rig the mean value closing time is 55ms [3]. This allows the simulation model to switch much faster than possible on the test rig. For example in the simulation represented by figure 6.2g, there are only four discrete forces, the system then switches very fast, working as a PWM system, between these four forces. If the simulation model would replicate the test rig this would not be possible.

At the same time the development of faster and better on/off valves have already started [13] and the used valve on LASHIPs test rig may not be the best on the market which is a subject that H. Belan discusses [3]. B. Winkler (2017) [27] presents a state of art on fast switching market valves and ongoing research in the field. On the market today there are valves that have switching times of 5ms or less.

Chapter 8

Conclusion

Based on the results shown in this thesis a DHA system is not fault tolerant by default. It has been shown that, the area-pressure combination has a large impact on the fault tolerance. If the areas and pressures are chosen in the correct way an active fault tolerant system can be achieved. By distributing the chamber areas equally, the dependency of individual valves is minimized, this comes with a cost of controllability of the system. For applications such as aviation where both controllability, safety and reliability are important, a good trade-of would be a semi-symmetrical cylinder.

A DHA system with a semi-symmetrical cylinder has a loss of more than 50% of the total force for the most critical failure. This should be taken into consideration when replacing current systems. A higher maximum/minimum force is required for the DHA system if the force after failure would be equal.

Among used fault accommodations closed failures have the smallest impact. Therefore, from a safety perspective normally closed valves should be used.

Under the assumption that fast switching on/off valves have similar failure rate as proportional valves, the DHA have similar system reliability. Therefore, a DHA system can be equally good from a safety perspective and a promising alternative for an aviation application.

8.1 Future studies

Some suggested future studies in the subject are:

- **Fault diagnostics** - To achieve the suggested controller a reliable fault diagnostic is a requirement and therefore a subject for future studies.

- **System requirements** - The assumption made in this thesis that the system requirement is just a percentage of force, κ, is probably incorrect. Properties such as number of discrete forces is most probably also a factor. More studies need to be done to get a better picture of this.

- **Reliability of fast switching on/off valves** - To get better calculations of the system reliability there is a need for better component data.
- **Other control strategies** - If the safety requirement demands a fault tolerant system to all single and double failures more complex control strategies are needed. Changing reference pressures to the pressure lines or adding more components could be solutions to overcome the problem.

Bibliography

[1] Arno, R. G. Nonelectronic parts reliability data-2. Tech. rep., RELIABILITY ANALYSIS CENTER GRIFFISS AFB NY, 1981.

[2] Barg, J. Safety in digital - hydraulics (en iso 13849).

[3] Belan, H. C. *Sistemas de atuação hidráulicos digitais para aviões com foco em eficiência energética.* PhD thesis, Federal University of Santa Catarina, 2018.

[4] Belan, H. C., Krus, P., Lantto, B., , and De Negri, V. Digital hydraulic actuator (dha) concept for aircraft actuation systems. In *Recent Advances in Aerospace Actuation Systems and Components* (2016), pp. 41–46.

[5] Belan, H. C., Locateli, C., Lantto, B., Krus, P., and De Negri, V. Digital secondary control architecture for aircraft application. In *The Seventh Workshop on Digital Fluid Power* (2015), pp. 26–27.

[6] Bender, N. C., Pedersen, H. C., Plöckinger, A., and Winkler, B. Reliability analysis of a hydraulic on/off fast switching valve. In *The Ninth Workshop on Digital Fluid Power* (2017).

[7] Blanke, M., Kinnaert, M., Lunze, J., Staroswiecki, M., and Schröder, J. *Diagnosis and fault-tolerant control*, vol. 2. Springer, 2006.

[8] Code of Federal Regulations. 14 cfr 25.671 - general. [Online] Legal Information Institute, Open access to law since 1992 "https://www.law.cornell.edu/cfr/text/14/25.671", 1970. Last accessed on 2018-02-21.

[9] Dell, A., Marcus, C., and Erik, N. Investigation of a digital hydraulic actuation system on an excavator arm. In *The 13th Scandinavian International Conference on fluid power* (2013).

[10] Dhillon, B. S. *Design reliability: fundamentals and applications.* CRC press, 1999.

[11] Ersfolk, J., Ahopelto, M., Lund, W., Wiik, J., Waldén, M., Linjama, M., and Westerholm, J. Online fault identification of digital hydraulic valves using a combined model-based and data-driven approach. *arXiv preprint arXiv:1803.05644* (2018).

[12] James E. Vance and Walter James Boyne. Airplane. [Online] Encyclopædia Britannica, inc. `https://www.britannica.com/technology/airplane`, 2017. Last accessed on 2018-02-05.

[13] Linjama, M. Digital fluid power: State of the art. In *12th Scandinavian International Conference on Fluid Power, Tampere, Finland, May* (2011), pp. 18–20.

[14] Linjama, M., Huova, M., Boström, P., Laamanen, A., Siivonen, L., Morel, L., Waldèn, M., and Vilenius, M. Design and implementation of energy saving digital hydraulic control system. In *In: Vilenius, J. & Koskinen, KT (eds.) The Tenth Scandinavian International Conference on Fluid Power, May 21-23, 2007, Tampere, Finland, SICFP'07* (2007).

[15] Linjama, M., Vihtanen, H.-P., Sipola, A., and Vilenius, M. Secondary controlled multi-chamber hydraulic cylinder. In *The 11th Scandinavian International Conference on Fluid Power, SICFP* (2009), vol. 9, pp. 2–4.

[16] RapidTables.com. Logic symbols. [Online] RapidTables `"https://www.rapidtables.com/math/symbols/Logic_Symbols.html"`. Last accessed on 2018-04-25.

[17] RapidTables.com. Set theory symbols. [Online] RapidTables `"https://www.rapidtables.com/math/symbols/Set_Symbols.html"`. Last accessed on 2018-04-25.

[18] Robert Braun. Hopsan project. [Online] HOPSAN website Linköping University `"https://www.iei.liu.se/flumes/system-simulation/hopsan?l=en"`, 2016. Last accessed on 2018-04-25.

[19] Robert Braun. Hopsan. [Online] Linköping University `"https://liu.se/forskning/hopsan"`, 2018. Last accessed on 2018-04-25.

[20] Robert T. Madison, McDonnell Douglas Corp. The md-80: hydraulics simple, reliable, and easy to operate. [Online] Hydraulics & Pneumatics `"http://www.hydraulicspneumatics.com/aerospace/md-80-hydraulics-simple-reliable-and-easy-operate"`, Jul 05, 1984. Last accessed on 2018-04-24.

[21] Scheidl, R., Linjama, M., and Schmidt, S. Is the future of fluid power digital? *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering 226*, 6 (2012), 721–723.

[22] Siivonen, L., Linjama, M., Huova, M., and Vilenius, M. Pressure based fault detection and diagnosis of a digital valve system. *Power Transmission and Motion Control (PTMC"07)* (2007), 67–79.

[23] Siivonen, L., Linjama, M., Huova, M., and Vilenius, M. Jammed on/off valve fault compensation with distributed digital valve system. *International Journal of Fluid Power 10*, 2 (2009), 73–82.

[24] Stelson, K. A. Saving the world's energy with fluid power. In *Proc. of the 8th JFPS international symposium on fluid power* (2011), vol. 15.

[25] The Swedish-Brazilian Research and Innovation Center (CISB). Cooperation brazil-sweden in aeronautics. [Online] CISB website "http://www.cisb.org.br/images/pdf/Cooperation-BR-SE-in-Aeronautics---2017.pdf", 2017. Last accessed on 2018-04-24.

[26] Ward, S. Digital hydraulics in aircraft control surface actuation. Master's thesis, Linköping university, 2017.

[27] Winkler, B. Recent advances in digital hydraulic components and applications. In *Proc. of The Ninth Workshop on Digital Fluid Power, Aalborg, Denmark* (2017).