# Active Model-based diagnosis
# -applied on the JAS39 Gripen fuel pressurization system

Diagnosis

Ronny Olsson

Reg nr: LiTH-ISY-EX-3264-2002

13 February 2002

# Active Model-based diagnosis
# -applied on the JAS39 Gripen fuel pressurization system

Master thesis performed at Vehicular systems
at Linköping Institute of Technology by

Ronny Olsson

Reg nr: LiTH-ISY-EX-3264-2002

Supervisors: Marcus Klein, Vehicular systems LiTH
Martin Jareland, Saab AB
Examiner: Lars Nielsen, Vehicular systems LiTH
Linköping 13 February 2002

# Abstract

Traditional diagnosis has been performed with hardware redundancy and limit checking. The development of more powerful computers have made a new kind of diagnosis possible. Todays computing power allows models of the system to be run in real time and thus making model based diagnosis possible.

The objective with this thesis is to investigate the potential of model based diagnosis, especially when combined with active diagnosis. The diagnosis system has been applied on a model of the JAS39 Gripen fuel pressurization system.

With the sensors available today no satisfying diagnosis system can be built. However, by adding a couple of sensors and using active model based diagnosis all faults can be detected and isolated into a group of at most three components.

Since the diagnosis system in this thesis only had a model of the real system to be tested at this thesis is not directly applicable on the real system. What can be used is the diagnosis approach and the residuals and decision structure developed here.

# Acknowledgement

This work has been carried out in cooperation with Saab AB. I would like to thank my supervisor at Saab AB, Martin Jareland, and my supervisor from LiTH, Marcus Klein, for all their guidance and support throughout this work.

I would also like to thank my colleagues at GDGT for making me feel so welcome and for always taking the time for discussions and questions.

# Contents

Chapter 1

# Introduction

This chapter gives an introduction and describes the objective of this thesis. The background to the assignment is presented together with the limitations. An outline for the reader is also given.

## 1.1 Introduction

Saab AB is an international, high technology company, active both in civil and military industry. Saab Aerospace is a business area within Saab AB, specialized in the development and production of the Gripen combat fighter. Gripen is the first operational fourth generation aircraft, it uses integrated computerized systems in order to get air superiority. Information is gathered from all parts of the aircraft which provides new possibilities to use information for diagnosis purposes. These information systems are crucial for a safe flight and therefore it is very important to supervise them. This thesis investigates the possibilities to use model-based diagnosis in order to analyze the systems.

The work of this master thesis has been performed at the section for system simulation and thermal analysis of general systems, under the business unit Gripen, Linköping, Sweden.

## 1.2 Objectives

The objective with this thesis is to investigate the potential of model-based diagnosis, both in a future Unmanned Air Vehicle as well as in Gripen. The use of active diagnosis will also be presented. The main task is to exemplify diagnosis concepts by building a diagnosis system for the fuel tank pressurization in Gripen. An overview of the diagnosis systems used today will be presented and new methods within diagnosis will be investigated.

## 1.3 Background

The general aircraft system is complex, dynamic and nonlinear. These are all factors that makes diagnosis complicated. A combat fighter also contains many subsystems, often crucial for the aircraft performance. It is therefore important to supervise these systems in order to detect and if possible isolate any malfunctions. Traditionally, systems of this kind are supervised with sensor redundancy, limit checking or trend checking. In a small aircraft it is desirable to use as little hardware as possible in order to reduce weight and save space. This is why new methods like model-based diagnosis have become more interesting. Model-based diagnosis is an approach that uses more software than traditional diagnosis systems. In model-based diagnosis, a model of the system is built in software and the values from the model are compared with the values from the system. Traditionally software is only used for diagnosis, not model building. This thesis will investigate the potential of using model-based diagnosis as a complement to, or instead of, hardware redundancy in aircraft systems.

The focus is held on the fuel system, which has originally been developed by a subcontractor but is now maintained and developed by Saab Aerospace. This opens the possibility to add new functionality and to investigate how model-based diagnosis can be used to improve the diagnosis in an aircraft system.

## 1.4 Limitations

Since no data from the real Fuel System was available, the system was replaced with a model. Saab had already built a model of the Fuel System in Easy5, a simulation software provided by Boeing. The fuel system contains few sensors and in order to build a working diagnosis system more sensors were added to the system. The fuel system was also simplified into only two tanks.

The main objective is to exemplify how a model-based diagnosis system can be built, so the model in this system is not optimized nor are the thresholds optimized with statistic methods.

Since it is supposed to be unlikely for more than one fault to occur at the same time and a diagnosis system for multiple faults would be complex the diagnosis system is limited to single faults.

The diagnosis system is also not automated, that is, the faults must be detected and isolated by observing the residual results manually.

## 1.5 Outline

The theory concerning diagnosis, model-based diagnosis and active diagnosis is presented in Chapter 2. In Chapter 3 the fuel pressurization system is presented and all components are described, both physically and how they are modelled. In Chapter 4 the diagnosis system for the fuel pressurization system is presented. All fault modes are described and the residuals are presented. Chapter 5 contains the conclusion of the verification of the system, together with the most interesting results. In Chapter 6 the results are discussed and suggestions for future work are made. In Appendix A all results from the verification experiments are presented. Appendix B contains a description of the diagnosis system as it is built in Simulink.

## Chapter 2

# Theory

This chapter introduces the theory and methods used in this thesis. The background and motivation of diagnosis are presented. Some of the terminology used in the area of diagnosis is described in order to simplify both the understanding and the reading.

## 2.1 Diagnosis background

Technical systems have been manually diagnosed as long as they have existed. When computers became available and more powerful, automatic diagnosis became possible. As the computing capacity improved more advanced software could be used. In for example model-based diagnosis an entire model of the system is built in software. The first reports in the area appeared in the 70’s and automatic diagnosis is still an active research area. Few general theories exist and much work is still to be done.

## 2.2 General diagnosis theory

In order to unify the terminology the International Federation of Automatic Control, (IFAC), has suggested some common basic terms. These terms are presented below with a short explanation. The explanations are based on the definitions made by IFAC.

- **Fault**

A fault is an unpermitted deviation of at least one characteristic property or variable of the system from acceptable/standard behavior.

- **Failure**

A fault that implies permanent interruption of a systems ability to perform a required function under specified operating conditions.

- **Fault Detection**

To determine if faults are present in the system and usually also the time when the fault occurred.

- **Fault Isolation**

Determination of the location of the fault, i.e. which component or components that have failed.

- **Fault Identification**

Determination of size and time-variant behavior of a fault.

- **Fault Diagnosis**

Two common views exists, the first includes fault detection, isolation and identification, the other only includes fault detection and isolation.

- **Active Diagnosis**

When a diagnosis is performed by actively exciting the system to reveal possible faults.

- **Passive Diagnosis**

To passively observe the system in order to detect and isolate faults without affecting its operation.

In all kinds of diagnosis the system behavior is compared with its expected behavior. If the system does not act as expected the conclusion is drawn that something is wrong. There are several ways of comparing the systems current behavior and its expected behavior.

Traditionally, diagnosis has been performed by limit checking, sensors are checked against a set of data which is predefined. If a sensor value leaves its normal range an alarm is generated. This method has a couple of drawbacks, the system might behave in different ways depending on the operating conditions. If this is the case the data set might have to be very large in order to cover all possible working conditions or the thresholds used might have to be generous. This way of diagnosing the system is also very closely connected to one specific system. Since the set of data is adapted to a specific system it might be hard to reuse on a similar system.

Another way of diagnosing a system is to use multiple sensors. This approach is called hardware redundancy. Hardware redundancy has the advantage that even if one sensor fails the system might still be able to function normally, using the working sensors. The drawback is that in order to identify the failing component, and not just that *some* component is failing, at least three sensors measuring the same value is needed. The extra hardware is expensive, adds weight and requires space. Extra hardware also increase the complexity of the system.

Model-based diagnosis is the latest contribution to diagnosis theory. Model-based diagnosis offers an opportunity to improve traditional diagnosis based on limit checking and hardware redundancy. It could be used on its own, but also as a complement to the above mentioned methods.

## 2.3 Model-based diagnosis

An alternative to the traditional approaches is model-based diagnosis. This approach might be used on its own or as a complement to other methods. In model-based diagnosis a software model of the system is built and the system is compared with the model, see Figure 2.1. If the model is correct the systems output should be equal, or close to, the output from the model, given the same input. These values can then be compared and faults can be detected and in some cases also isolated and identified.

Compared to the traditional methods model-based diagnosis has potentially a couple of advantages.

- Smaller faults can be detected and the detection time is shorter. This is due to the fact that the thresholds can be kept closer to the optimal case since the model should be designed to function under all working conditions.
- It is valid for the entire working range.
- It can be performed passively as well as actively.
- Isolation and sometimes identification becomes possible.
- Disturbances can be compensated for which makes it possible to diagnose faults in spite of the presence of disturbances.
- Compared to hardware redundancy model-based diagnosis is suitable for more kinds of components. Some components might not be possible to duplicate and other components than sensors might be modelled.
- Model-based diagnosis also offers the opportunity to re-use models or model components, in some cases only parameter changes or some other smaller adjustments have to be made.
- If a model for the control system is already built, which is often the case, that model could with small adjustments be used also for diagnosis.

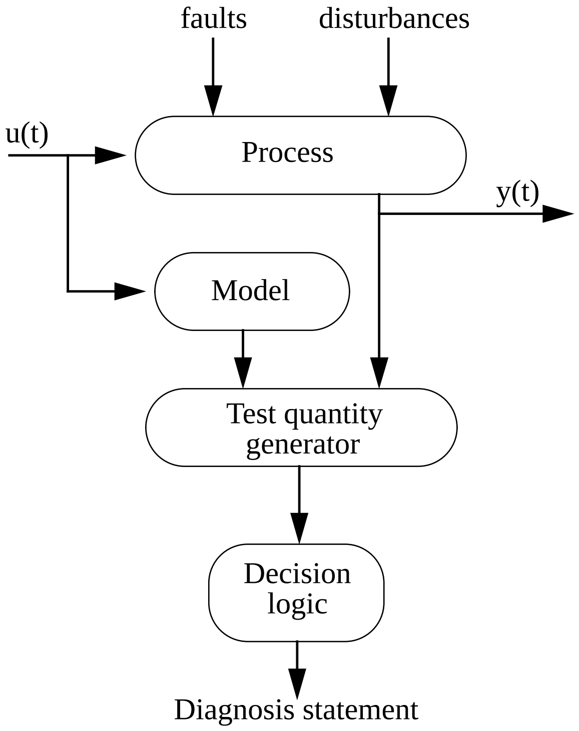


Figure 2.1: Basic diagnosis system

The problem with model-based diagnosis is the need of a reliable model and perhaps also a more complex design procedure. In order to build a satisfying model good system knowledge is needed. The limiting factor of the performance is usually the accuracy of the model. Much work must be done in order to get a satisfying model. Model-based diagnosis sometimes also requires more computing capability.

There are also situations where model-based diagnosis not fully can replace hardware redundancy. Critical components in for example an airplane might have to be duplicated so that it is possible to switch from a failing sensor to a working one. Model-based diagnosis does on the other hand offer the opportunity to switch to the model if the hardware fails. If the diagnosis system for example identify a sensor as the failing component it is possible to keep running the system, using the values from the model instead of the values from the sensor. This approach is referred to as Fault Tolerant Control, (FTC).

## 2.4 Fault models

In a diagnosis system not only the system has to be modelled, also the faults need to be modelled in order to be detected. A fault model is a representation of possible faults and how they affect the system. If an unmodelled fault occurs, the diagnosis system will not be able to give a correct diagnose. All faults might not be possible to model and which ones to model requires good system knowledge. There are several ways to model a fault, see Nyberg and Frisk [8], but these are the most common fault models.

- **Fault signals**

A fault can be modelled as an additive signal, typically:

$$y_{obs}(t) = y_{corr}(t) + f(t) \tag{2.1}$$

where

$y_{obs}(t)$ = observed value
$y_{corr}(t)$ = correct value
$f(t)$ = fault signal

This is the most general way of modelling a fault, it can describe all types of faults. It is often used for sensor faults of the type “off sets”. Unfortunately general fault models makes fault isolation difficult.

- **Deviations in constant parameters**

A fault can also be modelled as a deviation of a constant parameter, typically:

$$y(t) = (k + f(t))u(t) \tag{2.2}$$

where

y(t) = Measured value
k = constant
f(t) = Fault signal, zero in the fault free case.
u(t) = Input

$$f(t) = \left\{ \begin{array}{c} 0 \ \{NF\} \\ \\ K \ \{NF\}^C \end{array} \right\}$$

Sensor faults are often modelled this way if they are of the type “gain errors”. This fault model is also useful when the signal in the fault free case has a low and constant variance, i.e. the deviations from the mean value of the signal are small. When a fault is present the variance is still constant but higher, i.e. the deviations are bigger. There are also some faults that consist of a deviation of a physical parameter, these faults are also suited for this kind of fault model.

A fault might behave in many different ways, usually the fault can be categorized into one of the following groups, also shown in Figure 2.2.

- **Incipient faults**

Incipient faults are faults that gradually develop to a larger and larger fault. It might occur for example when a component is worn out or developing calibration errors of a sensor.

- **Intermittent faults**

Intermittent faults are faults that occur and disappear repeatedly, typically a loose connection.

- **Abrupt changes**

When a variable suddenly changes its value, a typical example is a component that suddenly breaks.

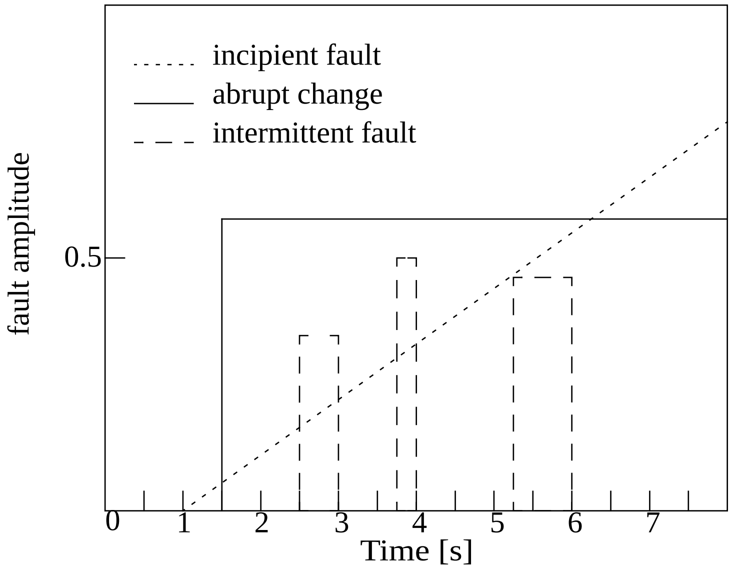


Figure 2.2: Different fault behavior

## 2.5 Test quantities

Test quantities are relations between the measured values and data from the model. The idea is that when a fault is not present the test quantity should be small and when a fault is present it should deviate significantly from zero. A test quantity should, in order to make fault isolation possible, be designed in such a way that some of the faults are decoupled. That a fault is decoupled means that the fault does not effect the test quantity in any way. By decoupling different faults from different test quantities it becomes possible to isolate faults. There are a number of ways to construct test quantities and some of them are presented below.

### 2.5.1 Consistency relation

A consistency relation is a direct relation between actuator and measurement signals. It is the most commonly used test quantity due to its simplicity. When comparing the values from the model with the measurements the difference between the values is called a residual.

If we for example compare the measured pressure $P_{meas}$ with the modelled pressure $P_{mod}$ the residual R is received as:

$$R = P_{meas} - P_{mod} \tag{2.3}$$

It is also possible to compare two values from the model, if there are two ways to receive the same value, i.e. two functions with different variables that give the same result. For example:

$$R = P_1(x_1) - P_1(x_2) \tag{2.4}$$

The residual R is what later can be used to isolate the fault with hypothesis tests in a decision structure. The residual has to fulfill two important demands.

The residual that describes the physical relations must be zero in the fault free case and the residual has to be non-zero when a fault is present. These requirements are important if the residual is to be used in a decision structure.

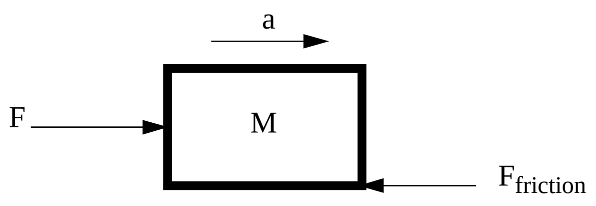
**Example.1**

Consider the mass M below, affected by the two forces $F_{friction}$ and F. Newtons equations gives the following consistency relation:

$$F = Ma + F_{friction}$$

Rewritten as:

$$F - F_{friction} - Ma = 0$$



F is an actuator signal, and the actuator signal is known in the fault free case. The acceleration is a sensor signal and $F_{friction}$ is a known disturbance. If the actuator signal F is to be supervised, and the actuator signal can be divided as:

$$F = F_1 + fault$$

Then the residual can be written as:

$$fault = Ma - F_1 + F_{friction}$$

-------------------------------------------------------------------------------------

In this example the two requirements are fulfilled.

In the non linear case it is usually harder to form residual generators with desired decoupling properties. There are no general theories like there were in the linear case. If higher order derivatives are present it might be a good idea to decouple them since they are usually hard to measure. One way of dealing with derivatives and compute the residual is to approximate the differentiated variables.

$$\hat{\dot{x}} = \frac{s}{sT_d + 1}y \qquad (2.5)$$

This method may not always be sufficient and other strategies then have to be chosen. The problem can also be solved by transforming the consistency relation, for reasonably small systems this is possible to do by hand, but for more complex systems this might be very difficult. The method is best presented by an example.

**Example.2**

Consider a system described by the following differential equation.

$$\dot{x} = -\sin^3(x) \cdot (u + f)^2$$
$$y = x + (u + f)$$

In these equations f is an actuator fault that has to be supervised. By differentiating the measurement equation and eliminating x a consistency relation is produced.

$$\dot{y} + \sin^3(y - u) \cdot u^2 - \dot{u} = h(y, u, f)$$

$$h(u, y, f) = \dot{f} - \sin^3(y - u - f) \cdot (u + f)^2 + \sin^3(y - u) \cdot u^2$$

In these equations the time derivatives are assumed to be unknown, therefore stable first-order dynamics is added to these equations.

$$r + \alpha \cdot \dot{r} = \dot{y} + \sin^3(y - u) \cdot u^2 - \dot{u}$$

By rewriting this equation the following relation is received.

$$\dot{z} = -\frac{z}{\alpha} - \frac{1}{\alpha}(y - u) + \sin^3(y - u) \cdot u^2$$

$$r = \frac{z}{\alpha} + \frac{1}{\alpha}(y - u)$$

The internal form of this filter is:

$$r + \alpha \cdot \dot{r} = h(u, u, f)$$

--------------------------------------------------------------------------------------

This example was taken from Frisk [1], page 73.

As mentioned earlier the theory behind non linear consistency relations is complicated and will not be covered further in this thesis, for a more complete examination of this theory see Frisk [1], or Nyberg and Frisk [8].

### 2.5.2 Observers

Another way of generating a test quantity is to use an observer. Observers are more powerful than consistency relations but are also more complex and harder to work with. It can be hard to get a intuitive feeling of how the observer is working, see Gustafsson *et al.* [5] or Glad and Ljung [3] for more information. Some major difficulties with observers are:

- Observer structure and to ensure stability.
- Decoupling of faults and disturbances.

A number of different observers can be generated, consider for example the system below.

$$\begin{aligned}\dot{x} &= Ax + Bu \\ y &= Cx \\ x(0) &= x_0\end{aligned} \tag{2.6}$$

The matrixes A, B and C are known and u and y can be measured, $x_0$ is the initial value and x is unknown. One way of estimating x would be to simulate the system using the real signal u.

$$\begin{aligned}\dot{\hat{x}} &= A\hat{x} + Bu \\ \hat{x}(0) &= \hat{x}_0\end{aligned} \tag{2.7}$$

This estimation will not be perfect since the equations have different initial values. This system is also very sensitive to disturbances. One way of improving this observer would be to use the information in y. If the simulation was perfect the estimated output would be equal to the output from the real system. Thus, the following signal can be used to improve the observer.

$$\dot{\hat{x}} = A\hat{x} + Bu + K(y - C\hat{x}) \tag{2.8}$$

In this equation K is a [n x m]-dimensional matrix which feeds back the estimation quality. There are several ways of choosing K but one good way is to use a Kalman filter, see Gustafsson *et al.* [5]. The Kalman filter ensures stability in the linear case. There is no general way of doing this in the non-linear case but one approach is to linearize the system around a number of working points and then use linear methods. This gives an observer which is likely to work in a surrounding of the working points.

The observer can then be used to compare the estimated value with the measured value, producing a residual in the same way as for a consistency relation.

Consistency relations are better suited for linear systems where simple models can be built. In the linear case the system can be modelled as a filter which is easy to transform into a consistency relation. Filters are well suited for real time systems since the calculations are simpler then when an observer structure is used.

Observers are better suited in the non-linear case, where filters are harder to design, especially in combination with linearization. The drawback with observers is the additional calculations that have to be made in order to estimate the future value of the signal. See Nyberg and Frisk [8] or Frisk [1] for more information about nonlinear residual generation.

## 2.6 Hypothesis tests

Formally the hypothesis test has two regions. The null hypothesis test, $H^0$, is that the fault mode present in the process belongs to the set M of fault modes. $H^1$ is the alternative hypothesis, and it means that the present fault mode does not belong to M. That is, if $H^0$ is rejected and $H^1$ accepted the fault must belong to the complement of M, i.e. $M^c$. Each hypothesis test gives additional information of which fault modes that can be present. Together with the decision logic this information is used to form a diagnosis statement.

The null hypothesis and the alternative hypothesis can formally be written as:

$H^0$: $F_p \in M$ “The faults in M can explain data”
$H^1$: $F_p \in M^c$ “No fault in M can explain data”

It is important to remember the convention that when $H^0$ is rejected we assume that $H^1$ is true, but when $H^0$ is not rejected we do not assume anything.

Each hypothesis test should contain a rejection region, a subset where the null hypothesis is rejected. The test quantities, $T_k(x)$, are compared with some threshold $J_k$. If $T_k(x) \geq J_k$ then $H^0$ is rejected. This statement could actually also be used as the definition of the rejection region. A set of hypothesis tests can then be used to form an influence structure or a decision structure. The influence structure describes how the faults ideally affect the test quantities while the decision structure describes how the fault diagnose depends on the test quantities.

## 2.7 Decision structure

By using test quantities that decouple different sets of faults and performing hypothesis tests on these the fault can be detected and hopefully also isolated. Each test quantity has a corresponding hypothesis test. When a fault is decoupled in a test quantity this means that the hypothesis test will not be sensitive to that particular fault.

It is useful to set up an influence structure in order to see how the faults ideally affect the test quantities. Ideal in this case means that no unmodelled disturbances exist and there is no noise present. An influence structure is a matrix, built up with 0:s, 1:s and X:s. Below is an example of an influence structure.

Table 1: Influence structure

| | NF | F1 | F2 | F3 |
|---|---|---|---|---|
| $T_1(x)$ | 0 | 0 | 1 | 0 |
| $T_2(x)$ | 0 | 0 | 1 | 1 |
| $T_3(x)$ | 0 | X | 0 | 1 |

A 1 in the k:th row and j:th column means that $T_k(x)$ will be affected of all faults belonging to the fault mode of the j:th column. A 0 in the k:th row and j:th column means that if the fault mode present in the system is equal to the fault mode of the j:th column, then $T_k(x)$ will not be affected, i.e. that fault is decoupled. An X in the k:th row and j:th column means that for some but not all faults belonging to the fault mode of the j:th column, $T_k(x)$ will be affected. The X:s could be seen as “don’t care”.

Unfortunately the ideal case is rarely present, therefore it is necessary to relax the conditions and replace the influence structure with a decision structure. In reality some of the 1:s in the influence structure might appear in such a way that it is better to replace them with an X, in order not to draw false conclusions. The influence structure above can then for example be transformed into the following decision structure.

Table 2: Decision structure

| | NF | F1 | F2 | F3 |
|---|---|---|---|---|
| $\delta_1(x)$ | 0 | 0 | X | 0 |
| $\delta_2(x)$ | 0 | 0 | X | 1 |
| $\delta_3(x)$ | 0 | X | 0 | X |

From the decision structure it is possible to see which tests will respond to a particular fault. For example in Table 2 it can be seen that if no fault, NF, is present no test will respond, but if F2 is present both $\delta_2(x)$ and $\delta_3(x)$ may respond.

**Example.3**

Given the decision structure in Table 2, assume that $\delta_1(x)$ and $\delta_2(x)$ react, showing that $H_1^0$ and $H_2^0$ are rejected. The following diagnosis is then received:

$$S = \{F_2\} \cap \{F_2, F_3\} \cap \Omega = F_2$$

--------------------------------------------------------------------------------

In this equation Ω is the set of all faults. Obviously the fault is isolated to be fault mode 2.

## 2.8 Thresholds

When comparing the values from the model with the values from the system one can not expect the values to be exactly the same. Due to model errors, measurement noise and disturbances the residual can not be expected to be exactly zero. This forces us to use thresholds in order to avoid false alarms. If $T_k(x)$ is the test quantity and $J_k$ is the threshold this can be written:

$H^0$ is not rejected if $T_k < J_k$<br>
$H^0$ is rejected if $T_k \geq J_k$

The test quantity can also be based on the likelihood function and in that case the relations are reversed, see Nyberg and Frisk [8].

It is not obvious how to set the thresholds in such a way that faults easily can be detected at the same time as the number of false alarms are minimized. One way of setting the thresholds is to perform a large number of simulations. No simulations will give exactly the same result since noise is present. The noise is chosen as white noise. The threshold is then set according to a worst case scenario. This will give a system that is unlikely to fire false alarms but unfortunately there is a risk for missed detection instead. The thresholds might be set so high that an alarm is not even generated when a fault is present.

The level of the constant and time invariant thresholds can also be calculated with statistic methods. By running the system and observe the variance of the signal the threshold can be set to a value where the risk of false alarms is for example 5% or the risk for missed detection is for example 3%.

When only white noise is present, constant and time invariant thresholds is applicable, but this is however rarely the case. It is therefore usually better to use adaptive thresholds. These thresholds are based on knowledge of model uncertainties and adapt themselves to the current operating condition. When known model uncertainties are small the thresholds can be kept small and where the uncertainties are larger the thresholds are enlarged in order to avoid false alarms. No general method for adaptive thresholds exists but a commonly used structure is the one presented in equation (2.9), see Nyberg and Frisk [8].

$$J_{adp}(t) = kH_{LP}(p)(\left|H_{FD}(p)u(t)\right| + c) \tag{2.9}$$

The idea with adaptive thresholds is to adapt the threshold to the model uncertainties. $H_{FD}$ and $H_{LP}$ are linear filters, k and c are constants and p is the differentiating operator. The filter $H_{FD}$ handles weighting in frequency domain, the threshold is made large for the frequencies where the model is more uncertain and small where the model is more accurate. Filter $H_{LP}$ is a low pass filter for handling high frequency disturbances. The constant c is determined by measurement noise and also prevents the threshold from equaling zero when the input signal is zero. The constant k controls how generous the threshold should be.

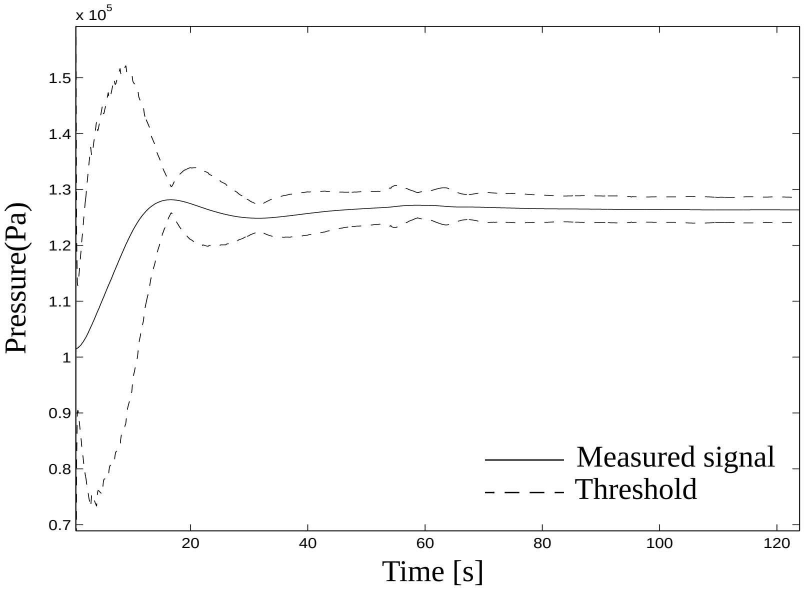


Figure 2.3: Adaptive threshold

In Figure 2.3 the function of an adaptive threshold is shown. The threshold becomes more generous when the system is dynamic since the model in this case is less accurate in the systems dynamic parts but very accurate in steady state. It is actually often the case that the model is uncertain for high frequencies and thus $H_{FD}$ is often designed to make the threshold generous in these cases.

As was mentioned above there is no general method to construct adaptive thresholds. By using statistic methods it is possible to see what model uncertainties that affect the diagnosis system the most. By using Monte Carlo simulations better adaptive thresholds can be built. The idea is to perform a lot of simulations, each with slightly different variables and with sensor noise present, and then use statistic methods to calculate the level of the thresholds in order to minimize false alarms and maximize the systems ability to detect and isolate faults. Since no hardware components have an exact value this method makes it possible to construct thresholds with better performance than if just one simulation was compared to the real system in order to find out for which frequencies the thresholds should be more generous.

Since the simulations are very time consuming this method has not been used in this thesis, the system has only been compared with the model in one case and the thresholds are constructed ad. hoc. according to equation (2.9).

## 2.9 Models

In model-based diagnosis model building is essential. The results from the diagnosis system are directly dependent on how accurate the model is. Since the values from the model will be compared with the values from the physical system they must behave in the same way if not unacceptably large thresholds need to be used. There are several ways of building a software model and two common ways will be presented here. For a full description of different model designs, see Glad and Ljung [4].

### 2.9.1 Parametric model

One way of constructing a model is to ignore the systems physical structure and only observe the input and output. By using some identification software, for example the *System Identification Toolbox* (SITB) in **Matlab**, the system can be parameterized, these parameters can then be used when building a mathematical model of the system. The advantages with this kind of model is that the user does not have to bother with the internal behavior of the system, only input and output matters. Sometimes the system is so complex that it is impossible to set up any other model. This kind of model is sometimes referred to as a black box model. Parametric models can be very hard to build if the system is non linear or regulated since the identification software does often not support identification of non linear models. When some but not all of the systems internal behavior is known, this information could be added to the model, giving us what is called a grey box model.

A common linear model is the Box-Jenkins model in (2.10).

$$y(t) = \frac{B(q)}{F(q)}u(t-n_k) + \frac{C(q)}{D(q)}e(t) \tag{2.10}$$

where e(t) is white noise and:

$B(q) = b_1+b_2q^{-1}+...+b_{nb}q^{-nb+1}$

$C(q) = 1+c_1q^{-1}+...+c_{nc}q^{-nc}$

$D(q) = 1+d_1q^{-1}+...+d_{nd}q^{-nd}$

$F(q) = 1+f_1q^{-1}+...+f_{nf}q^{-nf}$

Box-Jenkins model can be simplified by for example ignoring to model the noise, i.e. to say that C(q)/D(q)=1. There are also other variations of this model but these will not be presented here.

When building this kind of model the systems in- and output need to be observed. It is important to choose input so that the systems behavior is revealed. Thus the input has to excite the system as much as possible. This is not always easy since it might be a working system and then only ordinary signals can be used. Much work should be put in the choice of input, some common inputs are noise or telegraph signals. See Glad and Ljung [4] for more information about parametric models.

### 2.9.2 Unique model

If the systems physical behavior is easy to understand and the system is not to big or complex it might be a good idea to build a unique model. In this kind of model building every physical relationship is modelled as equations in some software language, for example *Simulink* in **Matlab**. Naturally this demands good system knowledge and good understanding of how each element within the system works. It has the advantage that the model does not waste any parameters on estimating redundant information, which might be the case with a parametric model.

A unique model also makes it easier to estimate whether the results from the model are accurate or not. Since every physical component is considered it is also easier to understand how a fault influences the system and the fault is also easier to model.

If a unique or a parametric model should be used often depends on the identification software available and if the system contains non linear elements or is regulated in some way.

Below is a unique model of the earlier mentioned mass example.

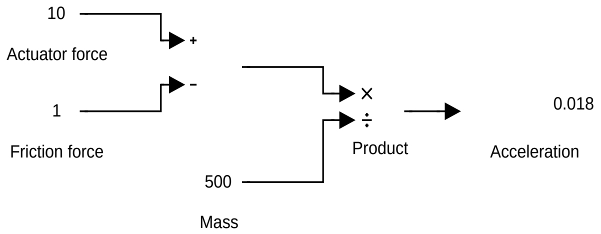


Figure 2.4: Mass example

## Chapter 3

# Fuel system

In this chapter the Gripen Fuel System will be described. The system will be described both on a general level and also with focus on the fuel tank pressurization and its components. The mathematical description of these components will be presented in section 3.2 and in section 3.3 the complete fuel pressurization model will be presented.

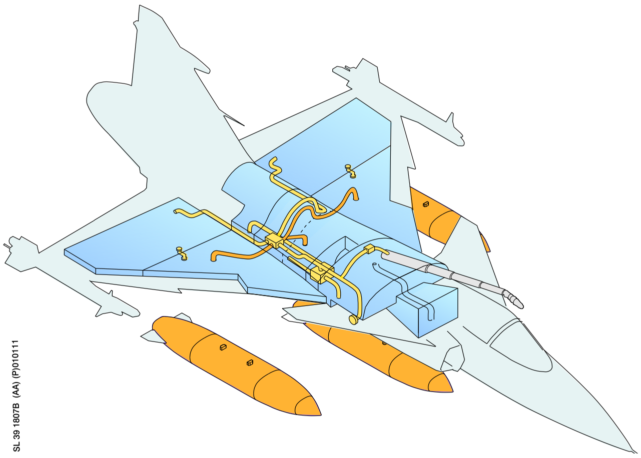


Figure 3.1: JAS 39 Gripen fuel system

## 3.1 System description

The Gripen fuel system has several tasks, of which the most important is to provide fuel to the engine, but the system is also helping the aircraft to optimize the center of gravity by moving fuel between the internal tanks. Fuel is also used as a cooling medium for some of the electronics on board. The fuel tanks have to be pressurized for several reasons, if the fuel is not kept under pressure there is a risk of cavitation problems especially at higher altitudes. The pressurization also helps when moving fuel between the tanks. Another important task is to help the engine to suck in fuel if the fuel pump should break down. In this thesis the focus is on fuel tank pressurization. The entire fuel system with all fuel tanks can be seen in Figure 3.1.

The air that supplies the fuel system is provided by the environmental control system, ECS. The air is dry, cold, and has been cleaned by the environmental control system before it enters the fuel system. As the air enters the fuel tanks it passes a pressure regulator. This regulator is set to keep the pressure in the Controlled Vent Unit, CVU, at 25 kPa over ambient pressure at all times. The air then flows through an air ejector which adds extra airflow into the tanks. The air ejector also helps with ventilating the tanks at refueling or fuel transfer. It is connected to a vent tank, kept at ambient air pressure at all times.

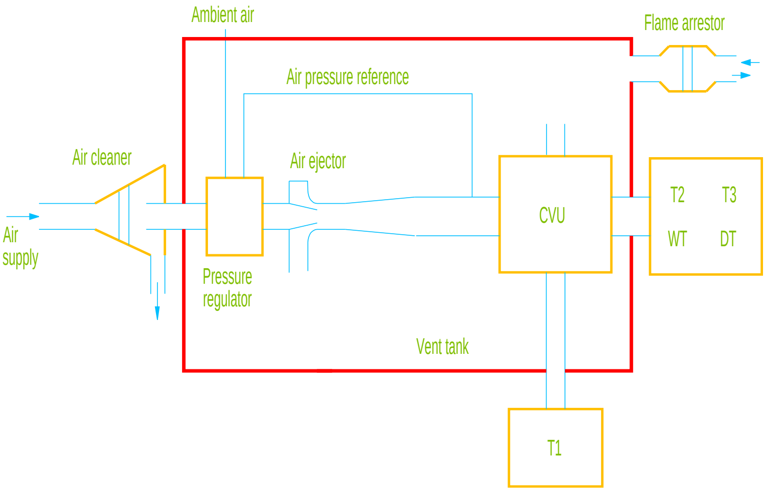


Figure 3.2: Pressurization System Principle

As the air leaves the air ejector it enters the CVU, the CVU is responsible for dividing the airflow to the different tanks. The CVU has three different positions, All, Partial, and Medium. Position Medium is only used during refueling. All tanks are then ventilated into the vent tank, making room for the fuel. When the CVU is in position All, all tanks are pressurized. When in position Partial, all tanks except tank 1 are pressurized. The reason why tank 1 is not always pressurized is because the fuel pump takes the fuel from tank 1 and therefore all other tanks should be pressurized in order to help with the fuel transfer to tank 1. The fuel tank pressurization principle can be seen in figure Figure 3.2.

## 3.2 Components

For a better understanding of how the system is operating and how it has been modelled, each component will here be described. Both the functionality and the mathematical expression of the components performance will be presented. Below is a figure of the refuel and fuel transfer system, with all tanks, pumps and the most important valves.

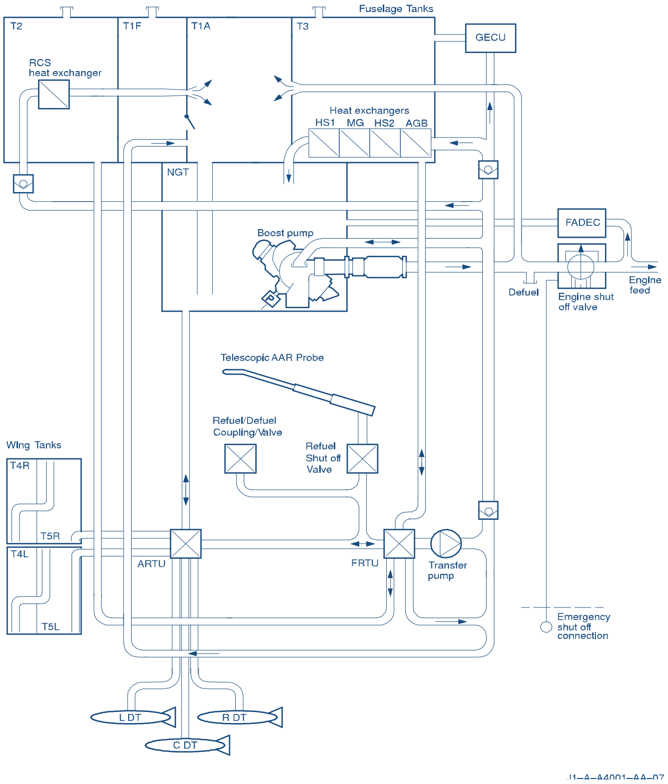


Figure 3.3: Refuel and fuel transfer system

Notice that only one boost pump is used, a rather unique solution in order to save space and weight. This also makes the fuel pressurization more important when it comes to the aspect of fuel transfer. Notice also the air to air refueling probe, designed for the export version of JAS 39 Gripen.

### 3.2.1 Pipes

The pipes in the fuel system are modelled as orifices. An orifice is a flow restriction in a duct. Orifices are well suited when modelling turbulent airflows, which is generally the case in the fuel system.

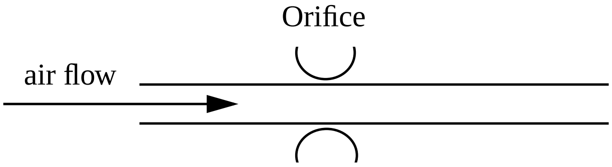


Figure 3.4: Orifice

The flow through an orifice is modelled by:

$$\dot{m} = \frac{A \cdot K \cdot P_u}{\sqrt{R \cdot T}} \cdot \frac{P_u}{P_d} \tag{3.1}$$

where

$\dot{m}$ = mass flow [kg/s]

A = orifice area [$m^2$]<br>
$P_u$ = upstream pressure [Pa] (abs)<br>
$P_d$ = downstream pressure [Pa] (abs)<br>
T = temperature [K]<br>
R = gas constant = 287 [J/(kgK)]<br>
$K(P_u/P_d)$ = look-up-table [-]

The values of $K(P_u/P_d)$ from the look-up-table depends on the values of $P_u/P_d$, the geometric shape of the flow restriction and on the fluid flowing through the orifice.

### 3.2.2 Pressure regulator

The pressure regulator has two main assignments. To regulate the pressure in the tanks to 25±5 kPa over ambient air pressure when the tanks are to be pressurized and to cut the airflow to the tanks when they are not to be pressurized. The pressure regulator is fed with air by the ECS and then the airflow passes the air ejector. There are also two other connections. One for reference pressure from CVU and one for the surrounding air pressure. The pressure regulator works like a valve. A valve is modelled as an orifice with variable area. The valves used in the model of the fuel system are of the same principal type as “butterfly valves”.

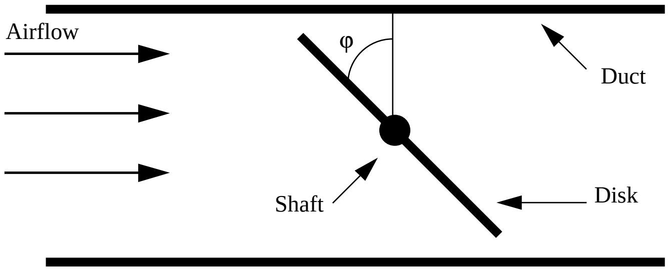


Figure 3.5: Butterfly valve

The flow through the butterfly valve is controlled by an actuator, regulating the angle φ. When φ=0˚ the valve is completely closed and when φ=90˚ the valve is completely open. The flow through the valve can be calculated by using (3.1). Alternatively the following formula might be used.

$$\dot{m} = \frac{A \cdot C}{\sqrt{T}} \sqrt{P_u^2 - P_d^2} \qquad (3.2)$$

where

C = constant of proportionality $\left[\frac{kg}{Ns}\sqrt{K}\right]$

The area is however as mentioned earlier not constant. The effective area of the valve has to be calculated by measuring angle position of the shaft using:

$$A_{eff} = A_0(1 - \cos\varphi) \tag{3.3}$$

where

$A_{eff}$ = effective area [$m^2$]
$A_0$ = maximum effective area [$m^2$]
$\varphi$ = valve angle [°]

The actuator that regulates the angle is controlled by an ordinary PI-regulator in the model. The proportionality and integral constants have been adapted to fit the “real system”. The pressure regulator is an active component, that is, it can be controlled in order to excite the system. This makes it possible to create additional residuals and thereby enhance the ability to diagnose the system.

### 3.2.3 Volume

The volume in the tanks as well as the temperature are considered to be constant at the time of measurement and calculation. This might seem to be a limiting factor but the measurement and calculating process is so fast that any volume changes due to fuel consumption etc. are negligible.

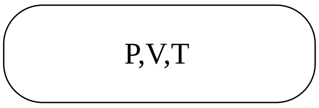


Figure 3.6: Volume

Since the volume is constant and the gas mass flow into the volume is known the pressure can be calculated using the ideal gas law.

$$PV = mRT \tag{3.4}$$

where

P = pressure [Pa]
V = volume [$m^3$]
m = gas mass in volume [kg]
R = gas constant = 287 [J/(kgK)]
T = temperature [K]

Since all variables except the gas mass are constant the ideal gas law can easily be differentiated. The temperature is in fact not constant but it can be set constant since the temperature is known at all times and therefore easily can be put into the equation. According to the simulations made this solution is satisfyingly accurate. By differentiating we get the rate of change in air pressure, which is used as feed back to the pressure regulator. The mass change is calculated as mass flow in minus mass flow out.

$$\dot{m} = \dot{m}_{in} - \dot{m}_{out} \tag{3.5}$$

The differentiation of the ideal gas law now gives us:

$$\dot{P} = \frac{RT}{V}(\dot{m}_{in} - \dot{m}_{out}) \tag{3.6}$$

### 3.2.4 Controlled Vent Unit

The Controlled Vent Unit, CVU, is an important part of the fuel pressurization system. It has the following assignments:

- Ensure that the tanks are ventilated during refueling.
- Keep all tanks except T1 pressurized during flight.
- Keeping T1 pressurized when ordered.
- Protect the tanks against large pressure differences.
- Send out an alert if the pressure is to high or to low.

The CVU is basically working like a switch, it has three positions, All, Partial and Medium. When the CVU is set in position All, it keeps all tanks pressurized by allowing air to flow from the pressure regulator out into the tanks. When it is set in position Partial the CVU cuts off the flow to T1 and thereby all tanks except T1 gets pressurized. Position Medium is used during refueling. When in position Medium the CVU allows all tanks to be ventilated and thus making room for the fuel. The CVU also has two pressure switches, indicating if the pressure is to high or to low, these switches are in the model replaced with pressure sensors in the tanks. In addition to this it has a relief valve that protects the tanks against high pressure differences.

The CVU is in Simulink modelled as a switch with three positions. The relief valve is modelled as an orifice connected to surrounding air pressure.

### 3.2.5 Air ejector

The air ejector is a simple construction with a complicated behavior. Its main task is to feed the CVU with air during pressurization of the tanks. The primary flow from the pressure regulator drives the secondary flow from the ventilation tank. When the air pressure from the regulator is higher than the pressure in the tanks air flows from the regulator through the air ejector, inducing a secondary flow from the vent tank. These airflows then mix and flow through the CVU to the tanks that are to be pressurized, see Figure 3.7 and equation (3.7).

When the air pressure in the tanks is higher than the pressure from the pressure regulator the ejector cuts off the flow from the pressure regulator in order to prevent fuel from entering the pressure regulator. The secondary flow opening stays open at all times, allowing the tanks to ventilate also this way.

$$\mathrm{FlowToCVU} = \mathrm{PrimaryFlow} + \mathrm{SecondaryFlow} \tag{3.7}$$

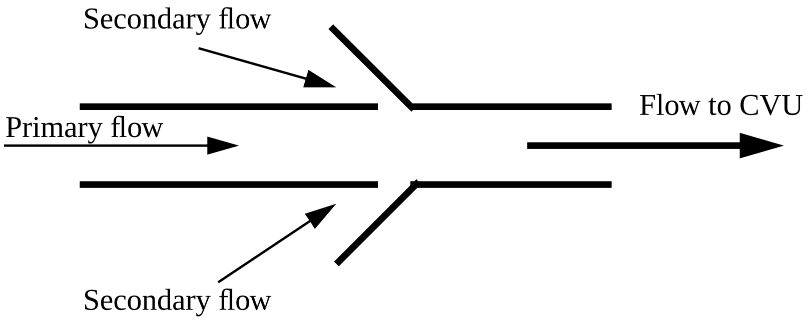


Figure 3.7: Air ejector

The Simulink model of the air ejector is based on the behavior of the ejector rather than on the physical equations describing it. It is modelled as a low pass filter together with a leakage from the tanks, corresponding to the leakage when the pressure regulator is deactivated or the pressure is higher in the fuel tanks than in the pressure regulator.

### 3.2.6 Flame arrestor

The flame arrestor is basically an orifice to ambient air, and it is also modelled like an orifice. It is designed to prevent external fire to spread into the fuel system. That is, the fuel or fuel gases that leak out from the vent pipe might be ignited and the flame arrestor contains a device that prevent the flames to reach the vent tank. Mass flow equation (3.2) is used to calculate the pressure loss out to ambient air.

### 3.2.7 Pressurization system

The two most critical parts of the fuel pressurization system are the pressure regulator and the Controlled Vent Unit, CVU. They control the level of the pressure and also which tanks that are to be pressurized. The pressure regulator and the CVU are also the most complex components in the fuel pressurization system and thus the ones that are hardest to build an accurate model of. Figure 3.8 shows a more detailed figure of the fuel pressurization system, with extra attention paid to the CVU.

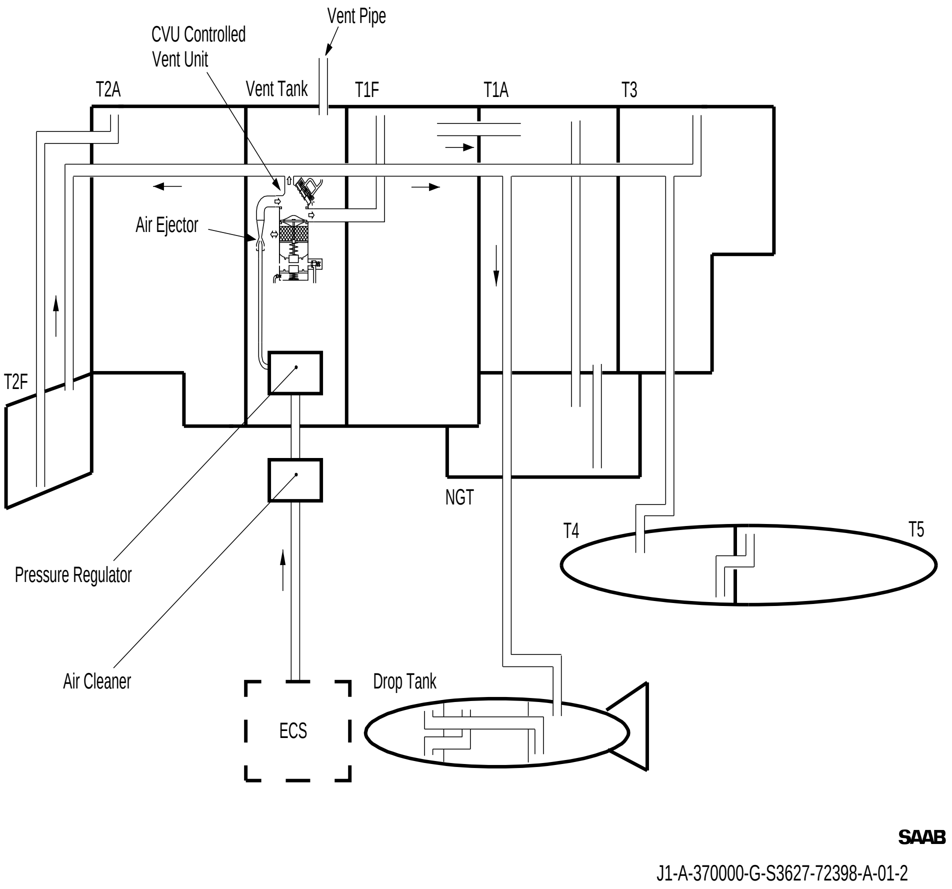


Figure 3.8: Function of the Controlled Vent Unit

Chapter 4

# Tank pressurization diagnosis

In this chapter, the diagnosis system for the tank pressurization is described. All residuals are presented together with the decision structure that makes fault isolation possible. Each fault mode is tested against the Easy5 model and presented together with their thresholds. First a general solution is presented and then the system will be limited to the number of sensors most likely to be added, and the use of model-based diagnosis in this case is also discussed. In this chapter only the theoretical behavior of the system is discussed, the validated system is discussed in Chapter 5.

## 4.1 Fault categories

The combat fighter Gripen has been flying for over ten years and during this time statistics over all faults that have occurred have been gathered and saved in order to continuously improve the system. This statistics is unfortunately not public. Therefore the following discussion has been made. The tank pressurization system has been chosen for testing active diagnosis since it is rather limited and contains one complex moving part, the so called CVU. The faults that can occur can be divided into four categories, **moving parts**, **sensors**, **solid objects** and **functionality**.

As for all systems some components are more error prone than other. In general, **moving parts**, such as valves, have shown to be error prone. Some **sensors,** like pressure sensors based on a thin membrane can be sensitive. Sensors that are exposed to high temperatures, vibration, i.e. can also be unreliable. Sensors some times also have the possibility to diagnose themselves and in those cases the diagnosis system can be made much more reliable. As mentioned earlier pipes, tanks and other **solid** objects are not very likely to fail. Sometimes **functionality faults** can be treated the same way as component faults. In the case of tank pressurization the incoming pressure is important to monitor. If this pressure is too low the entire diagnosis system will be uncertain since it is designed with a lower limit for incoming pressure.

## 4.2 Fault modes

In this section the 15 fault modes found in the tank pressurization system are presented. The two fault modes leakage and blocking has been set as only two fault modes, although there are many places where a pipe can leak or be blocked. This is done in order to limit the size of the decision structure, if a fault can be isolated as a leakage it is left up to the mechanic to find out where the leakage is. In all diagnosis systems there is also the state in which the system is supposed to be, the no fault state.

Below the faults considered are listed.

**Moving parts**

Fault 1: Pressure regulator failing.
Fault 2: Controlled Vent Unit failing.

**Sensors**

Fault 3: Pressure sensor in tank T1 failing, ($P_{T1}$).
Fault 4: Pressure sensor in tank Rest failing, ($P_{Rest}$).
Fault 5: Pressure sensor in ambient air failing, ($P_{Atmosphere}$).
Fault 6: Pressure sensor in the ECS system failing, ($P_{ECS}$).
Fault 7: Temperature sensor failing, (T).
Fault 8: Volume sensor in tank T1 failing, ($V_{T1}$).
Fault 9: Volume sensor in tank Rest failing, ($V_{Rest}$).
Fault 10: Position sensor for pressure regulator failing, (A).
Fault 11: Position sensor for Controlled Vent Unit failing, ($CVU_{Measured}$).

### Solid objects

Fault 12: Leakage.
Fault 13: Blocking.

### Functionality

Fault 14: Low pressure from Environmental Control System.
Fault 15: No Fault, referred to as NF.

Most of the faults are modelled in the same way and therefore it might be in place to once again present the most general way of modelling a fault, which also is the model that is generally used in this thesis, equation (2.1).

$$y_{obs}(t) = y_{corr}(t) + f(t)$$

This means that the observed value equals the correct value plus a fault signal. In the fault free case the fault signal equals zero.

Below the fault modes and their different ways of failing are presented.

### 4.2.1 Pressure regulator and Controlled Vent Unit

The pressure regulator is, as mentioned in section “Pressure regulator” on page 27, modelled as a PI-controller. There are several reasons why the pressure regulator might fail. Since it is supposed to be a controllable device there is of course the possibility of bad connection to the controlling device. There is also the possibility that some internal part is jamming or that the pressure regulator itself jams in some way. The fault where the connection to the controlling unit is failing, i.e. the pressure regulator does not assume the correct mode, active or closed, is modelled with a switch. Regardless of which of the other reasons for the fault it is simulated by adding a constant to the P- or I-values, or by changing the gain, i.e. the maximum area.

Since the Controlled Vent Unit, CVU, is basically working as a switch, all faults are modelled so that the CVU is in the wrong position compared to the one ordered by the controlling system. It is also possible for the CVU to get stuck between these positions and this fault mode is simulated by changing the outlet areas from the CVU.

### 4.2.2 Sensors

Sensors can break in different ways, but it is hard to know exactly how they will fail in every single case so the general fault model from equation (2.1) is used. Bias faults were simulated by adding a constant value to the values from the Easy5 model, to simulate a sensor that breaks a random signal was added.

### 4.2.3 Leakage and Blocking

All leakages are simulated with a new orifice leading to ambient air, with a variable area. Also in this case the fault model from equation (2.1) was used. When a pipe is blocked it is simulated by changing the pipe areas, i.e. equation (2.1) was used again.

### 4.2.4 Low ECS pressure

Low pressure from the ECS was simulated simply by using a small input signal. The model worked also under these circumstances but it is a fault case since the airplane does not meet the requirement stated in the specification if the input pressure is too low.

## 4.3 Diagnosis system

The diagnosis system that has been implemented for the tank pressurization system is based on a number of fictive sensors. This way eleven test quantities are produced and from these the ones that are possible to realize are selected. Each test quantity is described in detail below. For each test quantity a fault that excites that specific quantity is simulated and the thresholded result is presented. The thresholds are dashed and the measured signal solid, except when the measured value is compared to a constant level when both the constant level and the measured signal are solid. Each test quantity is also described mathematically. In order to get as much information as possible from the presented results different faults are used to excite the residuals when possible. Since it is possible to excite the system and thus perform active diagnosis, the residuals depend on the ordered position for the pressure regulator and the CVU.

The diagnosis system was tested during three different working conditions, pressure regulator **active** with CVU in position **All**, pressure regulator **passive** with CVU in position **All**, and pressure regulator **active** with CVU in position **Partial**. The fourth possible combination, pressure regulator **passive**, CVU in position **Partia**l, was also considered but did not contribute with any additional residual.

### 4.3.1 CVU in position All, regulator active

When the pressure regulator is set in position active and the CVU in position all, the following six residuals can be calculated.

**ECS pressure check**

Since the pressure level delivered by the ECS is critical for the tank pressurization it is important to supervise. This relation is an example of traditional limit checking where the measured values are compared with a predefined limit. If the measured value is below the limit an alarm is generated.

The residual is calculated as:

$$R_1 = P_{ECSmeasured} - P_{limit} \tag{4.1}$$

The limit is set to 200 kPa over ambient pressure. The residual $R_1$ is used to test the hypothesis $H_1^0$:

$H_1^0;F_p \in \{NF, F_1, F_2, F_3, F_4, F_5, F_7, F_8, F_9, F_{10}, F_{11}, F_{12}, F_{13}\}$

$H_1^1;F_p \in \{F_6, F_{14}\}$

This means that $R_1$ is sensitive for low pressure into the system or if the pressure sensor for ECS is failing. In order to determine which faults that effect a certain residual the residual itself is studied. All sensor signals in the residual must naturally affect its behavior. If there are any physical relations in the residual, containing variables of some kind, one must also consider whether these might effect the residual if one of them changes. Physical constants like the molar gas constant, etc. can of course not change their values and thus do not effect the residual in any other way than participating in the equations. In this case the only things that affect the residual are the sensor signal and the physical behavior of the ECS. so the residual is sensitive for fault modes $F_6$ and $F_{14}$. In Figure 4.1 an input signal that initially is under the threshold is shown. Observe that it is during the initial 50 seconds that the residual in this case would signal fault, after 50 seconds the pressure rises above the threshold.

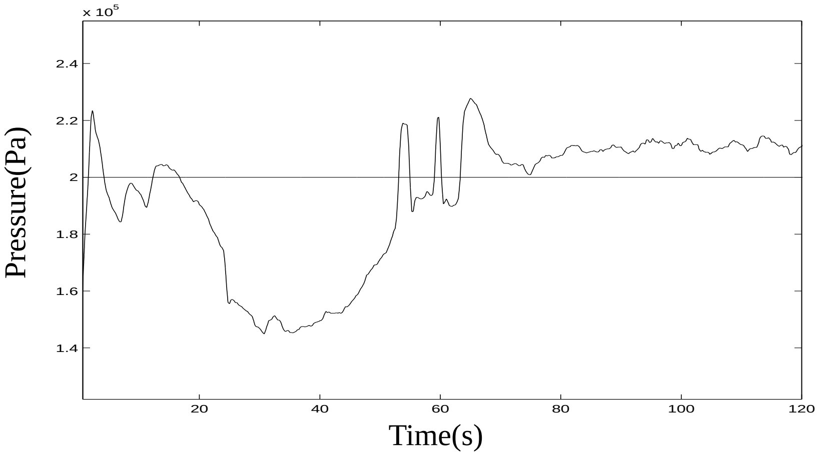


Figure 4.1: Thresholded input pressure

It is important to remember that even if $H_1^0$ is not rejected the fault modes in $H_1^1$ are not excluded as possible faults. This is due to the nomenclature presented in chapter 2, where the *don't care* symbol X was introduced. Since X is used in the decision structure it is not possible to say that since the null hypothesis was not rejected it is true, one must instead draw the conclusion that since the null hypothesis was not rejected all fault modes are possible, including NF. The decisions corresponding to hypothesis test $H_1$ are presented below.

$S_1 = \Omega$ if $H_1^0$ is not rejected.

$S_1 = \{F_6, F_{14}\}$ if $H_1^0$ is rejected.

**Pressure check Tank 1, (T1)**

Between the pressure sensor for ECS and the pressure sensor in tank T1 there are many components, among these the pressure regulator and the CVU, both with moving parts and thus error prone. The pressure in tank T1 is simulated in the fault free case and then compared with the measured value from the Easy5 model.

$$R_2 = P_{T1} - \frac{T \cdot R}{V} \cdot \int_0^t \frac{A \cdot C}{\sqrt{T}} \sqrt{P_{ECS}^2 - P_{T1}^2}\, dt + P_{Atm} \qquad (4.2)$$

Equation (4.2) uses the nomenclature from equation (3.1) and (3.2).

The residual $R_2$ is used to test the hypothesis $H_2^0$:

$H_2^0$;$F_p \in \{NF, F_4, F_{10}, F_{11}\}$

$H_2^1$;$F_p \in \{F_1, F_2, F_3, F_5, F_6, F_7, F_8, F_9, F_{12}, F_{13}, F_{14}\}$

This means that residual $R_2$ is sensitive to all faults except the sensor signals giving the pressure in tank Rest and the positions for the pressure regulator and the CVU, thus all other sensors or physical relations are embedded in the equation.

This residual is an example of model-based diagnosis, the pressure simulated in **Simulink** is compared with the measured pressure from **EASY-5**. Since model faults are impossible to avoid adaptive thresholds prove very useful. Here the first example of how an adaptive threshold might be used is presented. Adaptive thresholds have previously been presented in“Thresholds” on page 18.

Below in Figure 4.2 is the thresholded pressure in tank T1, the pressure regulator here goes from active to closed after 70 seconds, i.e. one of the regulators fault modes.

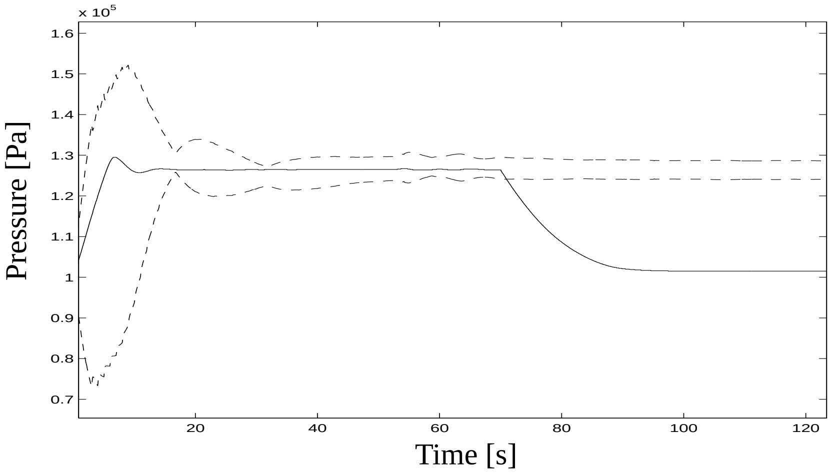


Figure 4.2: Thresholded pressure tank T1

It is clearly shown how the thresholds are more generous in the initial, more dynamic case, and how they get closer to the measured value when the system reaches a region where the model is more accurate. Faults during the dynamic stages are thus harder to detect than faults that occur during steady state. This is a limitation but not as big a limitation as one might think. During dynamic stages of the flight high stress is put on all parts of the aircraft, making sensors less accurate and also making other systems than the diagnosis system go into special modes. It can therefore be discussed whether or not any diagnosis should be performed during these stages or if the diagnosis system should be limited to steady flight, or at least allowed to leave less accurate results during dynamic stages. This also shows the benefits of using adaptive thresholds, the results are relevant during the entire working range if the thresholds are constructed correctly.

### Pressure check Rest

Residual 3 is very similar to residual 2, the pressure difference between the simulated and measured pressure in tank Rest is calculated. The difference between these residuals is only the use of different sensors.

The residual looks like:

$$R_3 = P_{Rest} - \frac{T \cdot R}{V} \cdot \int_0^t \frac{A \cdot C}{\sqrt{T}} \sqrt{P_{ECS}^2 - P_{Rest}^2} dt + P_{Atm} \qquad (4.3)$$

The nomenclature is like before taken from equation (3.1) and (3.2). The residual $R_3$ is used to test the hypothesis $H_3^0$:

$H_3^0; F_p \in \{NF, F_3, F_{10}, F_{11}\}$

$H_3^1; F_p \in \{F_1, F_2, F_4, F_5, F_6, F_7, F_8, F_9, F_{12}, F_{13}, F_{14}\}$

Compared to $R_2$, $R_3$ is sensitive for $F_4$ instead of $F_3$, and apparently not sensitive to $F_2$. The reason why $R_3$ is not sensitive for faults in the CVU is that tank Rest is pressurized both when CVU is in position Partial and in position All. Should the CVU fail in such a way that the passage to tank Rest is blocked in any way this would count as a blocking and not a failing CVU. In Figure 4.4 the thresholded pressure in tank Rest is shown. The solid line shows the measured pressure and the dashed line is the adapted threshold. In this case a sensor fault with the size of

5 kPa was introduced after approximately 50 seconds, causing the measured value to break the threshold shortly afterwards.

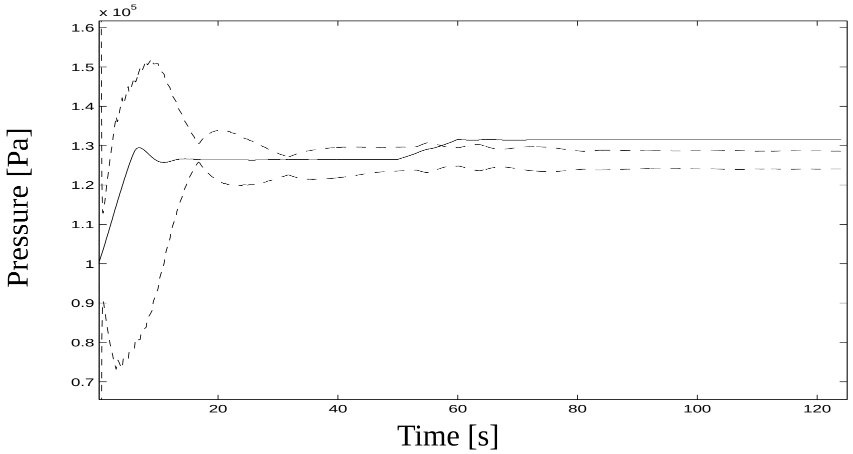


Figure 4.3: Thresholded pressure tank Rest

Since the same model uncertainties are present in this case a similar threshold as for $R_2$ was used. This example also illustrates the need of both an upper and lower threshold, the faults can naturally cause deflections both to higher and lower values.

**Area check**

The regulated area in the pressure regulator can be simulated. This simulation is used when constructing $R_4$. In $R_4$ the simulated area is compared to the measured area. The fact that a regulator is present in the system actually makes diagnosis of the system a lot harder. The regulator has the capacity to hide other faults, like a leakage for example. The only way to get around this problem is to have a residual that actually checks the regulated area.

The residual looks like:

$$R_4 = A_{measured} - A_{simulated} \tag{4.4}$$

The function that describes the simulated area is rather complex, actually more like a small program, so the details of how the area is simulated is left to Appendix B.

The residual $R_4$ is used to test hypothesis $H_4^0$:

$H_4^0$;$F_p \in \{NF, F_2, F_3, F_4, F_{10}, F_{11}\}$

$H_4^1$;$F_p \in \{F_1, F_5, F_6, F_7, F_8, F_9, F_{12}, F_{13}, F_{14}\}$

In Figure 4.4 the thresholded area has been affected by a failing temperature sensor.The size of the fault was large, 1000 K, which was necessary in order to achieve a significant change of the area. The solid line shows the measured area and the dashed line is the threshold.

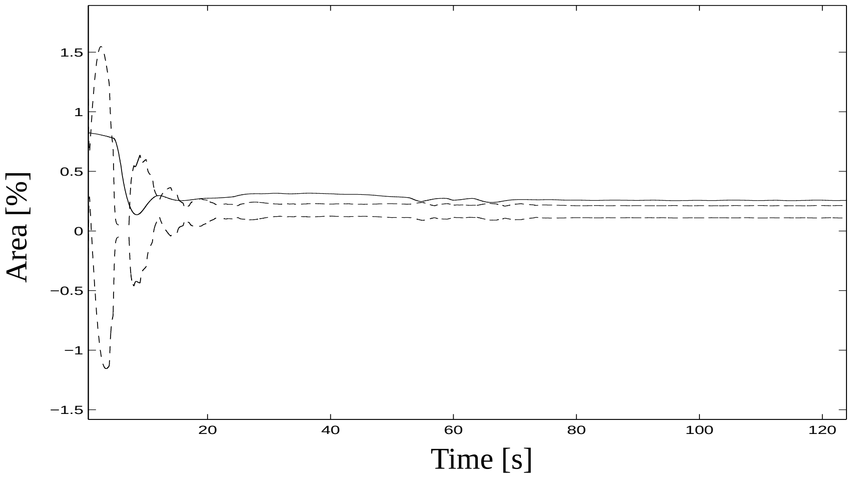


Figure 4.4: Thresholded area

This example also shows an other interesting effect. Since the pressure regulator is controlled with mechanical feedback in the real system, it is not affected by a failing sensor. In this case it is instead the model that is giving the wrong value, since the software model of course is depending on sensors, and the threshold is also generated from the model. The false temperature affects the simulated area but the mechanically controlled area remains correct.

This means that the measured value of the regulating area actually is correct, and that the threshold has been displaced. The residual however still gives the correct result, during the fault free state it is zero and when a fault is present it is non-zero.

**CVU check**

When checking the Controlled Vent Unit the measured position is simply compared with the position that has been ordered by the control system. A measurement sequence where the CVU is ordered in different positions and the positions are measured would reveal any faults.

The residual looks like:

$$R_5 = CVU_{measured} - CVU_{ordered} \tag{4.5}$$

The residual $R_5$ is used to check the hypothesis $H_5^0$.

$H_5^0$;$F_p \in \{NF, F_1, F_3, F_4, F_5, F_6, F_7, F_8, F_9, F_{10}, F_{12}, F_{13}, F_{14}\}$

$H_5^1$;$F_p \in \{F_2, F_{11}\}$

Since the sensors that measure the CVU:s position actually are switches, there will be no uncertainties in the measured values and thus no threshold is necessary. Below a figure where the CVU leaves its position after 50 seconds, the residual is zero in the fault free case and signals one when fault is detected.

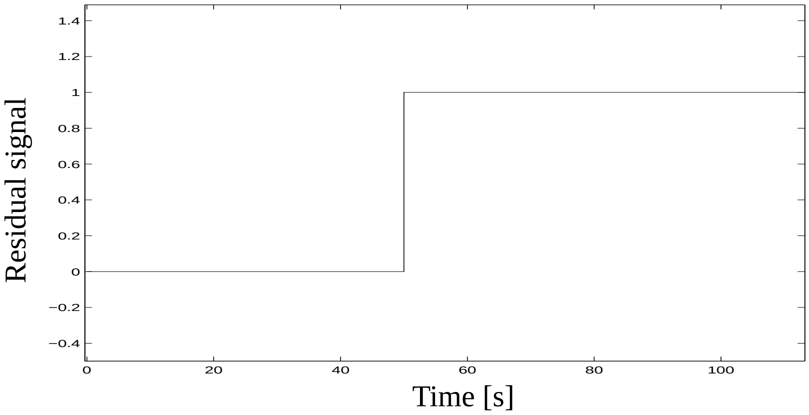


Figure 4.5: CVU residual

When the CVU is checked in this way the system is not in the same state all the time. It is also possible to build one residual for each case but here only this one is presented.

**Pressure check T1, Rest**

When the pressure regulator is active and the CVU in position All, the pressure should be the same in both tank T1 and tank Rest. The measured values in these two tanks are compared and used to form residual $R_6$.

The residual looks like:

$$R_6 = P_{T1} - P_{Rest} \tag{4.6}$$

The residual $R_6$ is used to check the hypothesis $H_6^0$.

$H_6^0;F_p \in \{NF, F_1, F_5, F_6, F_7, F_8, F_9, F_{10}, F_{11}, F_{12}, F_{14}\}$

$H_6^1;F_p \in \{F_2, F_3, F_4, F_{13}\}$

In Figure 4.6 the thresholded pressure in tank Rest is shown. The sensor in tank Rest is here failing after approximately 40 seconds. The size of the sensor fault is 5 kPa.

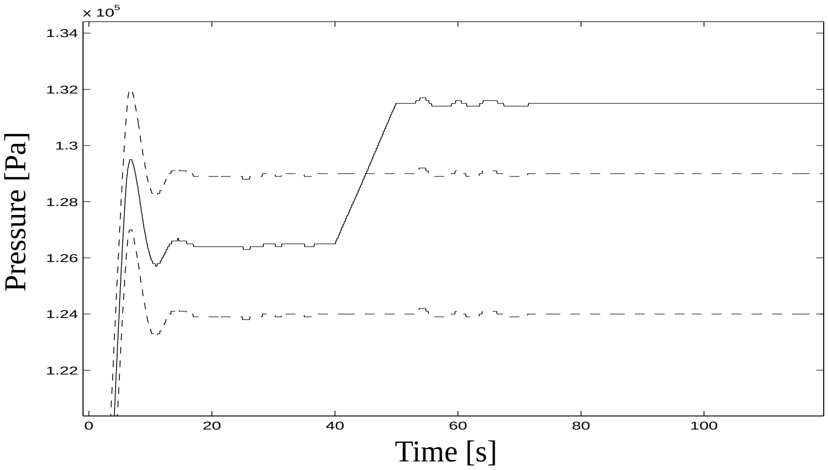


Figure 4.6: Sensor check T1 Rest

By using the values from the sensor in tank T1 to form a threshold, in this case a threshold with constant value, faults can be detected. A constant threshold was chosen this time since the values are supposed to be exactly the same for the two sensors. The reason why the threshold appears to be so close to the measured value during the transient stage is only a visual effect, the threshold is equally large during the entire measurement. If the sensor in tank T1 had failed instead of the sensor in tank Rest it would have been the threshold that had been displaced but the result would have been the same anyway, an alarm would have been generated since the values differ to much.

In Figure 4.7 the thresholded residual is shown instead of the thresholded pressure. It can here be seen how the residual is approximately zero in the fault free case and how the residual clearly deviates from zero and crosses the threshold when a fault is introduced.

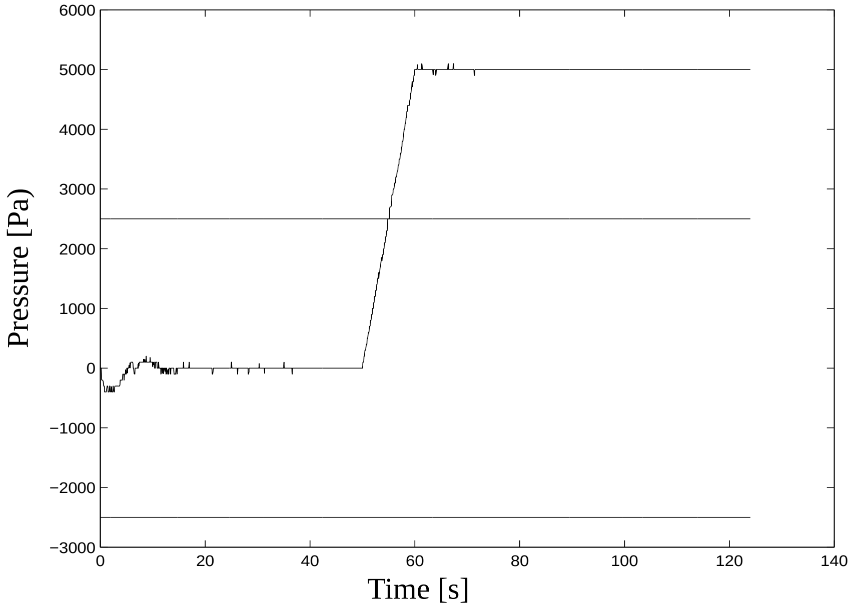


Figure 4.7: Thresholded residual tank Rest

### 4.3.2 CVU in position All, regulator passive

By keeping the CVU in the same position but turning the pressure regulator passive, four of the residuals are possible to use again. Since the working conditions now are different the residuals will be sensitive to an other set of faults. All these residuals are sensor checks, i.e. hardware redundancy or limit checking. It could though be argued that hardware redundancy is the same thing as model-based diagnosis, only that in this case the relationship between the two sensors is one to one.

**Pressure check T1, Rest**

This residual is very similar to the previous one, but since the regulator is passive and all tanks should have atmospheric pressure, faults in the CVU does not affect this residual. This is because even if the CVU should come into the wrong position, i.e. position Partial, the tanks can still be ventilated and thus should still have the same pressure.

The residual looks like:

$$R_7 = P_{T1} - P_{Rest} \tag{4.7}$$

The residual $R_7$ is used to check the hypothesis $H_7^0$.

$H_7^0; F_p \in \{NF, F_1, F_2, F_5, F_6, F_7, F_8, F_9, F_{10}, F_{11}, F_{12}, F_{14}\}$

$H_7^1; F_p \in \{F_3, F_4, F_{13}\}$

The residual is tested by introducing a failing sensor after 50 seconds, as before the size of the fault is 5 kPa. Also in this figure the measured signal is solid while the threshold is dashed.

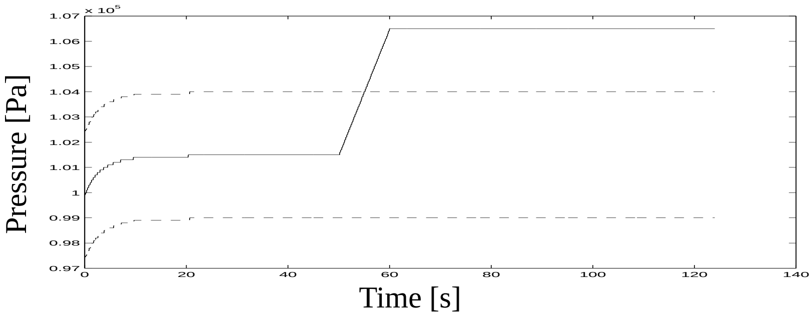


Figure 4.8: Sensor check T1 Rest

The two following residuals are very similar to this one so no figures will be presented for them.

### Pressure check T1, Atmosphere

Since the tanks are supposed to have the same pressure as the ambient air the tank pressure could also be compared with the ambient pressure. This is done in order to form residual $R_8$.

The residual looks like:

$$R_8 = P_{T1} - P_{Atmosphere} \tag{4.8}$$

The residual $R_8$ is used to check the hypothesis $H_8^0$.

$H_8^0; F_p \in \{NF, F_2, F_4, F_6, F_7, F_8, F_9, F_{10}, F_{11}, F_{12}, F_{14}\}$

$H_8^1; F_p \in \{F_1, F_3, F_5, F_{13}\}$

### Pressure check Rest, Atmosphere

The same test can of course also be done for tank Rest, forming residual $R_9$.

The residual looks like:

$$R_9 = P_{Rest} - P_{Atmosphere} \tag{4.9}$$

The residual $R_9$ is used to check the hypothesis $H_9^0$.

$H_9^0; F_p \in \{NF, F_2, F_3, F_6, F_7, F_8, F_9, F_{10}, F_{11}, F_{12}, F_{14}\}$

$H_9^1; F_p \in \{F_1, F_4, F_5, F_{13}\}$

### Area check

Since the pressure regulator is passive the regulated area should be zero. It is possible to form yet another area residual in order to check this. The advantage with this residual compared to the other area check is that here there is no relation to a model, only limit checking. This is thus another example of how to use traditional approaches together with new methods like model-based diagnosis, together they give a better result than they would have if used on their own.

The residual $R_{10}$ looks like:

$$R_{10} = A_{measured} \tag{4.10}$$

The residual $R_{10}$ is used to check the hypothesis $H^0_{10}$.

$H^0_{10}$;$F_p \in \{NF, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_9, F_{11}, F_{12}, F_{13}, F_{14}\}$

$H^1_{10}$;$F_p \in \{F_1, F_{10}\}$

In this case it is not possible to check the residual without a threshold, as when the CVU was checked. The reason why this is impossible is that in the case with the CVU switches were used to measure the position, but the pressure regulator uses an ordinary linear sensor, and therefore there is a risk for sensor disturbances. Below a thresholded fault is presented, the pressure regulator here becomes active after 50 seconds. The constant threshold is dashed and the measured value is solid.

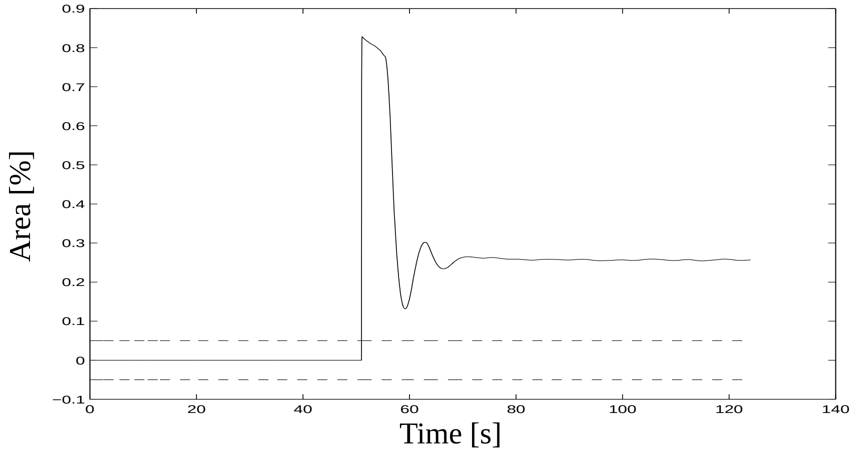


Figure 4.9: Thresholded area

Obviously the failing pressure regulator makes the area go outside its thresholds and thus generating an alarm.

### 4.3.3 CVU in position Part, regulator active

When the CVU is in position Partial, tank Rest is completely cut off from tank T1. This means that the sensor values from tank T1 does not affect $R_3$ like they did before. This means that also these residuals are sensitive to different faults than before.

### Pressure check Rest

The following residual is formed:

$$R_{11} = P_{Rest} - \frac{T \cdot R}{V_{Rest}} \cdot \int_0^t \frac{A \cdot C}{\sqrt{T}} \sqrt{P_{ECS}^2 - P_{Rest}^2} dt + P_{Atm} \tag{4.11}$$

The nomenclature is like before taken from equation (3.1) and (3.2). The difference compared to $R_3$ is that the simulated pressure does not use the volume sensor in tank T1. Since the two tanks are not connected there is no need to use this sensor in order to simulate the pressure in tank Rest. Only the volume sensor in tank Rest is needed.

The residual $R_{11}$ is used to test the hypothesis $H_{11}^0$ :

$H_{11}^0 ; F_p \in \{NF, F_3, F_8, F_{10}, F_{11}\}$

$H_{11}^1 ; F_p \in \{F_1, F_2, F_4, F_5, F_6, F_7, F_9, F_{12}, F_{13}, F_{14}\}$

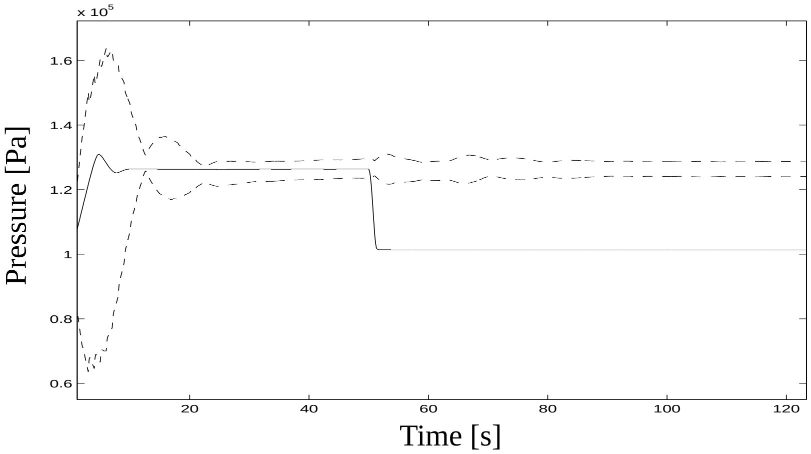


Figure 4.10: Pressure check Rest

Since this residual decouples a sensor that $R_3$ did not decouple it is a good example of how to use active diagnosis in order to receive residuals sensitive to different faults. In Figure 4.10 the thresholded pressure in tank Rest is shown. As earlier the threshold is dashed and the measured value is solid. After approximately 50 seconds a leakage occurs in tank Rest and the pressure drops to a level close to ambient air pressure, clearly outside the thresholds.

## 4.4 Decision structure

The hypothesis tests presented in the previous section can be used to form a decision structure. At first the full decision structure will be presented, then a smaller, for the Gripen project more relevant, decision structure will be derived.

In Table 3 the full decision structure is presented. $R_1$ to $R_6$ are received when the pressure regulator is **active** and the CVU in position **All**, residuals $R_7$ to $R_{10}$ are received when the pressure regulator is **passive** and CVU in position **All**. Residual $R_{11}$ is received when the pressure regulator is **active** and CVU in position **Partial**.

Table 3: Decision structure

| | $F_1$ | $F_2$ | $F_3$ | $F_4$ | $F_5$ | $F_6$ | $F_7$ | $F_8$ | $F_9$ | $F_{10}$ | $F_{11}$ | $F_{12}$ | $F_{13}$ | $F_{14}$ | NF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $R_1$ | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 |
| $R_2$ | X | X | X | 0 | X | X | X | X | X | 0 | 0 | X | X | X | 0 |
| $R_3$ | X | X | 0 | X | X | X | X | X | X | 0 | 0 | X | X | X | 0 |
| $R_4$ | X | 0 | 0 | 0 | X | X | X | X | X | 0 | 0 | X | X | X | 0 |
| $R_5$ | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 | 0 | 0 |
| $R_6$ | 0 | X | X | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_7$ | 0 | 0 | X | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_8$ | X | 0 | X | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_9$ | X | 0 | 0 | X | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_{10}$ | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 | 0 | 0 | 0 |
| $R_{11}$ | X | X | 0 | X | X | X | X | 0 | X | 0 | 0 | X | X | X | 0 |

As mentioned earlier in chapter 2 a “X” means that the fault might affect the residual and a “0” means that the fault can not affect the residual. This means that if a residual reacts where the fault has a “0” in the column that fault can not be the reason why the residual is failing. With a good model and cleverly chosen thresholds and measurement areas, together with the initial statement that only single faults are considered it is possible to change most of the X:s into 1:s. This would mean that if a fault occurs all residuals with an X in that column should react.

It is of course impossible to say that the X:s could always be exchanged to 1:s, but together with experiments it is possible to get an idea of how likely it is. Experiments have shown that in steady state the model is very accurate and that the residuals react even to very small faults, more about the model verification further on. With this in mind the decision structure can be studied and used to give a very likely diagnosis, in order to help the mechanics to repair, or to inform the pilot of any hazardous faults. When working as expected the residual should react to the X:s.

When the decision structure is studied, one can see that the column for $F_6$ is equal to the column for $F_{14}$, and that the column for $F_7$, $F_9$ and $F_{12}$ also are equal. This means that the faults within these two groups are impossible to isolate with this set of test quantities. That some faults are present can though be detected, as well as which group of faults that should be investigated further. This is very important since there might be test data or information about the components history which indicates which of the faults in one of the groups that is most likely to have occurred. Together with the diagnosis system this information gives the mechanic a good starting point for isolating and repairing the fault.

As can be seen in the decision structure active diagnosis significantly improves the capability to detect and isolate faults. Without the possibility to use active diagnosis no more than seven residuals would have been possible to construct, ($R_1$, $R_2$, $R_3$, $R_4$, $R_5$, $R_6$, $R_{11}$), but since several different working conditions can be used the decision structure can be made larger. Without active diagnosis $F_{10}$ would have been impossible to detect. $F_1$ and $F_5$ would form a group with $F_7$, $F_9$ and $F_{12}$ and would thus be impossible to isolate. With active diagnosis both $F_1$ and $F_5$ are possible to isolate. If the system had been running under these different conditions without interference from the diagnosis system, active diagnosis would not have been necessary.

The two most important components, the pressure regulator and the CVU are both possible to isolate when using active diagnosis. In Chapter 5 the diagnosis system will be validated and there the performance of the diagnosis system built in this thesis will be presented.

## 4.5 Limited diagnosis system

The diagnosis system in the previous sections is an example of how a diagnosis system could be designed in general. The specific tank pressurization system in Jas 39 Gripen does however not have all these sensors, in the following section a more limited diagnosis system will be presented. The sensors that already exist will be used and some sensors will also be added, sensors that are likely to be included if the system is to be upgraded in the future.

The system is also not quite as controllable as have been assumed in the previous sections. The CVU uses the fuel pressure in order to change its position, this means that the fuel pump has to be running in order for the CVU to change its position. In the following section it is first assumed that the diagnosis system is used when no fuel pressure is available and then with fuel pressure available. When no fuel pressure is available the CVU is in position All.

### 4.5.1 Current sensors

The sensors that already exist in the tank pressurization system are:

- Temperature sensor
- Volume sensor in tank T1
- Volume sensor in tank Rest
- Pressure sensor in ambient air
- Position switch for CVU

With these sensors only residual $R_5$ is possible to construct. More sensors have to be added in order to build a model-based diagnosis system.

### 4.5.2 Added sensors

The sensor that is absolutely most critical for the model-based diagnosis system is the sensor measuring the pressure from the ECS. Since this signal is used as an input signal to the diagnosis system almost all residuals are impossible to build without this sensor.

In order to set up any pressure relation it is necessary with more than just one sensor, the pressure sensors in tank T1 and tank Rest have therefore also been added. These three sensors are used together with the already existing ones in order to design a new model-based diagnosis system for the tank pressurization.

### 4.5.3 Decision structure 2

When inspecting the residuals in section 4.3 the following residuals are possible to construct with the limited set of sensors and without fuel pressure:

- Residual $R_1$
- Residual $R_2$
- Residual $R_3$
- Residual $R_5$
- Residual $R_6$
- Residual $R_7$
- Residual $R_8$
- Residual $R_9$

When the CVU only can be set in position All, the only information these residuals can give about the CVU is that it is not in position Partial when it is supposed to be in position All. Nothing can be said about what position the CVU is in when it is supposed to be in position Partial.

When fuel pressure is available also residual $R_{11}$ is possible to construct.

Thus we get the following decision structure:

Table 4: Limited decision structure

| | $F_1$ | $F_2$ | $F_3$ | $F_4$ | $F_5$ | $F_6$ | $F_7$ | $F_8$ | $F_9$ | $F_{11}$ | $F_{12}$ | $F_{13}$ | $F_{14}$ | NF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $R_1$ | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 |
| $R_2$ | X | X | X | 0 | X | X | X | X | X | 0 | X | X | X | 0 |
| $R_3$ | X | X | 0 | X | X | X | X | X | X | 0 | X | X | X | 0 |
| $R_5$ | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 | 0 | 0 |
| $R_6$ | 0 | X | X | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_7$ | 0 | 0 | X | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_8$ | X | 0 | X | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_9$ | X | 0 | 0 | X | X | 0 | 0 | 0 | 0 | 0 | 0 | X | 0 | 0 |
| $R_{11}$ | X | X | 0 | X | X | X | X | 0 | X | 0 | X | X | X | 0 |

When observing this decision structure it is clear that a couple of groups can be formed but also that some of the faults are possible to isolate. The column for $F_1$ is equal to the column for $F_5$, these faults can therefore not be isolated more than to a group of faults. The column for $F_6$ is equal to the column for $F_{14}$ so also these two faults form a group. The third group consists of the columns for $F_7$,$F_8$, $F_9$ and $F_{12}$. All of the other faults can be directly isolated. It is also clear that when adding the possibility to change the position of the CVU also $F_8$ can be isolated. As mentioned above more information about the CVU also can be gathered. When the CVU:s position can be changed the fault mode where the CVU stands in position All but is ordered to position Partial can be revealed. Thus, without this possibility all information about the CVU can not be gathered, only that it does not stand in the wrong position when ordered to position All is revealed.

Without the possibility to use active diagnosis but with fuel pressure, $F_1$, $F_5$, $F_7$, $F_9$ and $F_{12}$ would form one large group. $F_6$ would like before be equal to $F_{14}$ and the rest of the faults would be unique. Also in this case active diagnosis improves the diagnosis capability.

## Chapter 5

# Verification

In this chapter the diagnosis system is validated and the results obtained are presented. Some of the faults are presented together with the residuals behavior, a complete presentation of the faults with the residuals behavior is given in Appendix A. It is shown that the system is not behaving exactly according to the theory. At the end of this chapter methods to improve the system in order to make it perform according to the theory are discussed.

There are a number of factors that affects the ability of the diagnosis system to detect and isolate faults. The most important one is the model itself, in order to use a model for model-based diagnosis the model has to be accurate at least under the circumstances that the diagnosis system is supposed to work. It is also important that the thresholds are well adapted to the model faults so that there are few false alarms and so that even small faults can be detected. The residuals and decision structure also have to be correct, otherwise there is a risk of isolating the wrong components.

Since this master thesis uses a “model of a model” to build the diagnosis system the focus has not been on optimizing neither the model nor the thresholds. The main objective was to exemplify the principles of model-based diagnosis, not to build an optimal diagnosis system for the model.

The diagnosis model is however rather accurate and the thresholds are well adapted, although not optimal. Below Figure 5.1 is showing how well the diagnosis model follows the Easy5 model.

As can be seen in Figure 5.1 the Simulink model is very accurate at steady state while during the dynamic phase it differs a lot from the Easy5 model. This behavior is rather typical, usually it is easier to build a model that is accurate during steady state than during the dynamic phase. This is also when adaptive thresholds prove to be most useful.

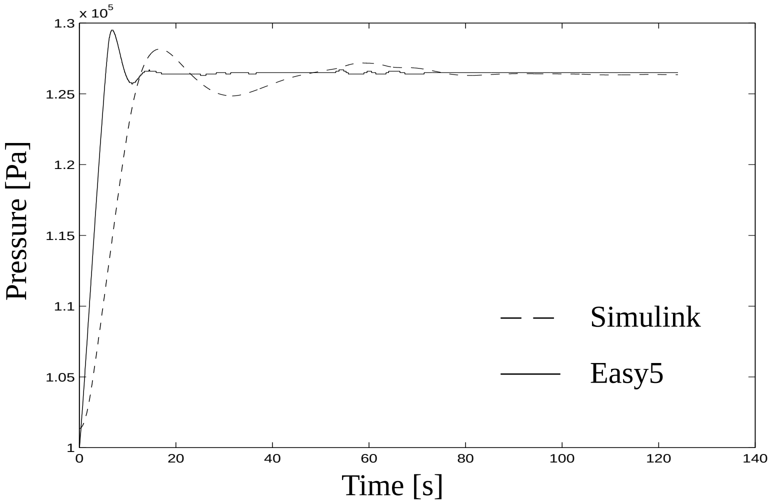


Figure 5.1: Validation of Simulink model

In the following section the decision structure that the diagnosis system actually delivered when the system was provoked with the different fault modes will be presented. Some of the faults will be presented together with the residuals that react to that particular fault, this in order to validate that the decision structure is working in practice as well as in theory, and if not, to explain why the system is not working as expected. The decisions taken by the diagnosis system are however taken with help of the decision structure in Table 3. This since although some residuals are not working as expected it is not possible to say that this is always the case, only one test was performed and the diagnosis system might be valid under other working conditions.

## 5.1 Achieved Decision structure

The decision structure achieved when running the system with faults added is presented in Table 5.

Table 5: Achieved decision structure

| | $F_1$ | $F_2$ | $F_3$ | $F_4$ | $F_5$ | $F_6$ | $F_7$ | $F_8$ | $F_9$ | $F_{10}$ | $F_{11}$ | $F_{12}$ | $F_{13}$ | $F_{14}$ | NF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $R_1$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| $R_2$ | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| $R_3$ | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| $R_4$ | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| $R_5$ | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $R_6$ | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $R_7$ | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $R_8$ | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $R_9$ | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $R_{10}$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| $R_{11}$ | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |

When comparing this decision structure with the decision structure in Table 3 it is clear that the diagnosis system does not behave as expected. The five first faults can be detected and isolated just as in Table 3 and $F_6$ forms a group with $F_{14}$. When $F_7$ occurs only residual $R_4$ reacts, giving an inconclusive answer. The diagnosis system does not react at all for fault modes $F_8$ and $F_9$, indicating No Fault. The rest of the fault modes give the expected results.

The diagnosis system is obviously not working as well as might be expected from a theoretical viewpoint. It is however still useful. The faults that give unexpected results are presented below together with an explanation to why the system does not behave as expected.

### Fault 1: Pressure regulator failing

In Figure 5.2 the pressure regulator is turning passive after 60 seconds. Obviously all residuals react the way they are supposed to, some are zero and some indicate fault. The diagnosis statement is:

Diagnosis statement: $S_1;F_p \in \{F_1\}$

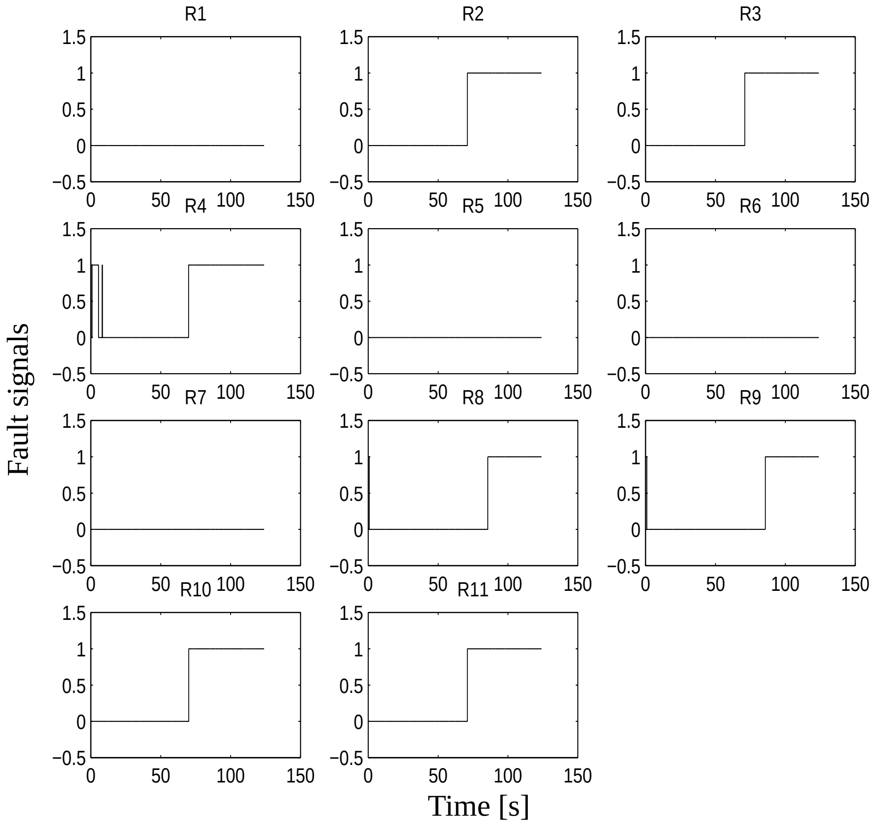


Figure 5.2: Residual reactions to $F_1$

### Fault 7: Temperature sensor failing

Figure 5.3 shows the results of a failing temperature sensor. In this case residuals $R_2$, $R_3$ and $R_{11}$ are not reacting as expected. The reason why they are not giving the correct result is the pressure regulator. In these three cases the pressure regulator is “hiding” the fault, since the pressure regulator is controlled directly by the pressure difference, the pressure in the tanks are correct anyway. Only initially are the residuals reacting as they should. This means that a failing temperature sensor might be hard to isolate, but an experienced mechanician could perhaps anyway draw the correct conclusion by inspecting the fault signals, an automatic system would though be hard to build. The rest of the residuals are reacting as expected and the diagnosis statement is:

Diagnosis statement: $S_7$;$F_p \in \{F_1, F_5, F_6, F_7, F_8, F_9, F_{12}, F_{13}, F_{14}\}$

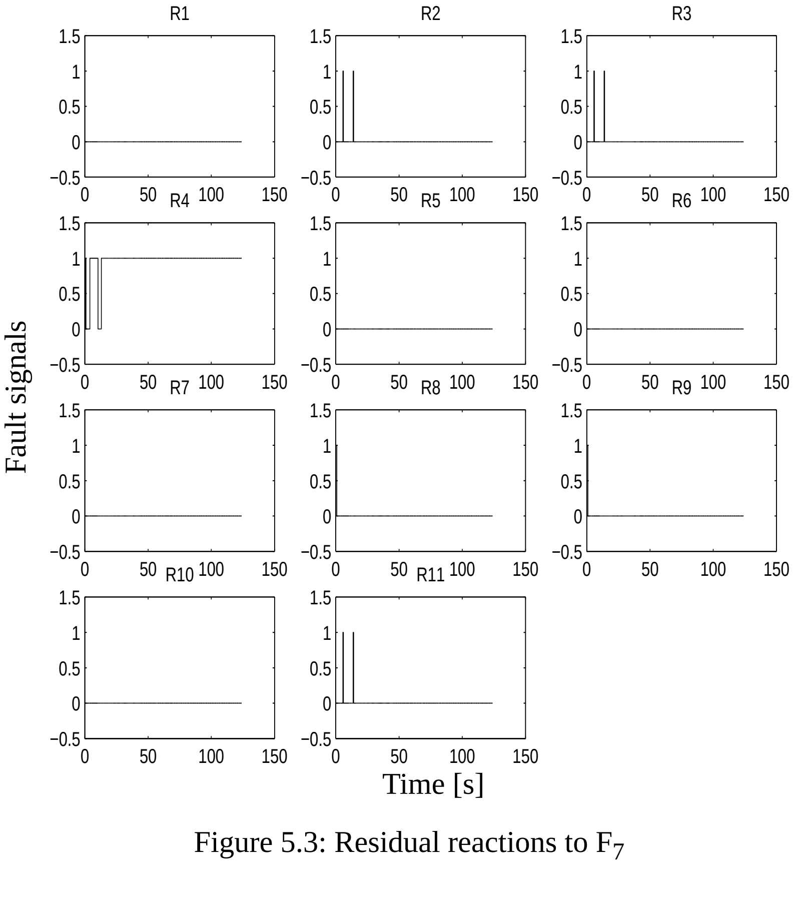


Figure 5.3: Residual reactions to $F_7$

### Fault 8: Volume sensor in tank T1 failing

The residual signals when the volume sensor in tank T1 is failing are presented in Figure 5.4. Just as in the case with the failing temperature sensor the pressure regulator is hiding this fault. This means that also this fault might be very hard to isolate, or even to detect. With a better model and better thresholds, large faults might still be possible to detect and isolate but small faults will still be hard to both detect and isolate. In this case the diagnosis statement is:

Diagnosis statement: $S_8;F_p \in \{NF\}$

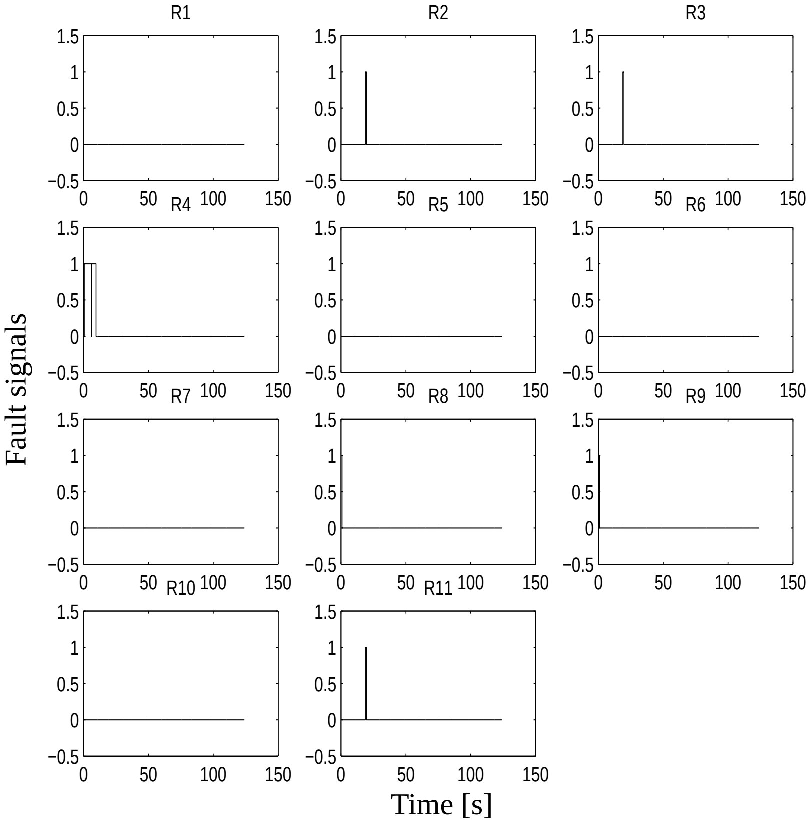


Figure 5.4: Residual reactions to $F_8$

### Fault 9: Volume sensor in tank Rest failing

When the volume sensor in tank Rest is failing the residual signals in Figure 5.5 are received. Just as for a failing volume sensor in tank T1 the residuals are not responding the way that they would have if the pressure regulator was not hiding the pressure fault. The diagnosis statement is:

Diagnosis statement: $S_9;F_p \in \{NF\}$

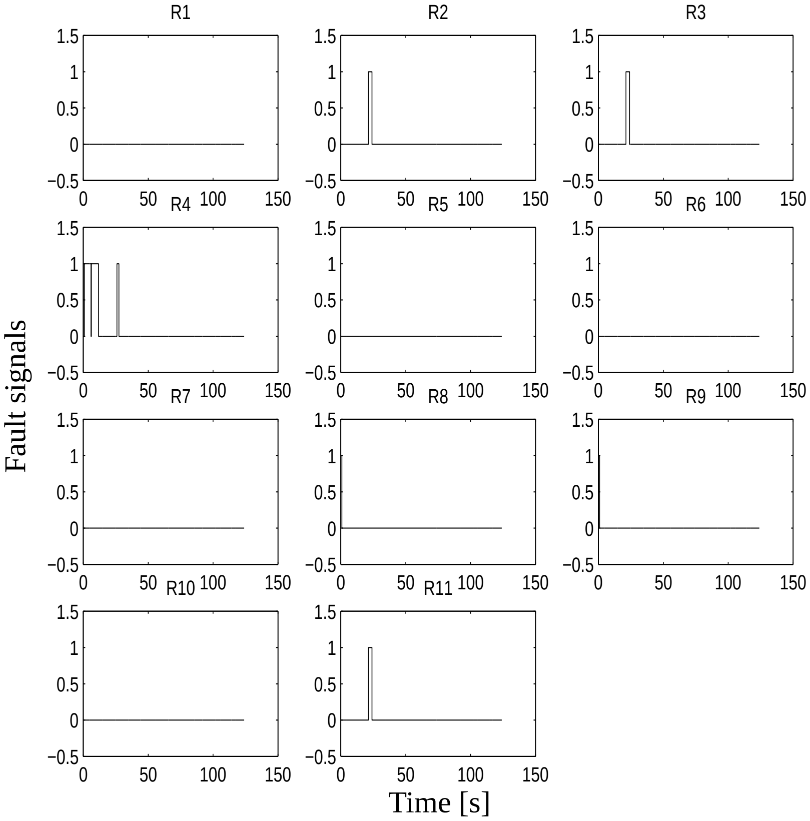


Figure 5.5: Residual reactions to $F_9$

## 5.2 Validation conclusions

In the previous section the reaction of the system to some of the possible faults were presented. Overall the system behaved as it was supposed to but it was also clear that some of the sensor signals would be hard to detect and isolate. This problem can be resolved by using self diagnosing sensors. Self diagnosing sensors use a test signal to check whether or not they are functioning. If self diagnosing sensors were used and the results from those checks were added to the decision structure all faults would be possible to detect and isolate. The way the system is currently designed fault $F_6$ and $F_{14}$ would be hard to differ from each other. $F_7$ gives a result in which $F_1$, $F_5$, $F_6$, $F_7$, $F_8$, $F_9$, $F_{12}$, $F_{13}$ and $F_{14}$ are pointed out as possible faults.$F_8$ and $F_9$ are impossible to detect, the diagnosis system actually indicates No Fault in these two cases. This might seem very limiting but all these fault modes are non critical for the pressurization and also rather unlikely to appear. As mentioned earlier the problem could also be helped with an extended diagnosis system. The two most important faults, $F_1$ and $F_2$ are however possible to both detect and isolate so the diagnosis system still proves useful.

# Chapter 6

# Conclusions

The objective with this thesis is to investigate the potential of model-based diagnosis in combination with active diagnosis. The diagnosis system is exemplified on the fuel pressurization system on JAS 39 Gripen. In order to do this a model of the fuel pressurization system in **EASY-5** is used as the real system and a diagnosis system is built in **Simulink**. The number of faults that can be detected and isolated is investigated under different assumptions. The use of active diagnosis is shown and a number of necessary sensors are pointed out.

## 6.1 Discussion

### 6.1.1 General approach

In order do design a diagnosis system much knowledge about the system itself have to be gathered. The history of the system has to be studied in order to find out which faults are most common and which faults that are most critical for the performance of the system. Studies of old fault reports and interviews with engineers who have the “silent knowledge” about the system are necessary if a good diagnosis system is to be designed.

The design of the model used in the model-based diagnosis system is critical and much effort should be put into making a satisfying model. If the diagnosis system is to be used in real time the processing time also have to be considered and the model might have to be simplified in order to keep the time constraints.

When designing the test quantities much effort should be put into examining the system in order to find all possible faults. If it is possible to simulate the process the test quantities should be tested before the decision structure is designed in order to make sure that they are performing as expected.

### 6.1.2 Diagnosis system for the fuel pressurization

With the sensors available in the fuel pressurization system today it is not possible to build an accurate model-based diagnosis system. At least three new sensors have to be added, one sensor measuring the pressure into the system, and two sensors, measuring the pressure fall over the CVU. With these sensors a limited diagnosis system can be built. The most important fault modes, the pressure regulator and the CVU, ($F_1$, $F_2$), can be detected and $F_2$ can also be isolated using these sensors. When adding the possibility to use active diagnosis, $F_1$ can also be isolated.

The best results are possible to achieve when adding a fourth sensor, measuring the position of the pressure regulator. The fourth sensor does not improve the system without using active diagnosis, actually additional fault modes are added, increasing the complexity of the system. However, when combining this fourth sensor with the possibility to use active diagnosis all faults can be detected and isolated completely or to a group of no more than three possible fault modes.

When testing the diagnosis system the theoretical results were not quite achieved. The most important fault modes could still be both detected and isolated but faults affecting the temperature sensor and the two volume sensors ($F_7$, $F_8$, $F_9$), were found to be hard to isolate or even to detect. The reasons why the system did not work as well in practice as in theory is analyzed in Chapter 5. The diagnosis system is however also with these limitations very useful since faults affecting all moving parts can be detected and isolated.

The use of active diagnosis in combination with model-based diagnosis obviously improves the capacity to both detect and isolate faults. When few sensors are available active diagnosis can be used to increase the size of the decision structure and thereby making the diagnosis system perform significantly better.

## 6.2 Future Work

Should a diagnosis system like the one suggested in this thesis ever be implemented in JAS 39 Gripen or any another airplane manufactured by Saab AB there is still much work to be done. From this thesis the principles to design a model-based diagnosis system and how to use active diagnosis to make it more efficient can be used. Since the diagnosis system in this report have been designed to fit a model of the aircraft, all parameters have to be redesigned and tested against the aircraft in question.

The diagnosis system presented here is also calculated in continuos time plane and if it is to be implemented it has to be redesigned to work in discrete time. Some of the components in the diagnosis model might have to be simplified or redesigned in order to cut the computation time since the computers in the airplane most likely are not as powerful as the ones used in this thesis. The system has to run in real time which can be complicated for nonlinear complex systems.

The possibilities to add the sensors have not been investigated here, but at least three new sensors are necessary to add in order for the diagnosis system to perform well.

It would be very interesting to investigate the possibility to implement this system in real time and to redesign the model used in the diagnosis system in order to cut the computation time.

It would also be of interest to further investigate the potential of using self diagnosing sensors in order to increase the decision structure and improve the capacity to detect and isolate faults.

## References

[1] Frisk E, Dissertation: *Residual Generation for Fault Diagnosis*, Linköpings tekniska högskola, No. 716

[2] Glad T, Ljung L, *Reglerteknik Grundläggande teori*, Studentlitteratur 1989

[3] Glad T, Ljung L, *Reglerteori*, Studentlitteratur 1997

[4] Glad T, Ljung L, *Modellbygge och simulering*, Studentlitteratur 1991

[5] Gustafson F, Ljung L, Millnert M, *Signalbehandling*, Studentlitteratur 2000

[6] Karlsson J, Master thesis: *Diagnosis of the air distribution system of the JAS39 Gripen environmental control system*, Linköpings tekniska högskola, LiTH-ISY-EX-3092

[7] Nilsson J, Master thesis: *Diagnosis on a principal environmental control system*, Linköpings tekniska högskola, LiTH-ISY-EX-3148

[8] Nyberg M, Frisk E, *Diagnosis and Supervision of technical Processes*, Linköpings tekniska högskola (course literature)

# Appendix A

## Verification

In this appendix all results from the verification will be presented together with a short explanation of the results and the diagnosis statement taken by the diagnosis system.

The diagnosis system did not perform according to the theoretical assumptions and possible explanations of the behavior for each residual are presented here.

The conclusions of the verification tests are presented in Chapter 5.

### Fault 0: No Fault, (NF)

When no faults are present none of the residuals should react, as can be seen in Figure 1 all fault signals are zero, that is, no measured signal leaves its thresholded area and thus no fault signal is generated. This is the first indication that the residuals are correctly designed, at least they fulfill the first requirement. The diagnosis in this case is:

Diagnosis statement: $S_{15}$;$F_p \in \{NF\}$

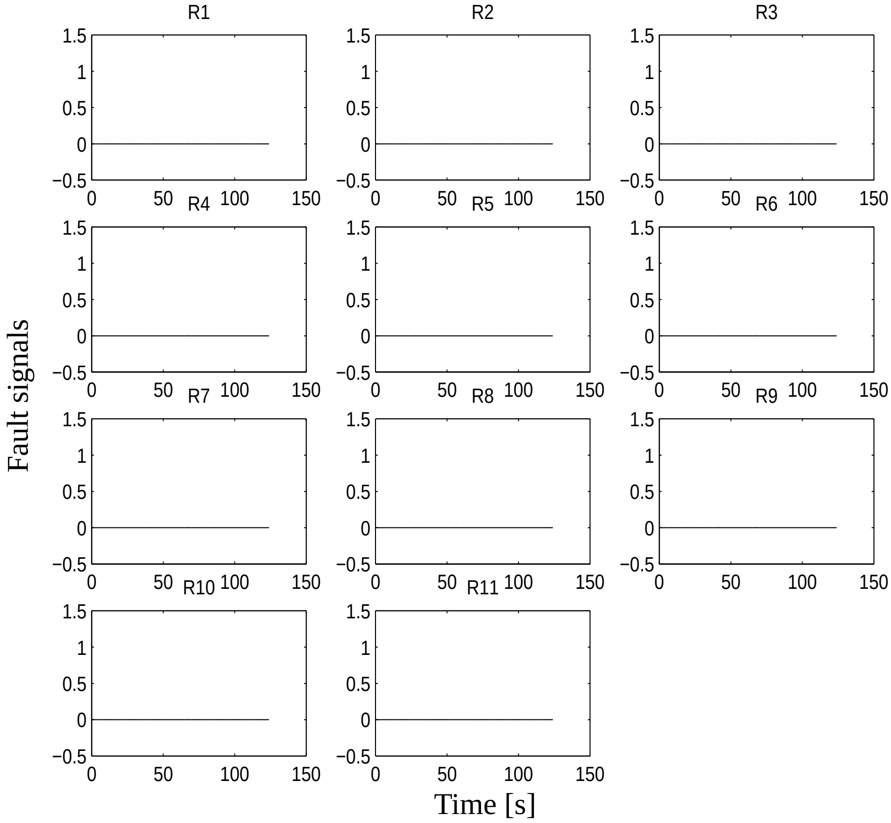


Figure 1: Residual reactions to No Fault

### Fault 1: Pressure regulator failing

In Figure 2 the pressure regulator is turning passive after 60 seconds. Obviously all residuals react the way they are supposed to, some are zero and some indicate fault. Observe that even if all fault signals are presented together in the following figures they were not generated simultaneously. Since active diagnosis is used in order to receive more residuals the system is in different states depending on which residuals that are generated, the states are presented in Chapter 4. The diagnosis statement in this case is:

Diagnosis statement: $S_1;F_p \in \{F_1\}$

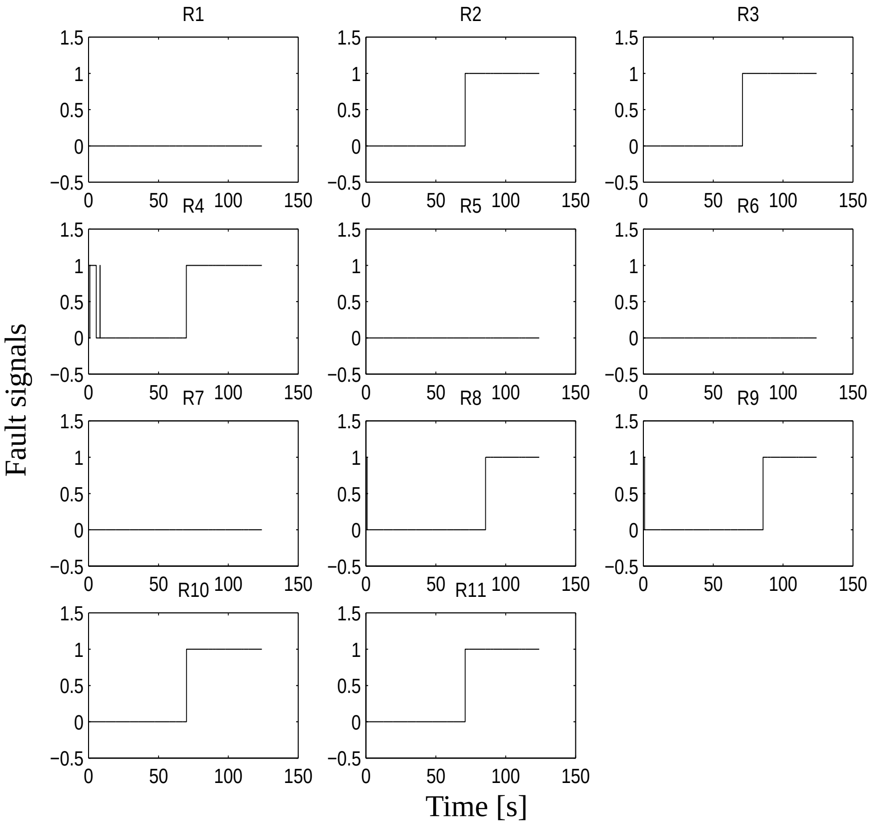


Figure 2: Residual reactions to $F_1$

### Fault 2:CVU failing

In Figure 3 the residuals when the CVU is failing are presented, the CVU is here in the wrong state. Which state that is wrong depends as mentioned earlier on which state the system is supposed to be in, but here all fault signals are presented together. All residuals are reacting according to the theory. Residual 4 is indicating fault initially, during the dynamic state the measured signal is apparently outside its threshold but in steady state the residual is delivering the correct result. The following diagnosis is received:

Diagnosis statement: $S_2;F_p \in \{F_2\}$

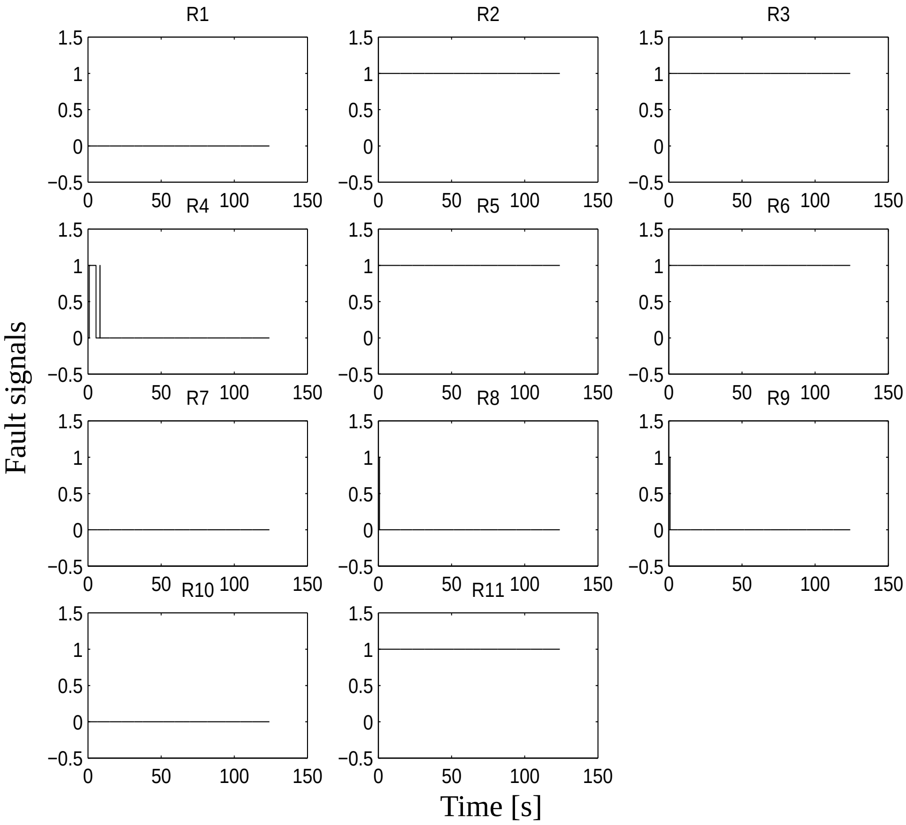


Figure 3: Residual reactions to $F_2$

### Fault 3: Pressure sensor in tank T1 failing

The residuals in Figure 4 show the results when the pressure sensor in tank T1 is failing. A fault with the size of 5 kPa was added to the sensor signal. Residual $R_2$ is not responding immediately but after about 30 seconds, when the system is in steady state, also this residual is giving the correct response, thus, the diagnosis statement is:

Diagnosis statement: $S_3;F_p \in \{F_3\}$

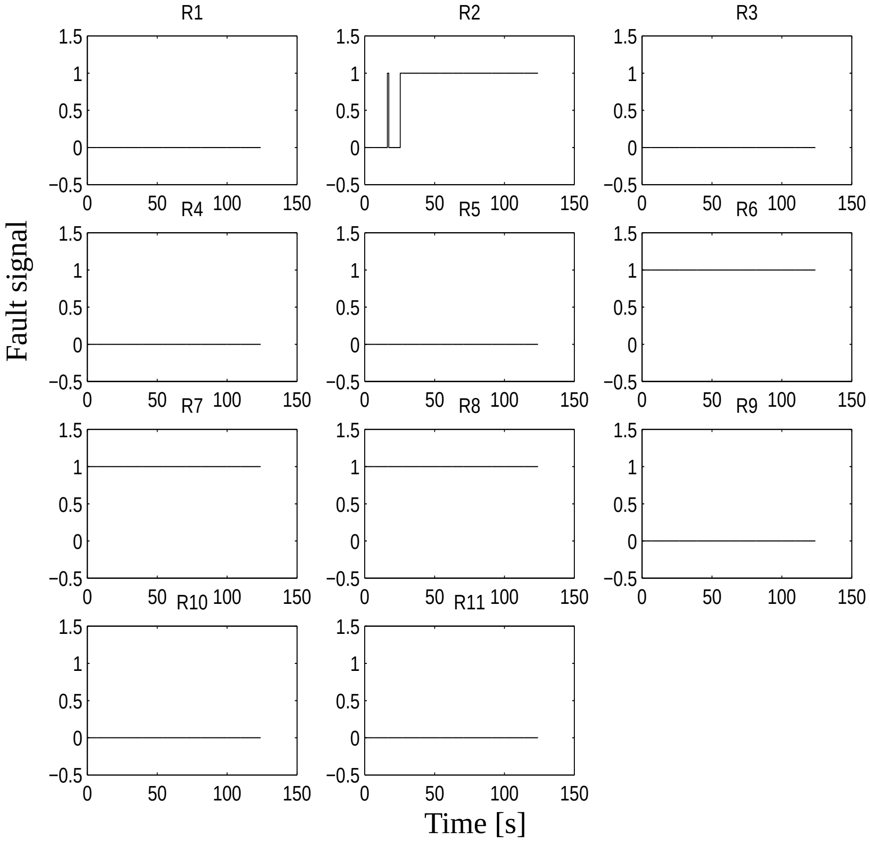


Figure 4: Residual reactions to $F_3$

### Fault 4: Pressure sensor in tank Rest failing

Figure 5 shows the residuals when the pressure sensor in tank Rest is failing, also in this case was the size of the fault 5 kPa. In steady state all the residuals give the correct response. In this case the pressure sensor was failing from the start, had the fault occurred after more then 50 seconds all the residuals would have given the correct result immediately since all transients would have died off by then. In this case the diagnosis statement is:

Diagnosis statement: $S_4;F_p \in \{F_4\}$

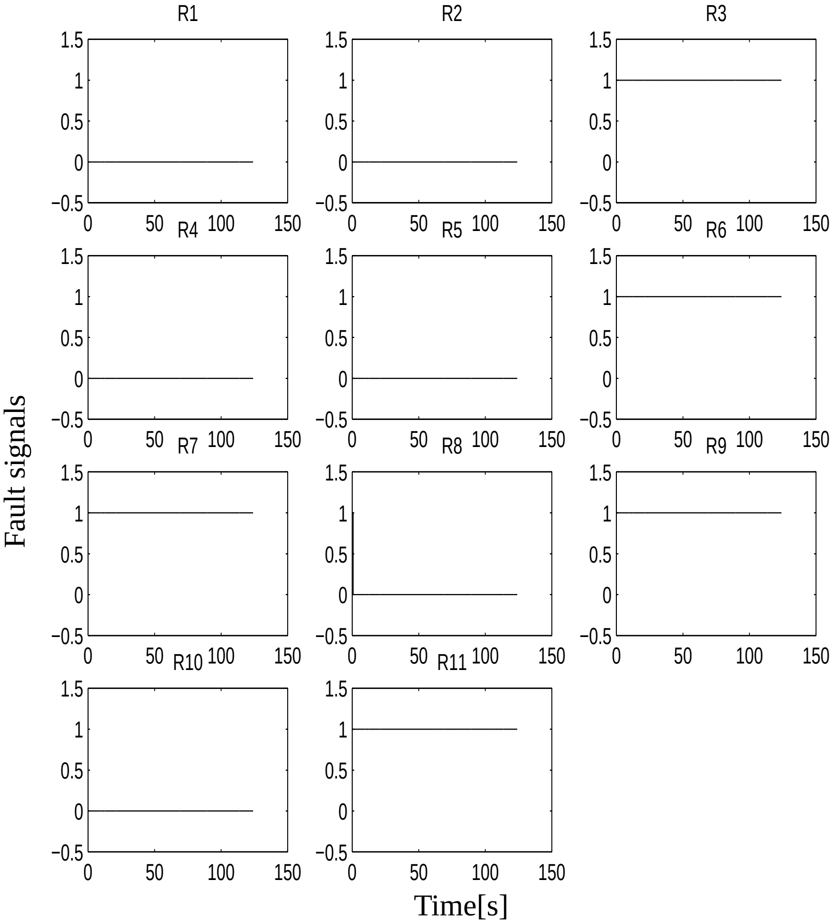


Figure 5: Residual reactions to $F_4$

### Fault 5: Pressure sensor in ambient air failing

When the pressure sensor in ambient air is failing the following result is received. The size of the fault is 5 kPa. As can be seen in Figure 6 all residuals give the correct result in steady state, although residual $R_9$ reacts a bit slow. In steady state the diagnosis statement is:

Diagnosis statement: $S_5;F_p \in \{F_5\}$

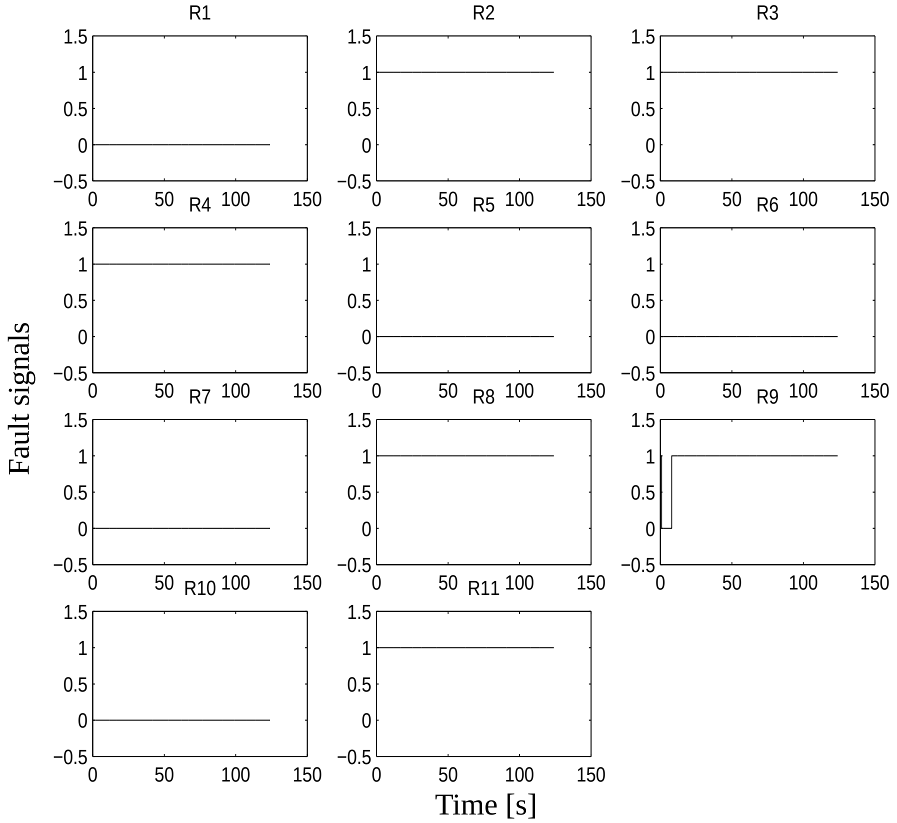


Figure 6: Residual reactions to $F_5$

### Fault 6: Pressure sensor for pressure from ECS failing

The results when the pressure sensor measuring the pressure from ECS is failing are presented in Figure 7. Residual $R_1$ is not giving the expected result during the entire measurement period. This is due to the fact that the pressure from ECS is a bit lower at the beginning of the period and is slowly getting larger and larger. This means that a small sensor fault only brings the residual under the threshold at the beginning of the measurement period. If the sensor fault had been positive in stead of negative the residual would not have reacted at all. This shows the importance of using X:s in the decision structure, this is an example of a residual that does not always react to this kind of fault.

Diagnosis statement: $S_6$;$F_p \in \{F_6, F_{14}\}$

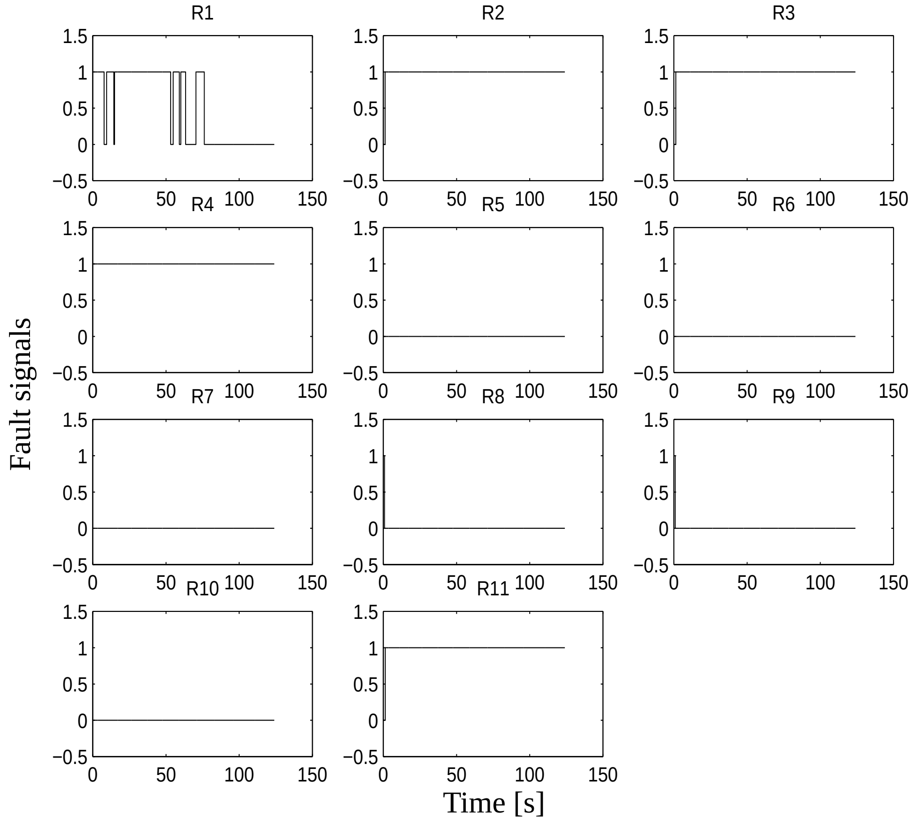


Figure 7: Residual reactions to $F_6$

### Fault 7: Temperature sensor failing

Figure 8 shows the results of a failing temperature sensor. A fault signal of 1000 K was added to the sensor signal. In this case residuals $R_2$, $R_3$ and $R_{11}$ are not reacting as expected. The reason why they are not giving the correct result is the pressure regulator. In these three cases the pressure regulator is “hiding” the fault, since the pressure regulator is controlled directly by the pressure difference the pressure in the tanks are correct anyway. Only initially are the residuals reacting as they should. This means that a failing temperature sensor might be hard to isolate, but an experienced mechanician could perhaps anyway draw the correct conclusion by inspecting the fault signals, an automatic system would though be hard to build. Following, inaccurate statement is received:

Diagnosis statement: $S_7$;$F_p \in \{F_1, F_5, F_6, F_7, F_8, F_9, F_{12}, F_{13}, F_{14}\}$

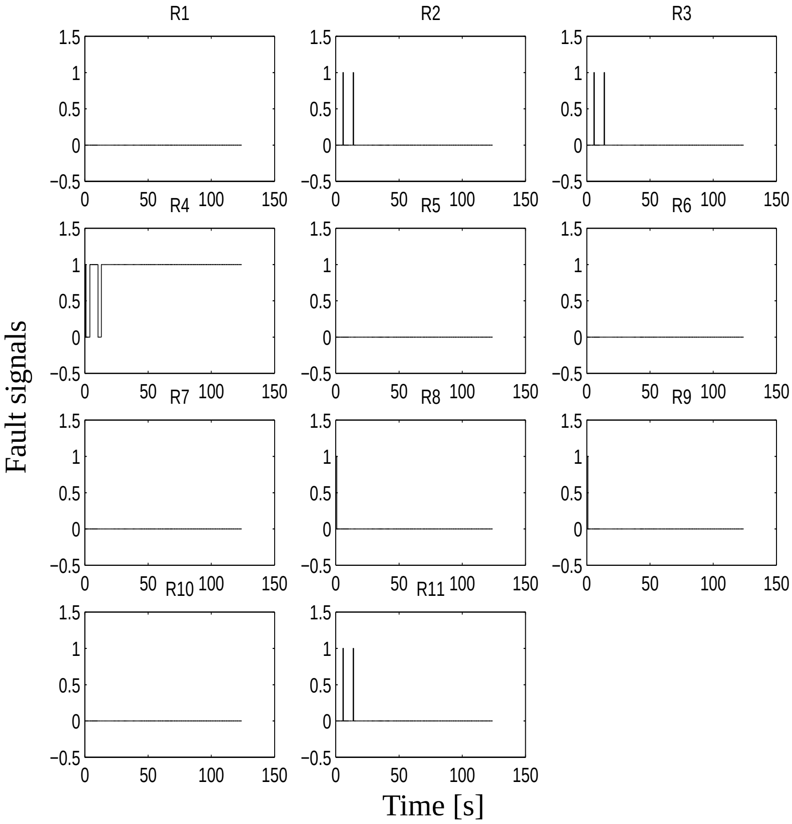


Figure 8: Residual reactions to $F_7$

### Fault 8: Volume sensor in tank T1 failing

The residual signals when the volume sensor in tank T1 is failing are presented in Figure 9. Just as in the case with the failing temperature sensor the pressure regulator is hiding this fault. This means that also this fault might be very hard to isolate, or even to detect. With a better model and better thresholds, large faults might still be possible to detect and isolate but small faults will still be hard to both detect and isolate. In this case a false statement is delivered.

Diagnosis statement: $S_8;F_p \in \{NF\}$

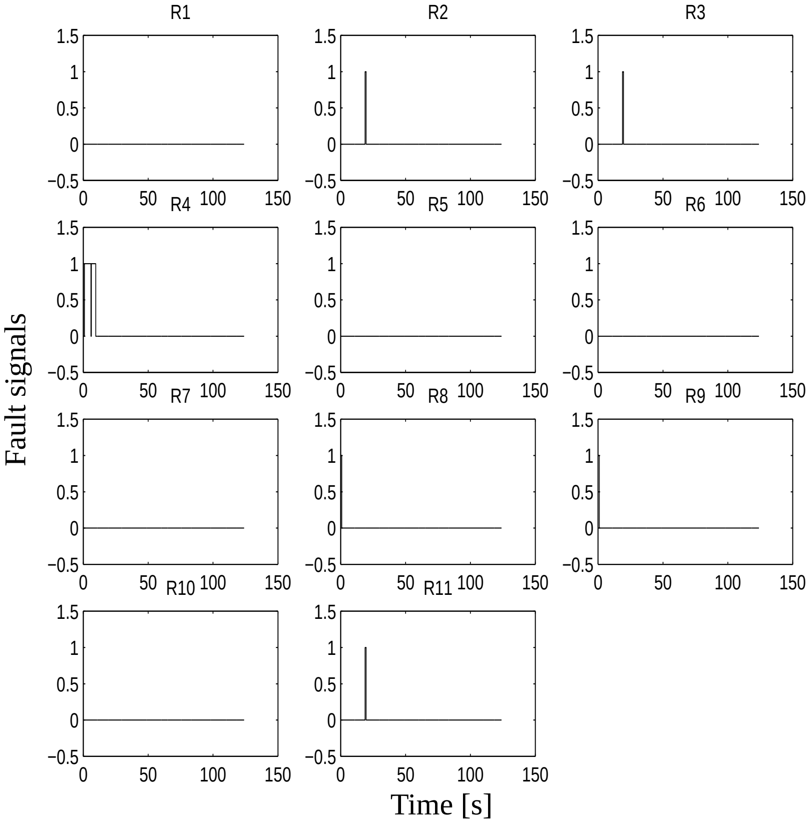


Figure 9: Residual reactions to $F_8$

### Fault 9: Volume sensor in tank Rest failing

When the volume sensor in tank Rest is failing the residual signals in Figure 10 are received. Just as for a failing volume sensor in tank T1 the residuals are not responding the way that they would have if the pressure regulator was not hiding the pressure fault. Also in this case a false statement was given by the diagnosis system.

Diagnosis statement: $S_9;F_p \in \{NF\}$

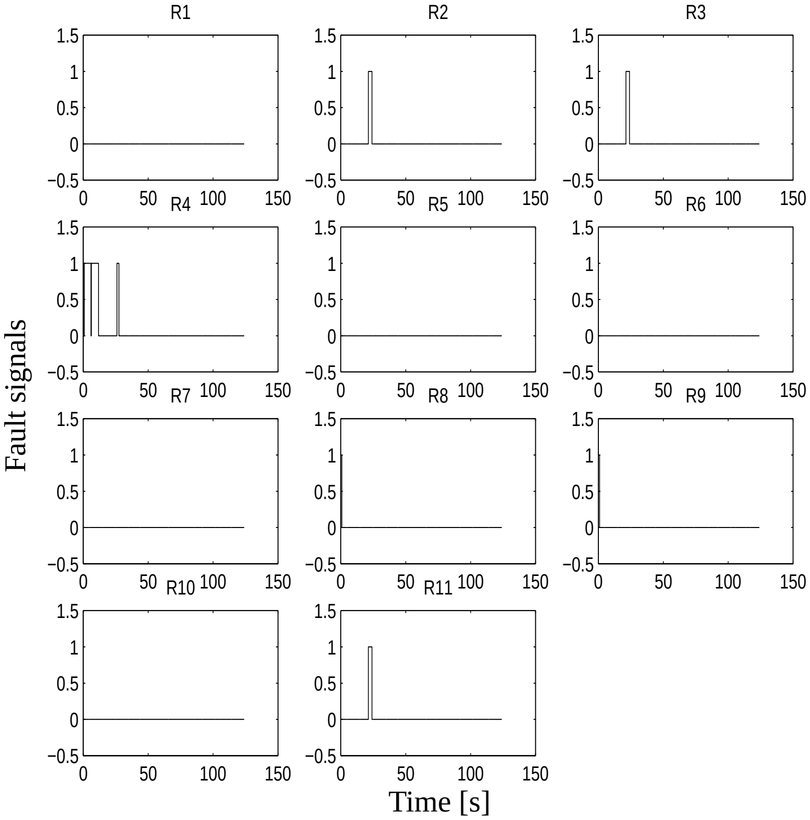


Figure 10: Residual reactions to $F_9$

### Fault 10: Position sensor for pressure regulator failing

In Figure 11 the residual signals when the position sensor for the pressure regulator is failing are presented. A fault signal adding 10% to the measured value was introduced. All residuals are reacting as they are supposed to, and since only one residual is reacting to this fault the isolation would be very simple. The diagnosis statement is:

Diagnosis statement: $S_{10};F_p \in \{F_{10}\}$

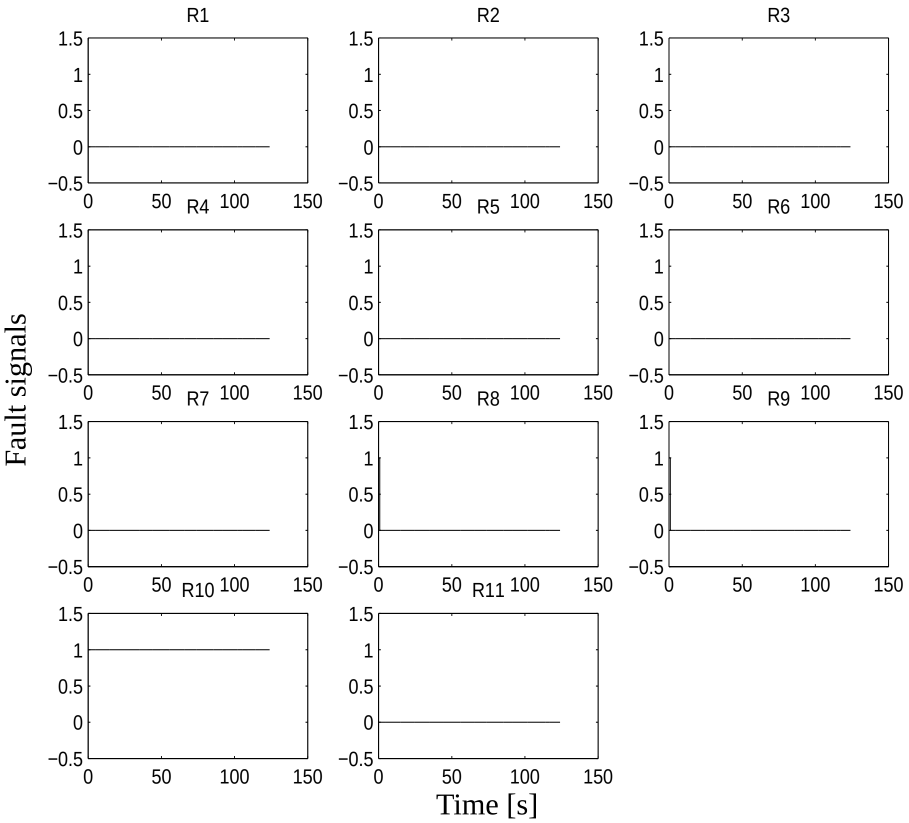


Figure 11: Residual reactions to $F_{10}$

### Fault 11: Position sensor for the CVU failing

When the position sensor for the CVU is failing the residuals in Figure 12 are received. In this case all residuals are reacting correctly, and just as in the previous case the fault i easy to isolate since only one residual is reacting. The diagnosis statement is:

Diagnosis statement: $S_{11}$;$F_p \in \{F_{11}\}$

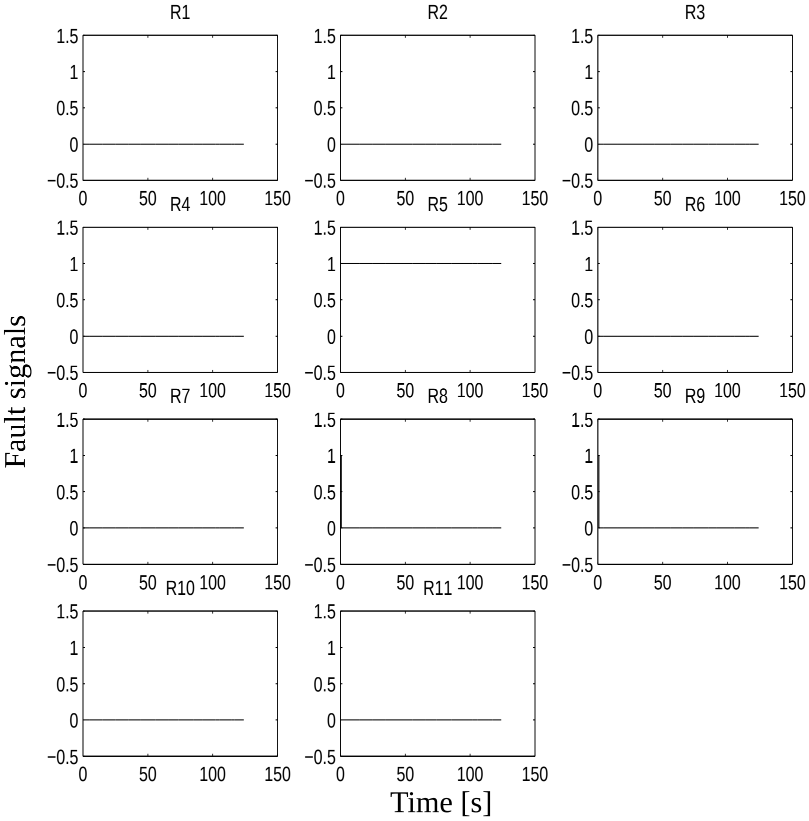


Figure 12: Residual reactions to $F_{11}$

### Fault 12: Leakage

In Figure 13 a leakage occurs after 50 seconds. The residuals are reacting as expected, residual $R_4$ is indicating fault also initially, during the dynamic state where the model is less accurate. This behavior could be prevented by making the threshold even more generous during the dynamic state but as was mentioned earlier it is the behavior during steady state that is most interesting. In steady state the diagnosis statement is:

Diagnosis statement: $S_{12}$;$F_p \in \{F_7, F_9, F_{12}\}$

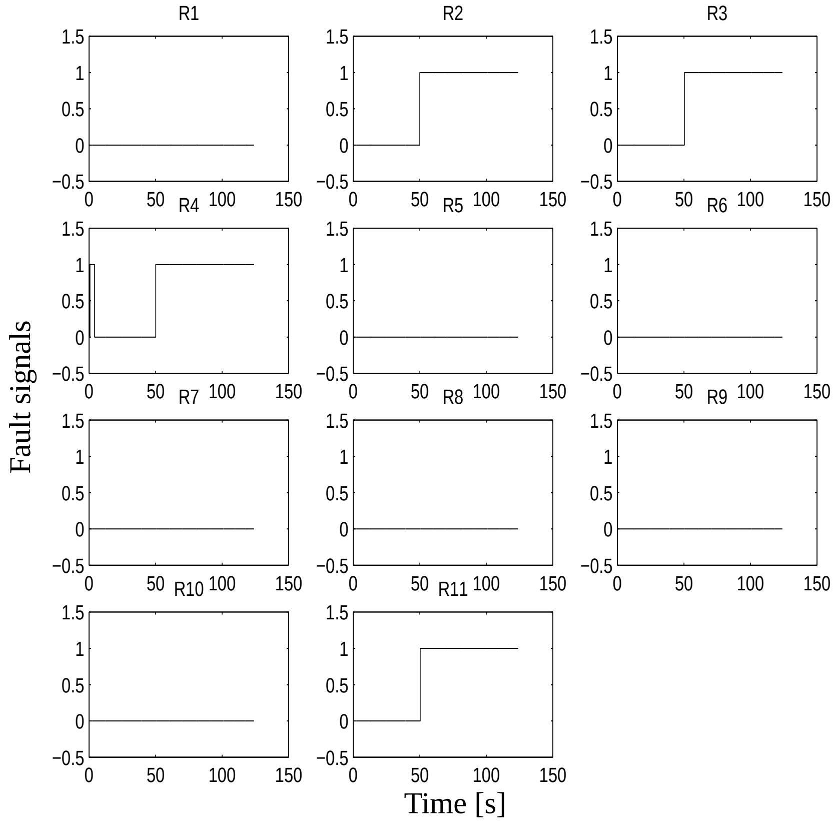


Figure 13: Residual reactions to $F_{12}$

### Fault 13: Blocking

Figure 14 shows the residual signals when some a in the tank pressurization system is entirely blocked. All residuals react as expected, only residuals $R_3$ and $R_{11}$ are a bit slow. It should however be mentioned that this fault is very unlikely since the air is cleaned before it is led into the pressurization system and the pipes are rather thick. The diagnosis statement is:

Diagnosis statement: $S_{13}$;$F_p \in \{F_{13}\}$

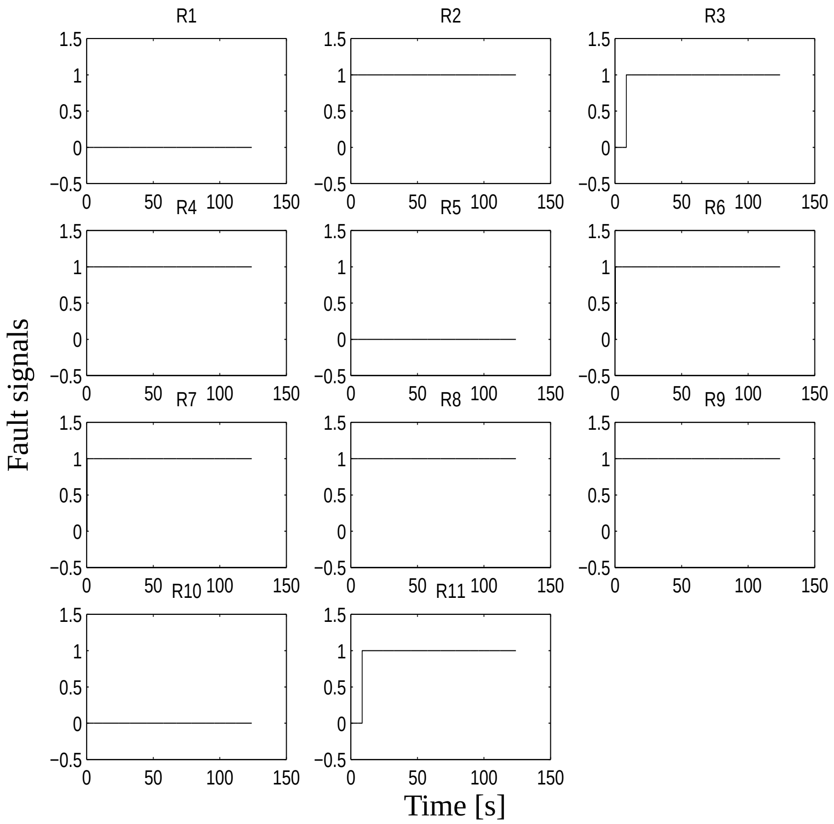


Figure 14: Residual reactions to $F_{13}$

### Fault 14: Low pressure from ECS

When the ECS system does not deliver a pressure above the specified level both the real system and the model becomes a bit unreliable, at least none of them perform as good as they are supposed to. As can be seen in Figure 15 the residuals react as can be expected, the reason why residual $R_1$ does not indicate fault during the entire period is that after 60 seconds the pressure rises above the threshold. That none of the other reacting residuals indicate zero at the same time indicates that the threshold should be a bit higher. In the initial state the diagnosis statement is:

Diagnosis statement: $S_{14}$;$F_p \in \{F_6, F_{14}\}$

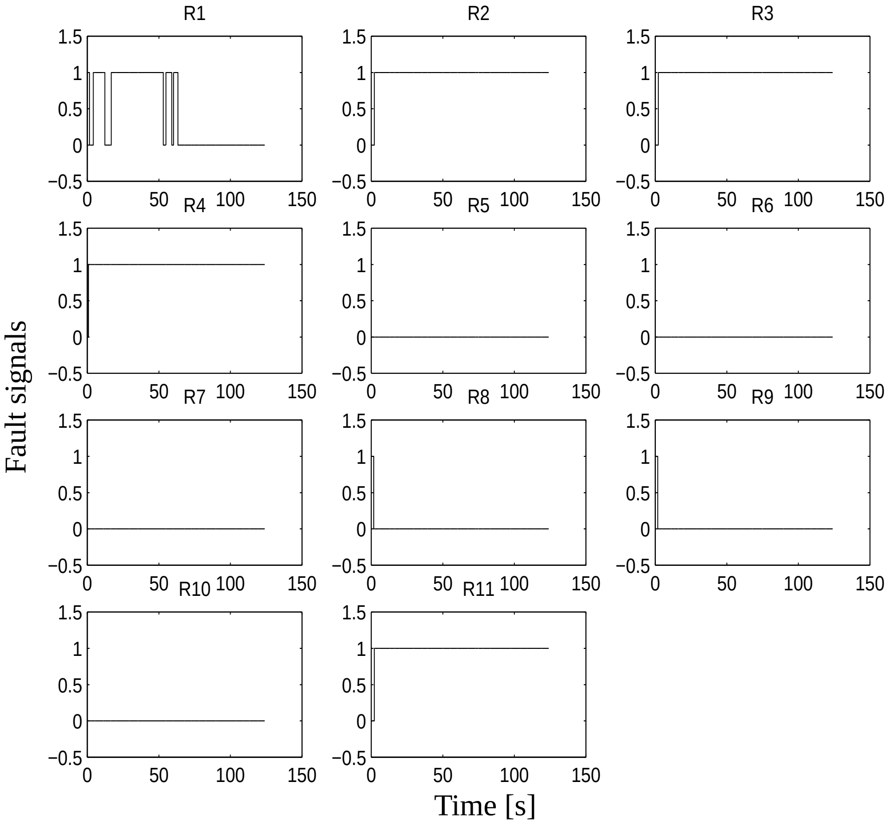


Figure 15: Residual reactions to $F_{14}$

# Appendix B

## Simulink models

In this appendix some of the Simulink models used in the diagnosis system are presented. A short explanation of how they are working is given together with a motivation of why they were implemented this way. The entire tank model is presented in Figure 16.

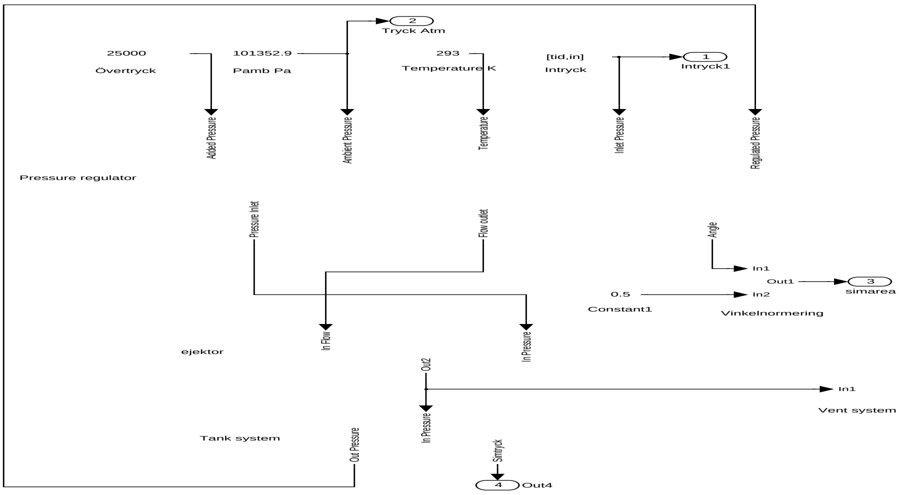


Figure 16: Tank model

## 6.3 Pressure regulator

The pressure regulator is modelled in Simulink according to Figure 17. A PI-controller controls the area and then the outlet flow and simulated area is calculated. The PI-controller is trying to keep the pressure at 25 kPa over ambient air pressure at all times. The outlet flow is used as an input signal to the ejector where the outlet pressure is calculated.

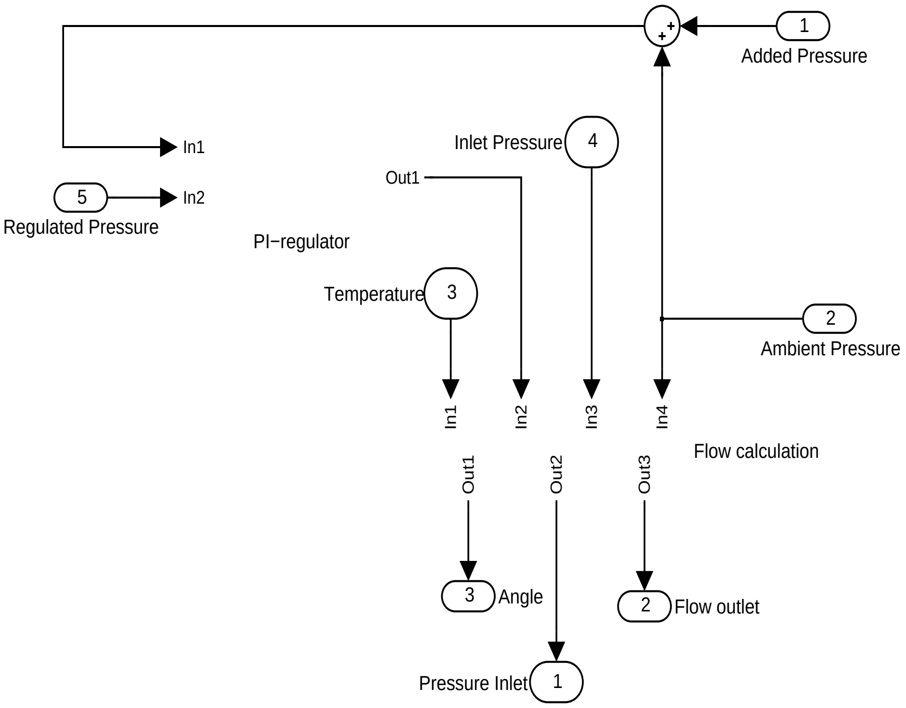


Figure 17: Pressure regulator

## 6.4 Area calculation

Inside the pressure regulator block the outlet flow is calculated. Since the PI-controller actually controls the inlet area to the system the area is what decides how high the pressure in tanks will be. The PI-controller controls a normalized area between 0-100%. This area is then recalculated as is shown in Figure 18. The normalized area is recalculated by a cosine function according to equation (3.3). The angle is limited to 0˚-90˚. The rate at which the angle can change is also limited.

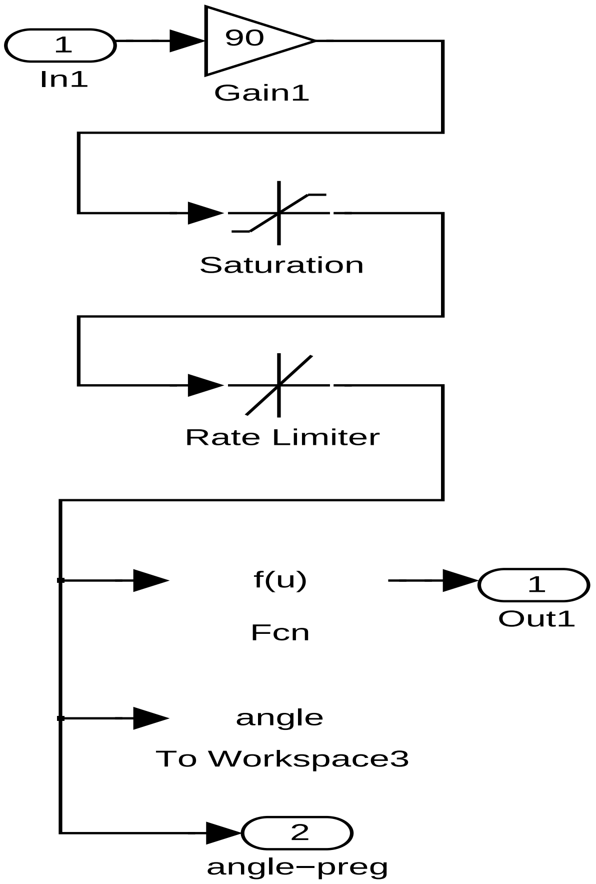


Figure 18: Area calculation

## 6.5 Ejector

The ejector is actually a black box model, shown in Figure 19. The inlet and outlet signals were observed and a gain and a filter was designed to fit these signals. An attempt to model the ejector with a more physical approach was made but was found hard to implement. Since the only interesting values for the diagnosis system are the ones that can be measured the use of a black box model was not limiting in any way. The internal states in the ejector could not be measured so only the outlet signal was of any interest.

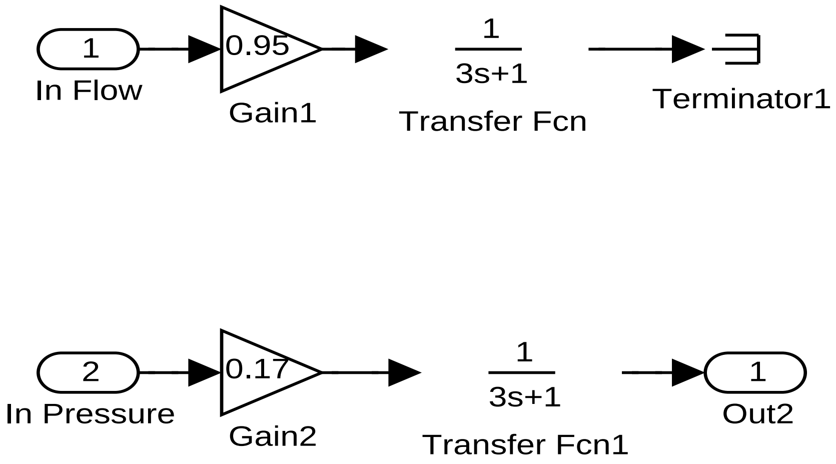


Figure 19: Ejector

## 6.6 Tank system

The tank system is consisting of the tanks and a leakage out to ambient air. The leakage could also have been added to the ejector model since it actually the effect of the counter pressure form the tanks to the ejector that is simulated but it was found easiest to implement this way. The fuel tanks have volumes that are possible to change depending on how much fuel that is in the system. No engine was simulated so the fuel level is constant during each simulation. The tank system is presented in Figure 20.

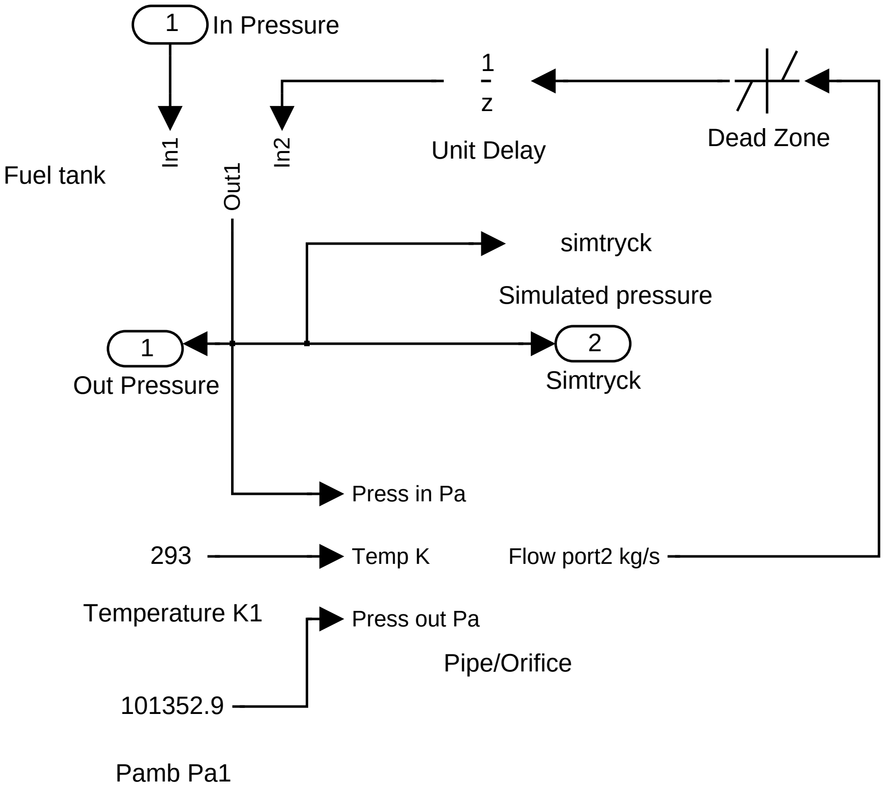


Figure 20: Tank system

## 6.7 Thresholds

The thresholds were designed according to Figure 21. The thresholds were calculated according to equation (2.9) or just simply by adding a constant level to the simulated signal. The measured signal is then compared with the simulated signal and the difference is compared to the threshold. If the compared signal is higher than the threshold an alarm is genrated.

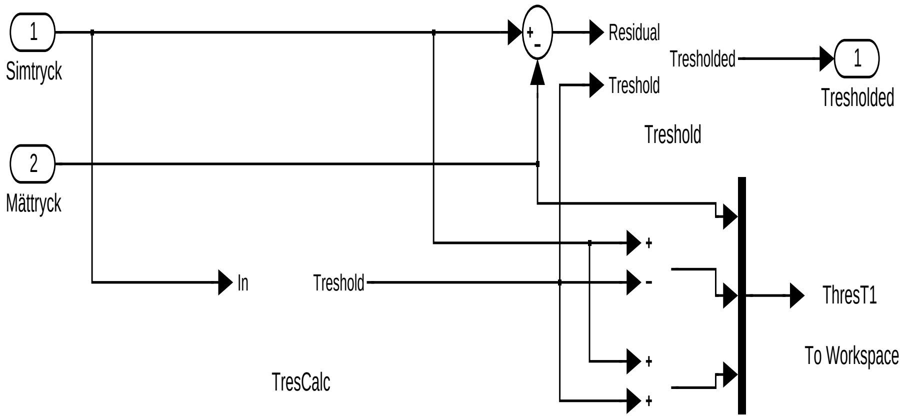


Figure 21: Threshold generator

When constructing a model in for example **Simulink** good system knowledge is needed and throughout the implementation of this model the regulating theories from Glad and Ljung **[2]** were used.