Diagnosis of the air distribution system of the JAS39 Gripen environmental control system

Johan Karlsson

Reg nr: LiTH-ISY-EX-3092

28 February 2001

Diagnosis of the air distribution system
of the JAS39 Gripen environmental control system

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

Johan Karlsson

Reg nr: LiTH-ISY-EX-3092

Supervisors: Erik Frisk, Vehicular systems LiTH
              Birgitta Lantto, Saab AB

Examiner: Lars Nielsen, Vehicular systems LiTH
Linköping 28 February 2001

Titel
Title

Diagnosis of the air distribution system of the JAS39 Gripen environmental control system

Författare
Author

Johan Karlsson

Sammanfattning
Abstract

Traditionally supervision has been achieved using limit checking and hardware redundancy, but these methods have proven insufficient. The availability of information from all parts of the aircraft and the computing capacity available in the Gripen today enables the implementation of sophisticated supervision methods, for instance model based diagnosis.

The purpose of this thesis was to investigate which faults in the distribution part of the Environmental Control System (ECS) could be detected with the sensors available today, using model based diagnosis, and to clarify where new ones could be useful in order to design an improved diagnosis system.

No measurement data from a real ECS could be obtained, so the real system had to be replaced by an Easy5-model. Therefore the diagnosis system developed in this thesis is not directly applicable on a real ECS.

With the sensors available, 8 of the 9 faults important to detect, can be detected. The last important fault can be detected if one new pressure is installed.

95-11-01/lli

Abstract

Traditionally supervision has been achieved using limit checking and hardware redundancy, but these methods have proven insufficient. The availability of information from all parts of the aircraft and the computing capacity available in the Gripen today enables the implementation of sophisticated supervision methods, for instance model based diagnosis.

The purpose of this thesis was to investigate which faults in the distribution part of the Environmental Control System (ECS) could be detected with the sensors available today, using model based diagnosis, and to clarify where new ones could be useful in order to design an improved diagnosis system.

No measurement data from a real ECS could be obtained, so the real system had to be replaced by an Easy5-model. Therefore the diagnosis system developed in this thesis is not directly applicable on a real ECS.

With the sensors available, 8 of the 9 faults important to detect, can be detected. The last important fault can be detected if one new pressure is installed.

Acknowledgements

Contents

Chapter 1

Introduction

This thesis has been carried out in cooperation with Saab Aerospace, which is a business area within Saab AB. The main product of Saab Aerospace is the Gripen fourth-generation multi-role combat fighter. What characterises a fourth generation aircraft is an extended use of integrated computerized systems. The availability of information from all parts of the aircraft and the computing capacity available in the Gripen today enables the implementation of sophisticated supervision methods. This is what this thesis is about, and it has been performed at the section for system simulation and thermal analysis of general systems.

1.1 Background

A modern combat fighter contains many subsystems, for instance fuel-, hydraulics-, electrical- and environmental control system. Often these systems are crucial for providing a safe flight, and they are therefore important to supervise and as soon as possible detect any malfunction. Since many of these systems are very complex and nonlinear, this is not a trivial task. Traditionally supervision has been achieved using limit checking and hardware redundancy[1]. Limit checking has the advantages of being a simple method that works well under steady-state conditions. However, it has problems handling large transients in the system, and the result might be frequent false alarms.

If an alarm is generated in an aircraft, false or not, an investigation about what has happened has to be undertaken. Meanwhile the aircraft is grounded. With this in mind it is not hard to realize that it is of great interest to decrease the number of false alarms, and *model based diagnosis* has the potential to do this. Besides better handling of system transients, model based diagnosis also offers a technique to determine which component caused an occurred fault.

---

1. More about traditional supervision in Chapter 2

These two characteristics could increase aircraft availability and render more effective mainte-
nance.

This is why Saab has decided to look further into model based diagnosis and see whether or
not the technique is applicable to an aircraft subsystem. This thesis focuses on the environ-
mental control system (ECS), which has all of the characteristics mentioned above. It is very
complex, nonlinear and it is necessary for operating the aircraft safely. The ECS can be
divided into three main sections: air supply, air conditioning and air distribution. I have been
working with the distribution part, since it contains the largest amount of sensors and therefore
is the easiest part to diagnose. The two other sections contain very few sensors.

1.2 Objectives

The purpose of this thesis is to investigate which faults in the distribution part of the ECS can
be detected with the sensors available today, using model based diagnosis, and to clarify where
new ones could be useful in order to design an improved diagnosis system.

1.3 Limitations

Unfortunately no data from a real ECS has been available. There were data from old runs in
the ECS rig at hand, but these runs were undertaken in a faultless system. Introducing all inter-
esting faults and making the necessary runs would have taken a few weeks, and that much time
was not vacant in the rig. The only possibility was to replace the real system with a model, and
fortunately Saab had already built a model of the ECS in Easy5, a simulation software. This is
a very large and complex model and therefore simulating it is quite time consuming. The
Easy5-model is validated in static cases, but it has not been validated for dynamic cases, and
that is of course a major drawback for this thesis.

The diagnosis system developed in this thesis only works when the ECS is operating in its nor-
mal mode. There are a few degraded modes, for instance additional cooling air is available
through ram air intakes in emergency situations. When these intakes are open the system is
reconfigured and works completely different from the normal mode. Then the model used to
describe the system is no longer valid and cannot be used for diagnosis purposes.

Throughout the thesis only single faults is assumed, i.e. no more than one fault at a time is
supposed to be present.

1.4 Readers guide

The theory necessary to follow the reasoning in this thesis is presented in Chapter 2. Chapter 3
contains a description of the Gripen ECS, its components and how they are modelled. In the
end of the chapter the component models are assembled into a model of the ECS distribution
section. In Chapter 4 the development and evaluation of the two diagnosis systems built is pre-
sented. Furthermore, all considered fault modes and how they affect the system is included.
Chapter 5 contains conclusions and suggestions for further work.

Chapter 2

Model based diagnosis

2.1 Traditional supervision - model based diagnosis

Diagnosis has traditionally been performed mainly by limit checking. That means observing a quantity all the time, and if it leaves its normal operating range an alarm is generated. The normal operating range is defined by thresholds. These thresholds are often dependent on the operating point of the system, since the normal operating range of a quantity can vary a lot with the operating point. If there was a corresponding set of thresholds for every possible operating point, that would actually be a kind of model based diagnosis, but then lots of data would have to be stored. Instead a limited number of operating points are used, and in order to avoid false alarms the thresholds must be set according to a worst case scenario. This makes it hard to detect small faults. Since limit checking only compares measured values with certain limits, the method assumes all sensors and actuators are working correctly. This is a risky statement to make, and implies a great drawback for the method. Model based diagnosis on the other hand focuses on hardware faults and considers their effect on the supervised process. With this approach any desired fault can be considered, and since the effect of different faults is known, fault isolation is also possible. Limit checking does not provide a natural way to isolate faults.

Another method that has been used traditionally, often together with limit checking, is to duplicate, or triplicate, hardware. This is called hardware redundancy. It has at least three significant drawbacks: it adds weight to the system, it is expensive and it requires space. Furthermore it adds extra sources of errors to the system. On the other hand, hardware redundancy offers reliable and fast diagnosis.

Model based diagnosis has proven a useful alternative to the traditional approaches, and has potentially the following advantages:

- It can provide a higher diagnosis performance, smaller faults can be detected and the detection time is shorter.

- Different faults can be isolated.

- It can be performed over a large operating range.

- Disturbances can be compensated for, which enables high diagnosis performance in spite of present disturbances.

- It is applicable to more kinds of components. Not all hardware can be duplicated.

- No extra hardware is needed, which saves space, weight and sometimes even money.

The disadvantage of model based diagnosis is the need of an accurate model, computing capability and perhaps also a more complex design procedure. Building the model is probably what takes the most work when designing a diagnosis system, and it also is the most important part since the model normally is what limits the performance of the diagnosis system.

Even though model based diagnosis is a very powerful technique, it can probably never fully replace hardware redundancy. If it for instance is crucial that a correct measurement signal always is available (perhaps it is used to control the process), an extra sensor combined with model based diagnosis might be the best way to solve the problem.

2.2 How does a model based diagnosis system work?

First of all, a model of the process to supervise is needed. Secondly all faults that might affect the process and knowledge about how they do this is needed. The diagnosis system then compares the behaviour of the supervised process and the model, and if differences arise it tries to deduce if one, or perhaps several, of the modelled faults can explain these differences.
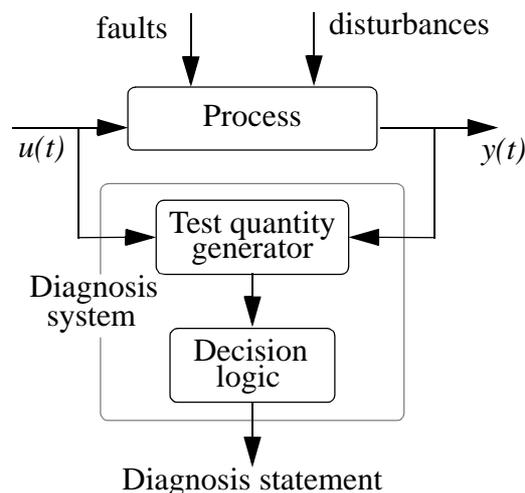
Figure 2.1: Principal diagnosis system

In Figure 2.1, the principle of a diagnosis system is shown. The two signals "faults" and "disturbances" affects the process, but cannot be measured. The diagnosis system is fed with the

control signals *u*, and the measurements *y*, and from this information it generates a certain amount of test quantities. These test quantities are based on the process model and are designed to be small or equal to zero when no fault is present, and large when there is a fault present. Not all test quantities react (differ from zero) to all faults, and this is used by the decision logic to perform a number of hypothesis tests to determine if, and in that case which faults might be present. This is called a diagnosis statement.

2.3 Fault models

As mentioned before the process model is a very important part of the diagnosis system. Fault models are another important component. Models are needed for all faults supposed to be detected or isolated. If a fault not modelled occurs, the diagnosis system will give an unknown response. What faults to model is, of course, dependent on the system concerned, but a rule of thumb is that moving parts are error prone. Putting too much trust in sensors is also dangerous.

How a fault is modelled is also an important issue. There are many different ways to model faults, see [1], but a few examples are:

- **Intermittent fault** is a fault that repeatedly occurs and disappears. Example: loose connectors.

- **Incipient fault** is a fault that gradually develops from no fault to a larger and larger one. Example: A slow degradation of a component.

- **Abrupt change** is a fault that appears as a very quick change of a variable. Example: Sudden breakdown of a component.

Mathematically a fault can for instance be expressed as:

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

where

y_{obs}(t) = observed value of *y(t)*
y_{corr}(t) = correct value of *y(t)*
f(t) = fault affecting *y(t)*

In (2.1) the fault is modelled as an arbitrary additive signal. This is a very general model and covers all possible faults.

To explain the state of the process a number of fault modes can be defined. The process is then said to belong to one of these fault modes in every instant. Each fault mode is associated with one fault and there is also one fault mode corresponding to the state "no fault". This is of course needed, because otherwise the diagnosis system would believe there was always a fault present. The diagnosis system's task is to decide which one of the predefined fault modes that can explain the behaviour of the process.

For most systems one can assume that only one fault will occur at a time, but if that is not the case, fault modes containing two or more faults can be constructed.

2.4 Hypothesis tests

A hypothesis test, see [2], is used to choose between two possibilities. In model based diagnosis hypothesis tests are used to decide which fault mode that can explain the current behaviour of the process. The test is applied to make a choice between two different sets of fault modes. It is then checked whether or not a test quantity is greater than a threshold.

2.4.1 Test quantities

A test quantity is a relation between measured process signals and data from the model, and they are used to detect deviations from normal process behaviour.

When designing a test quantity, the aim is to decouple some of the fault modes. A fault mode decoupled in a certain test quantity does not affect that quantity at all, so even if the decoupled fault does occur it does not change the value of the test quantity. If F_p denotes the fault mode present in the system and R_k denotes a set of fault modes, the hypothesis can be written:

$$H^0: \qquad F_p \in R_k \;=\; \{\text{no fault and decoupled fault modes}\}$$
$$H^1: \qquad F_p \in R_k^C \;=\; \{\text{all other fault modes}\}$$

If H^0 is rejected we assume H^1 is true. On the other hand, if H^0 is not rejected we do not assume anything.

2.4.2 Thresholds

How do we know when to reject a hypothesis then? This is what thresholds are for. Even if there are no faults present in the process, the test quantity still cannot be expected to equal zero since measurement noise and model uncertainties will always be present. Therefore a threshold is needed, and this threshold must be greater than the disturbances influence on the test quantity. If the test quantity is greater than or equal to the threshold the hypothesis is rejected. Otherwise it is not rejected. If T_k is the test quantity and J_k is the threshold this can be written:

$$H_k^0 \text{ is not rejected if } T_k < J_k$$
$$H_k^0 \text{ is rejected if } T_k \geq J_k$$

(However, if the test quantity is based on the *likelihood function* it is the other way around, see [1])

The result of the hypothesis test H_k is a decision S_k:

$$S_k = \begin{cases} S_k^0 = \Omega & \text{if } H_k^0 \text{ is not rejected} \\ S_k^1 = R_k^C & \text{if } H_k^0 \text{ is rejected} \end{cases}$$

where Ω denotes the set of all fault modes.

2.5 Fault isolation

By designing test quantities decoupling different sets of fault modes and performing hypothesis tests on these, information about which fault mode the process is working in can be extracted. Every hypothesis rejected might exclude one or more fault modes able to explain the process behaviour. This implies that after k hypothesis tests are done the final decision is:

$$S = \bigcap_k S_k$$

Preferably S contains only one fault mode, but often the final decision is a list of possible present fault modes. The more measured variables there are, and the more variables that can be calculated in the model, the easier it is to isolate a specific fault.

To get a good overview of available test quantities and which fault modes they affect, a decision structure can be used. Table 1 shows an example of a decision structure.

	NF	$\mathbf{F_1}$	$\mathbf{F_2}$	$\mathbf{F_3}$
$T_1(\mathbf{x})$	0	0	X	0
$T_2(\mathbf{x})$	0	0	X	1
$T_3(\mathbf{x})$	0	X	0	X

Table 1: Example of a decision structure

A 0 in column i and row j in Table 1 above means the test quantity in question is unaffected by the corresponding fault mode i, i.e. fault mode i is then decoupled in test quantity j.

A 1 means this fault mode always affects the corresponding test quantity when a fault is present. However, this is a quite dangerous statement to make. Imagine the presence of fault f_2 (corresponding to the fault mode $\mathbf{F_2}$), which affects both T_1 and T_2, but assume its amplification is much larger to T_2 than to T_1. Then if f_2 is present H_2^0 might be rejected (T_2 is greater than its threshold) while H_1^0 is not.

In a decision structure consisting only of ones and zeros this situation would not be dealt with properly, because if H_1^0 is not rejected we directly exclude f_2. This is where the X (pronounced: *don't care*) comes in. Even though the test quantity might be smaller than its threshold, we do not say the fault has not occurred. For instance, even if H_1^0 is not rejected, $\mathbf{F_2}$ is not excluded.

Below is an example showing the principals of how a decision structure is used.

Example 2.1

Given the diagnosis system described in Table 1, assume that T_2 and T_3 shows that H_2^0 and H_3^0 have been rejected. We then get the diagnosis:

$$S = \Omega \cap \{F_2, F_3\} \cap \{F_1, F_3\} = F_3$$

On the other hand, if only H_3^0 is rejected we get:

$$S = \Omega \cap \{\Omega \backslash F_3\} \cap \{F_1, F_3\} = F_1$$

2.6 Examples of test quantities

There are many different kinds of test quantities, but they all have a few common properties. They are designed to be small when there is no fault present, and large when a non-decoupled fault is present. Using the notation developed in Section 2.5 we can say: If a fault mode in R_k^C can explain measured data, T_k should be large. Then H_k^0 along with all fault modes in R_k are rejected. If a fault mode in R_k can explain the measured data it is the other way around and T_k should be small.

Now two commonly used test quantities will be introduced.

2.6.1 Consistency relations

A consistency relation is perhaps the simplest of all test quantities. It is simply a relation between actuator and measurement signals, supposed to equal zero if the process and model behaviour match. For instance, measured flow minus modelled flow, see (2.2), always equals zero if the process behaviour follows the model. The left side of (2.2) is called *residual,* and this is a measurement of how well the process follows the model. The residual is what is compared to the threshold when performing a hypothesis test:

$$R = \dot{m}_{meas} - \dot{m}_{mod} \tag{2.2}$$

All test quantities must fulfil the following two requirements:

- The function describing the influence of actuator and sensor signals on the residual has to be zero. This ensures the residual will equal zero in the fault free case.

- The function describing the influence of a non-decoupled fault to the residual has to be non-zero, because otherwise the residual will not deviate from zero when a fault occurs.

Example 2.2
Consider the electric circuit to the right. Ohms law gives the consistency relation:

$$RI - U = 0$$
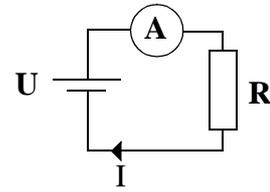
I is a sensor signal, and U is an actuator signal in this case. Suppose we want to supervise the actuator signal $U,$ and the true voltage is:

$$U = U_t + f_U$$

Then the residual can be written:

$$f_U = RI - U_t$$

This expression fulfils the two requirements above.

2.6.2 Observers

Another popular way of generating test quantities is to use a diagnostic observer. They are a powerful tool, but there are two major difficulties that has to be dealt with:

- How to choose observer architecture and ensure observer stability.

- Decoupling of faults and disturbances to make fault isolation possible.

Consider a non-linear system on state space form (see [3] for more about state space form):

$$\begin{aligned} \dot{x} &= f(x, u) \\ y &= h(x, u) \end{aligned} \tag{2.3}$$

The task of the observers is to estimate the state vector x, using only the actuator signals u, and the sensor signals y. The simplest way of doing this is to use the function f, which describes the system dynamics:

$$\dot{\hat{x}} = f(\hat{x}, u) \tag{2.4}$$

This observer design is however very sensitive towards disturbances, model errors and bad initial conditions. An improved observer design also feeds back the estimation quality $y - \hat{y}$, and can be written:

$$\dot{\hat{x}} = f(\hat{x}, u) + K(y - h(\hat{x}, u)) \tag{2.5}$$

where K is the feedback gain matrix. The feedback gain K can be either constant or time and state dependent. It also has to be chosen in such a way that observer stability is ensured. There is no general method for doing this in the non-linear case. A common approach is to linearize

the system around a working point and make a linear observer design, e.g. a Kalman filter design, see [3]. This will probably work in a neighbourhood surrounding the working point.

When using an observer for diagnosis purposes the estimated state space vector $\hat{x}$ is somehow compared to a measurement signal in order to obtain a residual. This can for instance be achieved by (2.6).

$$R \ = \ y - h(\hat{x}, u) \tag{2.6}$$

2.7 Adaptive thresholds

As mentioned earlier, disturbances, measurement noise and model errors force us to threshold our test quantities to avoid constant false alarms. Disturbances and measurement noise are often independent of which state the system currently is working in, but this is not the case with model errors. If a very good model is used, the model errors can be neglected and the process's deviation from the model is practically state-independent. The noise can often be assumed to be white noise, or at least filtered white noise. In this case a constant, time invariant threshold is applicable. However, this is very rare and that is why *adaptive thresholds* are introduced. These thresholds are based on knowledge of model uncertainties. In states where model errors are present the thresholds are enlarged in order to avoid false alarms. There is no general structure for adaptive thresholds, but they often look like (2.7).

$$J_{adp}(t) \ = \ kH_{LP}(p)(\left|H_{FD}(p)u(t)\right| + c) \tag{2.7}$$

where 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. Where model errors are known to be large the filter gain should be large, and of course the other way around as well. The constant c is determined by measurement noise and other disturbances. It also prevents the threshold from equalling zero when the input signal is zero. H_{LP} is a low pass filter for smoothing the threshold.

Chapter 3

The Gripen environmental control system

In this chapter the Gripen ECS will be described. First the system in general, but later a focus will be held on the distribution part and its components. The models used to describe these components mathematically will be presented in Section 3.2, and in Section 3.3 the complete model of the distribution part will be presented.

3.1 System description

The ECS has several tasks, but three of them are more important than the others. They are cooling of avionics and pressurization and temperature control of the cabin and the air ventilated suit (AVS). Cabin comfort is essential for the well-being of the pilot, and since some of the computers are necessary for keeping the aircraft in the air cooling of them is also very important.

Among the other, less crucial tasks performed by the ECS, windshield defrosting and pressurization of gearboxes and tanks can be mentioned. In future versions of the Gripen an on-board oxygen generator will be installed and it will be driven by the ECS as well.

In a near future the ECS, along with fuel and hydraulics systems, will be controlled by the General Electronic Control Unit (GECU). The functionality of the GECU is thoroughly described in [5].

When studying the ECS it is practical to divide the system into three main sections: *air supply, air conditioning* and *air distribution*. See Figure 3.1.
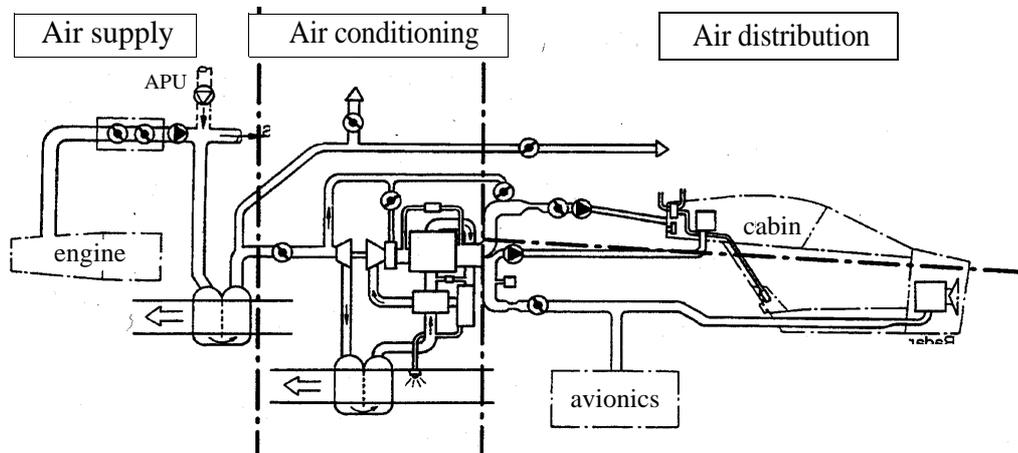
Figure 3.1: Overview of the ECS and its three main sections

The ECS takes hot, compressed air from the engine or the auxiliary power unit (APU). The air is then refrigerated and dehumified before it is distributed in the right amounts and temperature to the cabin and the avionics.

The tree main sections will now be dealt with more thoroughly. More detailed information about the ECS can be found in [4].

3.1.1 Air supply

The ECS is supplied with hot air under very high pressure from the engine, so called bleed air. It is desired to take as little air as possible, since it is used by the engine to propel the aircraft. The more air passing through the engine, the more thrust it develops. The first step is to reduce temperature and pressure to more handy working levels. A pressure reduction valve takes care of the high pressure and the primary heat exchanger decreases the temperature. A bypass valve leads hot air past the primary heat exchanger and this air is used to roughly control the temperature. After these pressure and temperature adjustments, a small amount of air is distributed to the windshield defroster and to the pressurization of tanks and gearboxes.

If the engine is shut down for some reason, or if it is desired not to load the engine any more, the APU can supply the ECS with air.

3.1.2 Air conditioning

The air conditioning section, more often called the "cooling pack", controls the airflow through the system and sees to it that the air delivered to the distribution system is dehumified and cold enough.

The cooling pack starts with a pressure control valve used to control the pressure at the cooling pack outlet. From this valve the air is led to a compressor that increases the air pressure and temperature. Then it is cooled again in the secondary heat exchanger, followed by a condenser and a water separator. To dehumify the air is of great importance to protect the avionics.

Finally the air expands through a cooling turbine, and hereby the temperature decreases below the freezing temperature. In order to attain the desired temperature 0°C, hot air from the cool-

ing pack inlet is bypassed the compressor and cooling turbine, and mixed with the cold air at the cooling pack outlet.

3.1.3 Air distribution

Figure 3.2 shows an overview of the air distribution subsystem. The Saab notation for the three control valves is 14HA, 15HA and 16HA.
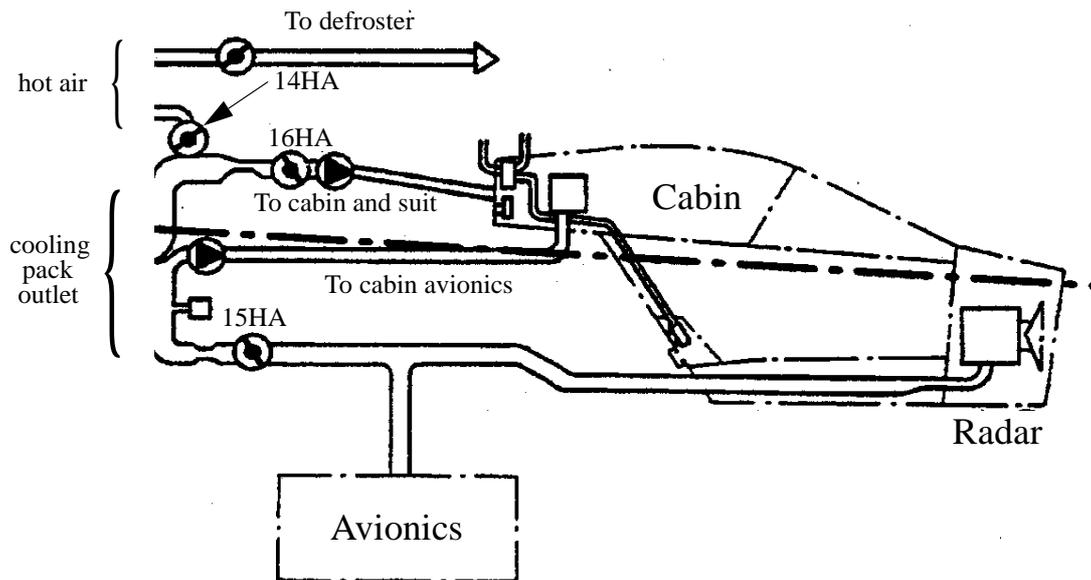
Figure 3.2: The air distribution system

When the air enters the air distribution subsystem it is immediately divided into three flows, through 16HA to the cabin, to the radar and avionics via 15HA and a small flow to the cabin avionics. The air used to cool the avionics is taken directly from the cooling pack outlet, and the flow is controlled by 15HA. Valve 15HA always provides enough cooling power to prevent radar and avionics from becoming overheated.

The cabin airflow, which is controlled by 16HA, is a mixture from cold air directly from the cooling pack outlet and hot air taken before the compressor. The temperature of this air is set by the pilot, who affects the temperature control valve, 14HA.

Cabin pressure is automatically controlled by a mechanical valve regulating the cabin outlet flow. There is also a safety valve to prevent unacceptable cabin pressures. This safety valve is controlled by a mechanism comparing cabin and ambient pressure, and if the difference is too large the mechanism opens the valve.

3.2 ECS components

As mentioned earlier no data from a real ECS has been available, so an Easy5-model of the ECS had to replace the real system. Two more theses also dealing with model based diagnosis of the Gripen ECS have been carried out ([6] and [7]), but the ECS-component models used in them did not comply very well with the Easy5-model. In [6] and [7] most models come from [8]. In [7], these models were applied to measured data from a limited part of the air distribution subsystem, and in [7] these models worked fine. This is perhaps a reason not to put too

much trust in the Easy5-model. However, new models had to be developed since the real system was replaced by the Easy5-model.

3.2.1 Venturi

In the ECS venturis are used to measure flows. A venturi is a flow restriction causing the least possible energy loss. It has a rounded inlet and a smooth outlet profile. By measuring the decrease in static pressure over the venturi, the upstream static pressure and the temperature, the GECU can calculate the flow through the nozzle. This arrangement is better known as a venturimeter, and since it does not steal so much energy from the system, and thereby does not affect the process significantly, it is a good flow meter. More about venturimeters can be found in [8].

No venturis are used in the model and they were dealt with only to explain how flows are measured in the real ECS.

3.2.2 Orifice

An orifice is a sharp edged flow restriction in a duct. Since the orifice is a more correct model than a venturi when dealing with turbulent airflows, it has been used when modelling the system. More about orifices can be found in [8].
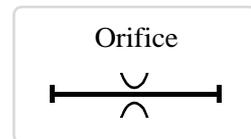
The flow through an orifice is modelled by the expression:

$$\dot{m} = \frac{A P_u K(P_u/P_d)}{\sqrt{RT}} \tag{3.1}$$

where

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

A = orifice area [m^2]

P_u = upstream pressure [Pa] (abs)

P_d = downstream pressure [Pa] (abs)

T = temperature [K]

R = gas constant = 287 [J/(kgK)]

$K(P_u/P_d)$ = look-up-table [-]

The look-up-table $K(P_u/P_d)$ contains different K:s for corresponding values of P_u/P_d. The value of K depends on the media flowing through the orifice and the geometric shape of the flow restriction. The values of K used in Easy5 has probably been obtained from measurements on an orifice with air flowing through it. Figure 3.3 shows a plot of the $K(P_u/P_d)$, and there it can be seen that it varies between 0 and 0.69.

An orifice does not affect the temperature at all, so it is the same before as well as after the orifice.
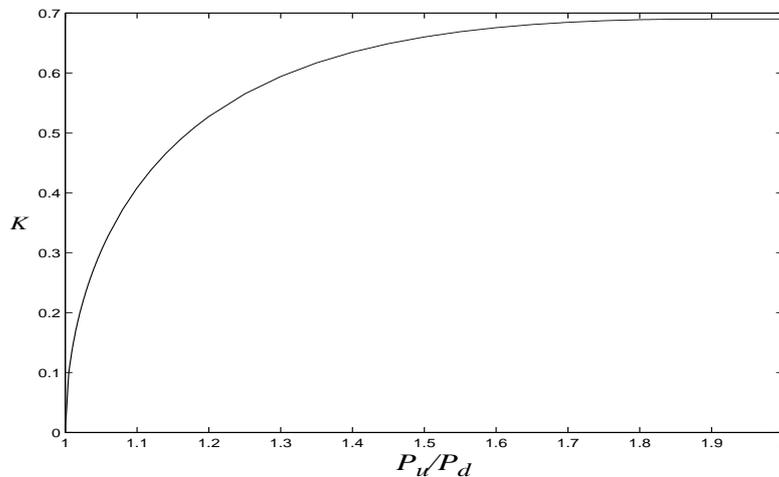
Figure 3.3: K as a function of P_u/P_d

3.2.3 Merging orifices

Orifices in series or parallel can be merged into one equivalent orifice. In the case of parallel orifices this is simple, the resulting orifice area is the sum of the original two. See (3.2).
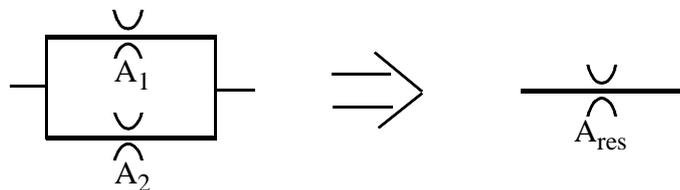
Figure 3.4: Orifices in parallel

The resulting orifice area A_{res} in Figure 3.4 becomes:

$$A_{res} = A_1 + A_2 \qquad (3.2)$$

When it comes to orifices in series it gets more complicated.
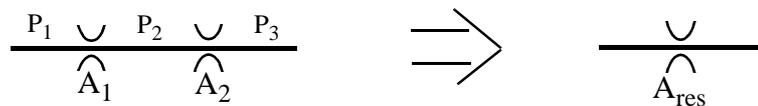
Figure 3.5: Orifices in series

When modelling the flow like in [8], see (3.3), A_{res} can be calculated analytically. By expressing the flow through A_1 and A_2 and assuming they are equal, P_2 can be expressed explicitly. When inserting the P_2 expression in one of the flow equations, A_{res} is found. See (3.4).

$$\dot{m} = \frac{AC}{\sqrt{T}}\sqrt{P_u^2 + P_d^2} \qquad (3.3)$$

where

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

$$A_{res} = \frac{A_2 A_1}{\sqrt{A_2^2 + A_1^2}} \qquad (3.4)$$

When look-up-tables are involved, like in (3.1), A_{res} cannot be calculated analytically. Modelling A_{res} like in (3.4) has been applied to real measurement data in [7] and there it worked satisfactorily. Therefore (3.4) was used here as well, and instead the thresholds had to be adapted to compensate for the model errors introduced.

3.2.4 Valve

The valve is modelled as an orifice with variable area, so the flow through a valve is calculated using (3.1).
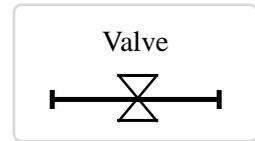
In the ECS almost all valves are of the type "butterfly". The principle of a butterfly valve is shown in Figure 3.6. A butterfly valve consists of a circular disc on a shaft mounted in the centre of a duct. The flow through the valve is controlled by an actuator, which changes the value of θ. When $\theta=0°$, the valve is completely closed and the disc is normal to the axis of the duct.
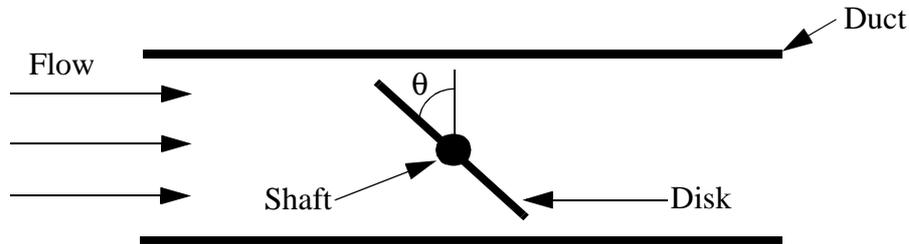
Figure 3.6: The principle of a butterfly valve

The effective area of the valve is calculated by measuring the position of the shaft θ, and using (3.5).

$$A_{eff} = A_0(1 - \cos(\theta)) \qquad (3.5)$$

where

A_{eff} = effective area [m^2]

A_0 = maximum effective area [m^2]

θ = valve angle [°]

The valve actuator model is taken from [9], but some simplifications have been made in order to introduce model errors. Without these simplifications the model complied a bit too well with Easy5 data.

The position of the disc is controlled by a P-regulator implemented in hardware. The simulink actuator model can be seen in Figure 3.7 and the complete valve model can be studied in [9].
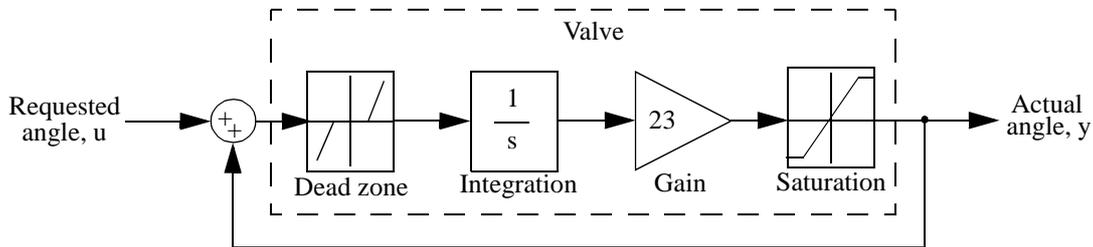
Figure 3.7: Valve model implemented in Simulink

The dead zone models play in the valve, and the saturation models the two end positions of the valve. The size of the dead zone is individual for each valve, while the saturation limits are 5° and 90° for all. The limits are taken from [9].

Written as a transfer function, the simulink model above looks like (provided that y is in between the saturation limits and that u-y is outside the dead zone limits):

$$Y = \frac{U}{\dfrac{s}{23} + 1}$$

(3.6)

which is a simple a LP-filter.

The model presented in Figure 3.7 applies to valves 14HA, 15HA and 16HA. Valves 33HA, 15HAM and 16 HAM will be dealt with in Section 3.3.

3.2.5 Volume

In a constant volume the pressure can be calculated using the ideal gas law, (3.7). The only volume used in the simulink model is the cabin, but unfortunately the air mass in the cabin is unknown. Thereby the ideal gas law like it looks in (3.7) does not offer an opportunity to calculate the cabin pressure.
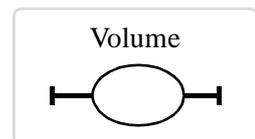
$$PV = mRT$$

(3.7)

where

P = pressure in volume [Pa] (abs)

V = volume [m^3]

m = gas mass in volume [kg]

R = gas constant = 287 [J/(kgK)]

T = temperature in volume [T]

If (3.7) was differentiated the mass would be transformed into mass flow, and mass flow can be estimated using (3.1). When differentiating the ideal gas law the time derivative of temperature turns up, which is not known. It is also hard to estimate it, because friction from the air when flying fast and sunlight warming up the cabin are two major disturbances. However, the temperature varies a lot slower than pressure and flow do, so constant temperature is assumed. Differentiating (3.7) now yields:

$$\frac{d}{dt}(PV = mRT) \Rightarrow \dot{P} = \frac{RT}{V}\dot{m} \tag{3.8}$$

The mass change $\dot{m}$ in (3.8) is calculated as $\dot{m}_{in} - \dot{m}_{out}$, i.e. mass flow in minus mass flow out of the volume. Now (3.8) looks like:

$$\dot{P} = \frac{RT}{V}(\dot{m}_{in} - \dot{m}_{out}) \tag{3.9}$$

3.3 Distribution subsystem model

The simplified model of the distribution subsystem (see Figure 3.8) has been constructed from the components described in Section 3.2. The air flows left to right in the figure.

Figure 3.8: Simplified model of the ECS distribution system

The locations of the sensors available in the system today can be seen in Figure 3.8, and they are:

> Temperature sensors
> 78HA, hot air temperature
> 21HA, cooling pack outlet temperature
> 38HA, mixed air temperature
> 19HA and 77HA, avionics cooling air temperature
> 13HA, cabin outlet temperature

Pressure sensors
17HA, cooling pack outlet pressure
12HA, cabin pressure

Flow sensors
32HA, flow through 16HA
30HA, flow through 15HA

Besides the sensors mentioned above ambient pressure (P_{amb}) is measured and used in the model and the diagnosis system. This sensor is situated elsewhere in the aircraft and therefore it is not present in Figure 3.8.

When it comes to 32HA and 30HA they are not really flow sensors. Instead they measure the differential pressure over a venturi, as mentioned in Section 3.2.1. To calculate, for instance the flow through valve 15HA, the GECU uses (3.10). For further details, see [5].

$$\dot{m}_{15} = C_{21}\sqrt{\frac{P_{17}P_{30}}{T_{19}}} \tag{3.10}$$

where

m_{15} = flow through valve 15HA [kg/s]

C_{21} = constant of proportionality [$ms\sqrt{K}$]

P_{17} = pressure measured by 17HA [Pa] (abs)

P_{30} = pressure measured by 30HA [Pa] (diff)

T_{19} = temperature measured by 19HA [K]

As can be seen in Figure 3.8, hot and cold air is mixed before it enters the cabin and the AVS (=Air Ventilated Suit). Then one might think that warm, mixed air finds its way down to the avionics, radar and cabin avionics as well, but this is not the case. There is in fact a non return valve between the cooling pack outlet and hot air outlet, preventing hot air from coming down.

When building the model, the system was divided into subsystems in order to simplify the modelling process. These subsystems will now be dealt with in detail.

3.3.1 Avionics branch

The avionics branch includes the four components 15HA, 33HA, avionics and radar. The avionics orifice in Figure 3.8 represents the aircraft's main avionics, which consists of more than 15 electronic boxes. In reality there are lots of pipes leading to all these boxes, but the resistance exerted on the air is modelled as a single flow restriction. Valve 15HA controls the cooling air flow to the avionics, which is a very important task, since the avionics literally keeps the aircraft flying.

Also the resistance exerted by the radar is modelled as a single orifice. Valve 33HA is a "shut off" valve, working with only two discrete positions, open or closed. When it is not still it always operates at full speed on its way between the two positions. If the amount of cooling air is not enough to keep the avionics at operational temperature, the radar is what is shut down first. Its cooling air is then redirected to the avionics by closing valve 33HA.

Unfortunately, no pressure sensor is available on the avionics branch. There is one at the cooling pack outlet (17HA), and then we have ambient pressure. This means the pressure loss over the entire avionics branch is the only thing known. Therefore all four components have to be merged into one flow restriction, using (3.4) and (3.2), and this yields:

$$\dot{m}_{15} = \frac{(A_{33ra} + A_{av})A_{15}}{\sqrt{(A_{33ra} + A_{av})^2 + A_{15}^2}} \frac{P_{17}K(P_{17}/P_{amb})}{\sqrt{RT_{19}}} \tag{3.11}$$

where

$$A_{33ra} = \frac{A_{33}A_{ra}}{\sqrt{A_{ra}^2 + A_{33}^2}} \tag{3.12}$$

and

A_{av} = avionics orifice effective area [m^2]

A_{33} = valve 33HA effective area [m^2]

A_{ra} = radar orifice effective area [m^2]

A_{15} = valve 15HA effective area [m^2]

K = the look-up-table described in Section 3.2.2 [-]

R = gas constant = 287 [J/(kgK)]

P_{17}, P_{amb} and T_{19} are pressures and temperature measured by the sensors indicated by each index, just like in (3.10).

Valve 33HA is a bit special since it is only a "shut off" valve, and its position is not measured. There are two switches sensing when the valve has reached one of its end positions, open or closed. Requested valve position is also available as a discrete signal with the two values open or closed. Area A_{33} is calculated using requested valve position and the dynamics of valve 33HA (see Figure 3.9) The dynamics of valve 33HA differs a bit from the valve dynamics presented in Section 3.2.4.
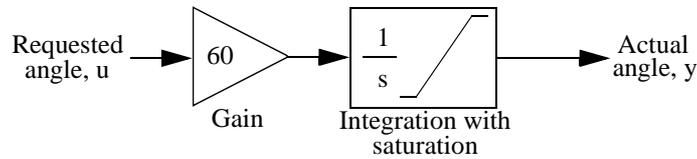
Figure 3.9: Simulink model of valve 33HA

The saturation limits are 5° and 90°, and provided that y is in between these limits, the transfer function of the valve becomes:

$$Y = \frac{60}{s}U \tag{3.13}$$

As mentioned in Section 3.2.2 an orifice does not affect the temperature at all. This means that the temperature is supposed to be the same throughout the entire avionics branch. In reality

this is not the case, but the temperature measured by 21HA at the cooling pack outlet and the one measured by 19HA and 77HA differs only about four degrees at the most, so assuming the same temperature is a good approximation. In Easy5 all these three temperatures are identical, so it does not matter which one is used to calculate the flow in (3.11).

3.3.2 Valve 16HA

Mixed hot and cold air enters valve 16HA, which controls the flow to the cabin. As seen in Figure 3.8 there are two more flows entering the cabin (from AVS and cabin avionics), but they are much smaller than the one coming through 16HA. After passing 16HA the air reaches a series of spray orifices leading to the cabin. These are all modelled as one big orifice. To be able to estimate the flow, valve 16HA and the spray orifice must be merged somehow. But instead of using (3.4), a numerical solution will be calculated in every instant. Since it is known that the same flow flows through both 16HA and the spray orifice, (3.14) can be constructed. From (3.14) a numerical value of P_{mid} is obtained, and by inserting this value in for instance the right side of (3.14), the flow can be calculated. This method takes more computer-power, but gives a better flow estimation.

$$\dot{m}_{16} = \frac{A_{16}P_{17}K(P_{17}/P_{mid})}{\sqrt{RT_{38}}} = \frac{A_{so}P_{mid}K(P_{mid}/P_{12})}{\sqrt{RT_{38}}} \tag{3.14}$$

where

P_{mid} = pressure between valve 16HA and the spray orifice [Pa]

A_{16} = effective area of valve 16HA [m^2]

A_{so} = effective area of the spray orifice [m^2]

Valve 16HA has variable area, and after measuring the position of the actuator shaft, (3.5) is used to calculate the effective area. The maximum area of valve 16HA and the constant area of the spray orifice have been taken from [9]. The valve dynamics of 16HA have been described earlier in Section 3.2.4. An evaluation of how well the valve 16HA-model, and all other models presented in this chapter, correspond to Easy5-data can be found in Section 4.2.

3.3.3 Cabin avionics

The resistance exerted on the air by the cabin avionics is just like in the avionics case modelled as a single flow restriction. The flow $\dot{m}_{ca}$ is modelled:

$$\dot{m}_{ca} = \frac{A_{ca}P_{17}K(P_{17}/P_{12})}{\sqrt{RT_{21}}} \tag{3.15}$$

where

A_{ca} = effective orifice area of the cabin avionics [m^2]

3.3.4 Air Ventilated Suit (AVS)

The AVS-branch is a quite problematic subsystem, since there are no measurement signals from any of the components situated on it. The components in question are: pressure control valve 24HAM, flow control valve 20HAM and the suit itself.

The pressure control valve 24HAM is controlled by a mechanical PI-controller, which is fed with measured cabin pressure and estimated AVS pressure. A slightly higher AVS pressure than cabin pressure is desired in order to ensure an airflow through the AVS.

The flow is manually regulated by the pilot through a three way valve, 20HAM, so there is no way of knowing how big the effective opening area is. The three way valve divides the incoming flow into two flows. One enters the suit and the other enters the cabin. The flow resistance exerted by the AVS varies depending on how big and how tight the AVS in question is, so the flow through it cannot be estimated.

If it was known when the three way valve was set to let all air out in the cabin the flow could be estimated then. However, this is not very common. Most of the time at least some air is lead into the AVS.

Summing up, the AVS flow cannot be estimated, but it is known how big it can be at the most. The pipe leading into the suit has the biggest area, so by assuming all air is lead into the suit and that no suit is connected, an absolute maximum value of the AVS flow can be obtained. This is why the suit and the three way valve are modelled only as a single orifice, as seen in Figure 3.8.

Maximum AVS flow is calculated using (3.16) in combination with the numerical method described in Section 3.3.2. The effective area of the AVS orifice, A_{AVS}, has been taken from [9]. The effective opening area of valve 24HAM, A_{24}, is decided by the modelled PI-controller mentioned above.

$$\dot{m}_{AVSmax} = \frac{A_{AVS}P_{AVS}K(P_{AVS}/P_{12})}{\sqrt{RT_{38}}} = \frac{A_{24}P_{17}K(P_{17}/P_{AVS})}{\sqrt{RT_{38}}} \tag{3.16}$$

3.3.5 Cabin outlet valves

The cabin has two outlet valves, 15HAM and 16HAM. These two are pneumatically controlled by the mechanical pressure regulator 13HAM, see [4]. 13HAM compares cabin and ambient pressure and controls the valves from how much the two pressures differ from each other. I have modelled 13HAM as a PI-controller, since this is how it is done in [9].

Valves 15HAM and 16HAM are not butterfly, but gate valves, and they do not entirely comply with (3.1). The effective area is fixed to its maximum value and instead a loss factor is calculated for different values of the opening area. This loss factor in turn affects the second argument to the look-up-table K, which in this case is not the downstream pressure, but a function of upstream pressure, downstream pressure and the loss factor, see (3.17). Thus instead of directly affecting the flow, the valve area affects the value of K. For further details, see the Simulink model file or [9].

$$\dot{m}_{co} = \frac{A_{co0}P_{12}K(P_{12}/(f(P_{12}, P_{amb}, L(A_{co}))))}{\sqrt{RT_{13}}} \tag{3.17}$$

where

A_{co0} = cabin outlet valves maximum effective area [m^2]

A_{co} = cabin outlet valves effective area [-] (normalized area)

L = loss factor [-]

f = function describing the influence of the opening areas on K [Pa]

3.3.6 Cabin

The cabin pressure can be modelled using (3.9).

$$\dot{P}_{cab} = \frac{RT_{13}}{V_{cab}}(\dot{m}_{16} + \dot{m}_{ca} + \dot{m}_{AVS} - \dot{m}_{co}) \tag{3.18}$$

where

V_{cab} = cabin air volume [m^3]

Since $\dot{m}_{AVS}$ is unknown, (3.18) is not a perfect model of the cabin pressure, but the model error introduced does not affect the modelled cabin pressure significantly.

3.4 Extended distribution subsystem model

The purpose of this thesis is to examine where in the distribution subsystem new sensors might be useful, and with new sensors the model can of course be extended. Only one new sensor is suggested to be introduced, and that is a pressure sensor measuring the pressure upstream valve 14HA. Why this sensor was chosen, and why this was the only new sensor suggested to be introduced will be explained in Section 4.3.

Naturally the models presented in Section 3.3 still applies, but the new sensor enables an enlargement of the distribution subsystem model. When the pressure before valve 14HA is known it is possible to calculate the flow through it.

$$\dot{m}_{14} = \frac{A_{14}P_{hot}K(P_{hot}/P_{12})}{\sqrt{RT_{78}}} \tag{3.19}$$

where

A_{14} = valve 14HA effective area [m^2]

P_{hot} = pressure upstream valve 14HA [Pa] (abs)

This new sensor also improves the diagnosis of the system, which is the reason to introduce it. This will be shown in Section 4.3.

Chapter 4

Diagnosis of the distribution subsystem

Two diagnosis systems have been developed. The first one constructed uses only sensors available in the system today (i.e. those displayed in Figure 3.8). This diagnosis system is then evaluated. It is sorted out which faults can be detected, and which additional faults it is desired to detect. When these additional faults are known, a new sensor is introduced in the system. The model is extended with the new sensor, see Section 3.4, and a new diagnosis system is also developed.

These two diagnosis systems together with all modelled faults will be presented in this chapter.

4.1 Fault models

How a fault is modelled is an important issue. The more knowledge there is about the fault and how it affects a certain component, and thereby the process, the easier it is to detect and isolate it. A fault model can for instance look like:

$$y_{obs}(t) = y_{corr}(t) + f(t) \tag{4.1}$$

$$y_{obs}(t) = y_{corr}(t) + f \tag{4.2}$$

$$y_{obs}(t) = (1 + f)y_{corr}(t) \tag{4.3}$$

where

$y_{obs}(t)$ = observed value of $y(t)$
$y_{corr}(t)$ = correct value of $y(t)$
f = fault affecting $y(t)$

In (4.1) the fault is modelled as an arbitrary additive signal. This is a very general model and covers all possible faults. If a fault's influence on the process is unknown this is a good model to use. The disadvantage is that this fault model gives little help when trying to isolate faults.

In (4.2) and (4.3) f is a constant, time-invariant signal. Here the influence of the fault is restricted and it gets easier to isolate the fault.

In this thesis all fault models are of type (4.1), since most of the modelled faults have never occurred. When it comes to those that has occurred not enough knowledge about how they affect the process has been gathered.

4.1.1 Fault modes

Since the Gripen has been operational for quite a long time, a lot of experience on what components tend to break down has been gathered, and as in all kinds of systems, moving parts have shown error prone. When designing the diagnosis system all kinds of faults were considered, but priority was given to detection and isolation of faults that had actually occurred in the aircraft.

The following fault modes were modelled:

Valves

F_{V14}	valve 14HA jamming
F_{V15}	valve 15HA jamming
F_{V16}	valve 16HA jamming
F_{V33}	valve 33HA jamming
F_{Vo}	valve 15HAM or 16 HAM jamming
$F_{\Theta14}$	valve 14HA position sensor
$F_{\Theta15}$	valve 15HA position sensor
$F_{\Theta16}$	valve 16HA position sensor

Sensors

F_{T13}	temperature sensor 13HA (cabin outlet)
F_{T19}	temperature sensor 19HA (avionics compartment)
F_{T21}	temperature sensor 21HA (cooling pack outlet)
F_{T38}	temperature sensor 38HA (mixed air)
F_{T77}	temperature sensor 77HA (avionics compartment)
F_{T78}	temperature sensor 78HA (hot air)
F_{Pamb}	ambient pressure sensor
F_{P12}	pressure sensor 12HA (cabin)
F_{P17}	pressure sensor 17HA (cooling pack outlet)
F_{P30}	differential pressure sensor 30HA (venturi before 15HA)
F_{P32}	differential pressure sensor 32HA (venturi before 16HA)

Leakages

F_{Lav}	leakage in the avionics branch

F_{Lcp} leakage in the cabin distribution pipe

F_{Lcab} cabin leakage

Miscellaneous

NF   no fault

F_{PR13} cabin pressure regulator

All these fault models will be dealt with in detail in Section 4.1.2 through Section 4.1.6.

It might seem odd that only three kinds of leakages are modelled, but these three are the only ones possible to detect without introducing any new sensors. Which areas the avionics branch and the cabin distribution pipe refers to is shown in Figure 4.1.
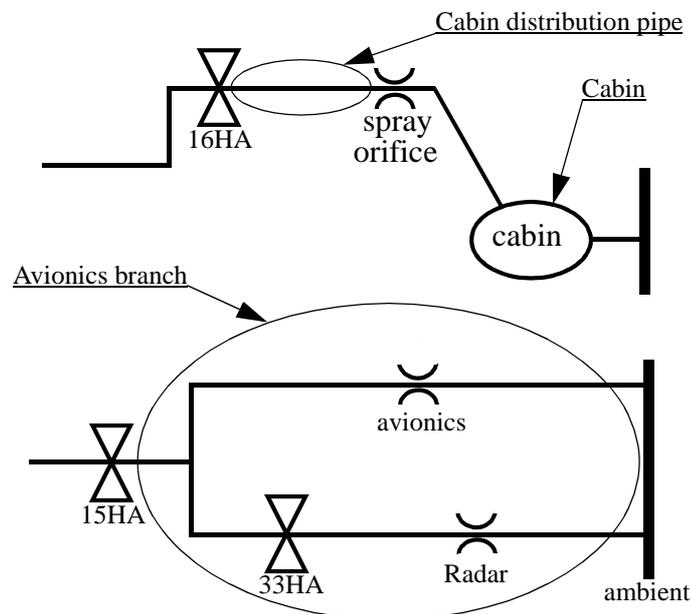
Figure 4.1: Areas where leakage can be detected

4.1.2 Valve jamming

When the valves in the ECS are jamming it is believed to be caused by a malfunctioning electrical servomotor controlling the valve disc. It is probably not due to increased friction or another mechanical phenomenon, as one might think. For some reason the servomotor randomly loses its connection to the driving voltage. This slows the valve down, and at first glance it looks just like increased friction.

Jamming valves are simulated like:

$$u_{obs}(t) \ = \ (1 - f(t))u_{corr}(t) \tag{4.4}$$

where

$u_{obs}(t)$ = observed servo control signal

$u_{corr}(t)$ = desired servo control signal

$f(t)$ = fault

In (4.4) *f(t)* denotes a telegraph signal, which is a signal jumping randomly between its two discrete states 0 and 1.

Even though valves are believed to break down as described in (4.4), nobody knows for sure that this is the only way they break down. Therefore the general fault model, (4.1), is used when modelling jamming valves.

This is because nobody can say for sure the fault will appear as described in (4.4).

4.1.3 Valve position sensors

It is not known how these sensors tend to break, so the general, additive fault model (4.1) has been used in this case.

When simulating a faulty sensor a bias changing its value perhaps every tenth second has been added to the measurement signal.

Since the desired valve position as well as the measured position are known, one might think it would be easy to supervise this component. There is an inner control loop, mentioned in Section 3.2.4, always making sure there is no difference between desired and measured valve position. However, this fault can still be detected, because if a fault occurs the disc is not in the correct position, and then calculated and measured flow through the valve will not match.

4.1.4 Temperature and pressure sensors

These sensors do not break very often and it is not known how, so fault model (4.1) is used here too. This fault model includes the perhaps most likely sensor fault, loose connections. The fault signal can then be said to change randomly between 0 and 1, using the notation from (4.4).

These faults were simulated just like the valve position sensor faults in Section 4.1.3.

4.1.5 Leakage

Leakage in the cabin distribution pipe is simulated by introducing a new orifice leading to the ambient air, situated between valve 16HA and the spray orifice. Cabin leakage is simulated by adding a new exit orifice, and avionics leakage is simulated by increasing the area of one of the exit orifices. Fault model (4.1) is used in all three cases.

4.1.6 Cabin pressure regulator

As mentioned in Section 3.3.5 the cabin pressure regulator is a PI-controller. It is not known how the controlling of the pressure fails, but the regulator probably gets slow or sticks in some way. It is after all a mechanical component with moving parts inside it. When simulating a faulty controller a constant was added to the P- and I-values, causing the controller to be slower than normal. As usual, fault model (4.1) was used.

4.2 Diagnosis system

The diagnosis system using only sensors available today (i.e. those displayed in Figure 3.8) consists of nine test quantities. They are all constructed from the equations used in the system model. All test quantities are described in detail below.

The strategy when designing test quantities is to build as many as possible, and afterwards select and keep the set offering the best performance. It is not obvious what is meant by "best performance", but in this case it could be to isolate as many faults as possible using as few test quantities as possible. Not to use too many and too complicated test quantities is important if only limited computerpower is available.

4.2.1 R_1, avionics flow

As mentioned in Section 3.3.1, all four orifices on the avionics branch must be merged into one if it is desired to estimate the flow through it. Since merging of orifices does not work very well, (again according to Section 3.3.1) this residual offers a great opportunity to show the benefits of adaptive thresholds. The residual looks like:

$$R'_1 = \left| C_F \sqrt{\frac{P_{17}P_{30}}{T_{19}}} - \frac{(A_{33ra} + A_{av})A_{15}}{\sqrt{(A_{33ra} + A_{av})^2 + A_{15}^2}} \frac{P_{17}K(P_{17}/P_{amb})}{\sqrt{RT_{19}}} \right| \tag{4.5}$$

where the notation is taken from (3.10),(3.11) and (3.12).

Multiplying (4.5) with $\sqrt{T_{19}}$ yields:

$$R_1 = \left| C_F \sqrt{P_{17}P_{30}} - \frac{(A_{33ra} + A_{av})A_{15}}{\sqrt{(A_{33ra} + A_{av})^2 + A_{15}^2}} \frac{P_{17}K(P_{17}/P_{amb})}{\sqrt{R}} \right| \tag{4.6}$$

The residual R_1 is used to test the hypothesis H_1^0:

$$H_1^0: \quad F_p \in M_1 = \{\Omega \backslash \{F_{V33}, F_{\Theta 15}, F_{P17}, F_{P30}, F_{Pamb}, F_{Lav}\}\}$$

$$H_1^1: \quad F_p \in M_1^c = \{F_{V33}, F_{\Theta 15}, F_{P17}, F_{P30}, F_{Pamb}, F_{Lav}\}$$

The quantity Ω above includes all fault modes presented in Section 4.1.1. A decision structure showing which test quantities each fault mode affects can be found in Section 4.4.

When determining which fault modes that might affect the residual, i.e. those belonging to M_1^c, one studies which signals are included in the residual. The three sensor signals P_{17}, P_{30} and P_{amb} are all included in R_1, so if one of these sensors is malfunctioning, an alarm might be fired. Therefore the fault modes $\mathbf{F_{P17}}$, $\mathbf{F_{P30}}$ and $\mathbf{F_{Pamb}}$ are included in M_1^c. The area A_{33ra} is affected if valve 33HA is jamming, and that is why $\mathbf{F_{V33}}$ is included. The avionics leakage fault mode, $\mathbf{F_{Lav}}$, is included since a leak affects A_{33ra} or A_{av}. Finally, measured position of valve 15HA is used (together with (3.5)) to calculate the opening area of the valve, and that is why $\mathbf{F_{\Theta 15}}$ also is included.

Even if H_1^0 is not rejected, the fault modes in M_1^c is not excluded as possible fault modes since the *don't care* symbol X (X was thoroughly dealt with in Section 2.5), is used in the decision structure. Thus the decisions corresponding to the hypothesis test H_1^0 looks like:

$$S_1^0 = \Omega \text{ if } H_1^0 \text{ is not rejected}$$

$$S_1^1 = \{F_{V33}, F_{\Theta 15}, F_{P17}, F_{P30}, F_{Pamb}, F_{Lav}\} \quad \text{if } H_1^0 \text{ is rejected}$$

The threshold applied to R_1 is quite complex. It depends on the desired position of valve 15HA, how fast it moves, and whether or not valve 33HA is open. The implementation of the threshold looks like:

$$J_1 = H_{LP}(s)(|H_{HP}(s)u_{15}(t)|) + f(u_{15}, u_{33}) \tag{4.7}$$

where

$\quad\quad u_{15} =$ control signal to valve 15HA

$\quad\quad u_{33} =$ control signal to valve 33HA

$\quad\quad H_{HP} =$ high pass filter

$\quad\quad H_{LP} =$ low pass filter

The filter H_{HP} enlarges the threshold when u_{15} contains high frequencies, since the model uncertainties are then known to be large. The low pass filter is used for smothering of the threshold. The function $f(u_{15}, u_{33})$ returns an offset level suitable for the present valve control signals.

Figure 4.2 shows how the size of the threshold changes in time. The dynamics present was created by moving valve 15HA, and when it moves, the thresholds are enlarged. After about 66 seconds valve 33HA opens, and now the model errors are smaller. Therefore the thresholds can be narrowed.

Solid: measured flow;   Dotted: estimated flow;   Dashed: thresholds
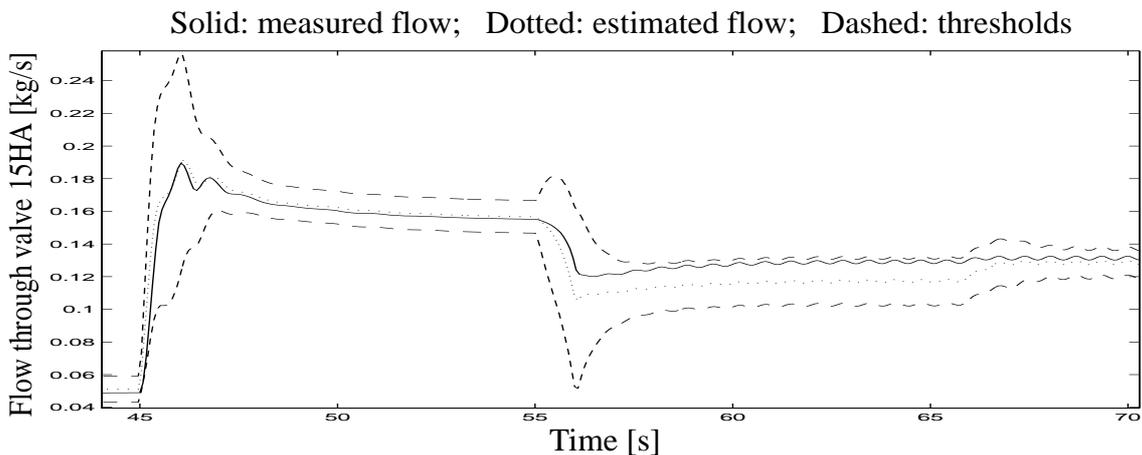
Figure 4.2: Position of valve 15HA vs time

Figure 4.2 shows that R_1, with its corresponding thresholds, manages heavy dynamics without firing an alarm. Figure 4.3 shows what happens when a fault occurs. Valve 33HA is jamming

and does not close as fast as it does in a fault free case. Measured flow exits the area between the thresholds, and an alarm is fired at the time 71.5 s.
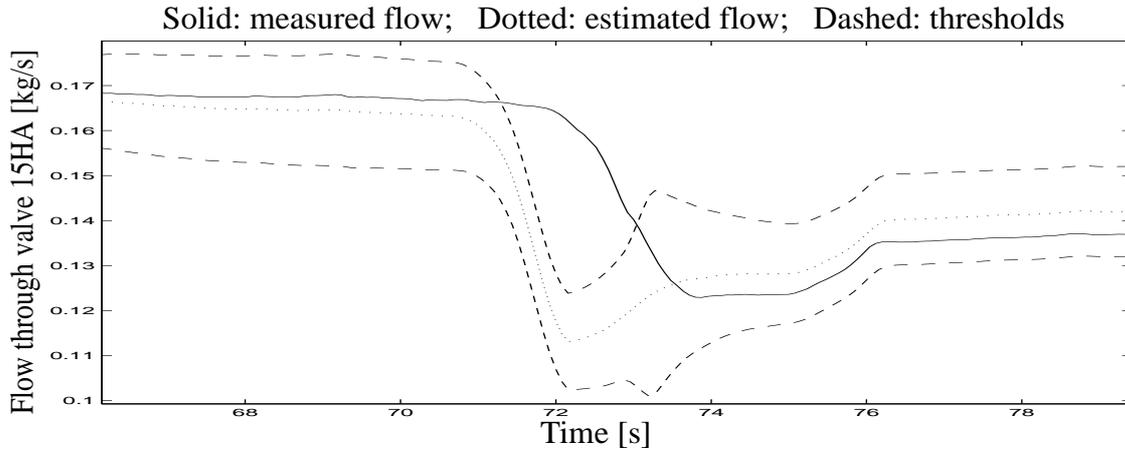
Figure 4.3: Valve 33HA jamming

Figure 4.3 is just an example of what happens when a fault occurs. In Section 4.5 a more complete evaluation of the diagnosis system will be carried out, and it will then be presented how large each fault must be in order to be detected by a certain test quantity.

4.2.2 R_2, cabin flow

The cabin flow residual looks like:

$$R_2 = \left| C_F \sqrt{P_{17} P_{32}} - \frac{A_{16} P_{17} K(P_{17}/P_{mid})}{\sqrt{R}} \right| \tag{4.8}$$

where P_{mid} is calculated as described in Section 3.3.2.

R_2 is used to test the hypothesis H_2^0:

$$H_2^0: \qquad F_p \in M_2 = \{\Omega \backslash \{F_{\Theta 16}, F_{P12}, F_{P17}, F_{P32}, F_{Lcp}\}\}$$

$$H_2^1: \qquad F_p \in M_2^c = \{F_{\Theta 16}, F_{P12}, F_{P17}, F_{P32}, F_{Lcp}\}$$

Figure 4.4 shows estimated and measured flow through valve 16HA with corresponding thresholds, during an engine thrust decrease (at approximately 20 s) and an engine thrust increase (at approximately 46 s). The estimated flow follows the measured flow quite well in spite of the heavy dynamics induced by the engine.

Solid: measured flow;   Dotted: estimated flow;   Dashed: thresholds
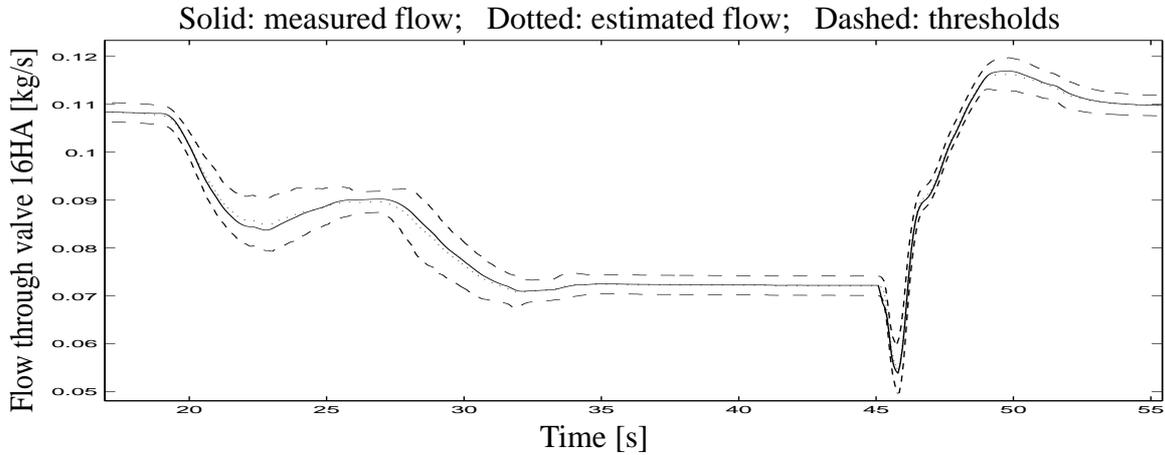
Figure 4.4: Flow through 16HA during engine dynamics

The model uncertainties have proven dependent on the speed and the desired position of valve 16HA, and also the desired position of valve 15HA, so these are the parameters determining the size of the adaptive threshold.

Solid: measured flow;   Dotted: estimated flow;   Dashed: thresholds
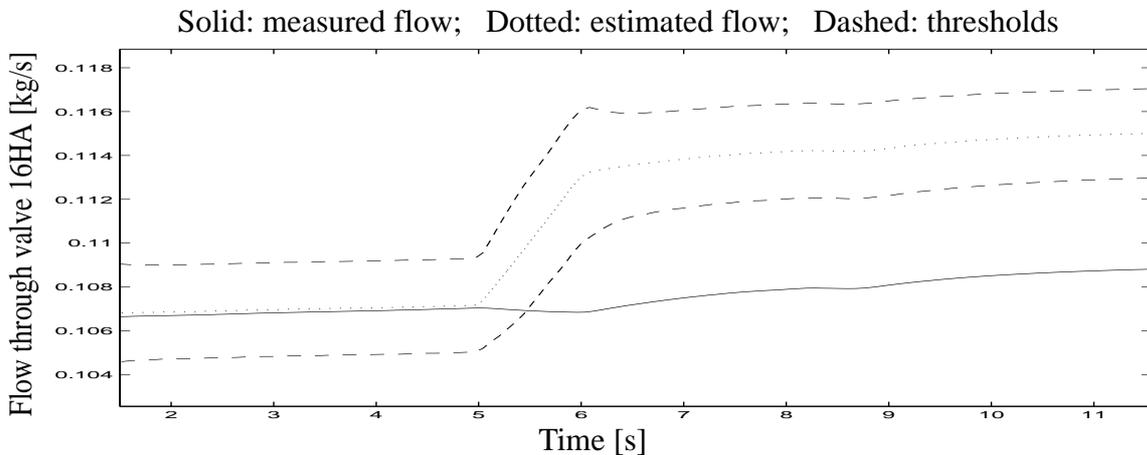
Figure 4.5: Flow through 16HA with a present position sensor fault of 1°

Figure 4.5 shows what happens when a valve position sensor bias fault is introduced. The sensor fault develops gradually between 5 s and 6 s from 0° to 1° positive offset. The model thinks the valve opening area has increased, and therefore estimated flow increases. The flow increase might seem a bit large to be caused by only a 1° offset, but the effect of a position sensor bias depends on the valve position. Also, if true valve position was changed, the up- and downstream pressures would be affected, preventing the flow from increasing as much as it did here.

Even if a fault of only 1° was easy to spot this time, one cannot say a fault of that size will always fire an alarm. The effect of the fault in this case depends on for instance valve position.

4.2.3 R_3, R_4, R_5, valve dynamics

Valve dynamics is modelled as described in Section 3.2.4, and the residual is:

$$R_i = \left| \Theta_{j,\,meas} - \Theta_{j,\,calc} \right| \tag{4.9}$$

where

Θ_{meas} = measured valve position

Θ_{calc} = calculated valve position

$i = \{3,4,5\}$

$j = \{14,15,16\}$, representing valves 14HA, 15HA and 16HA

The corresponding hypothesis tests are:

$$H_3^0: \qquad F_p \in M_3 \;=\; \{\Omega \backslash F_{\Theta 14}\}$$

$$H_3^1: \qquad F_p \in M_3^c \;=\; \{F_{\Theta 14}\}$$

$$H_4^0: \qquad F_p \in M_4 \;=\; \{\Omega \backslash F_{\Theta 15}\}$$

$$H_4^1: \qquad F_p \in M_4^c \;=\; \{F_{\Theta 15}\}$$

$$H_5^0: \qquad F_p \in M_5 \;=\; \{\Omega \backslash F_{\Theta 16}\}$$

$$H_5^1: \qquad F_p \in M_5^c \;=\; \{F_{\Theta 16}\}$$

When thresholding R_3, R_4, and R_5 an adaptive threshold of the form (2.7) has been used. The valve model errors are large when the valve disc moves rapidly, so the thresholds are enlarged when the control signal reaches high frequencies.

Solid: measured angle;   Dotted: estimated angle;   Dashed: thresholds
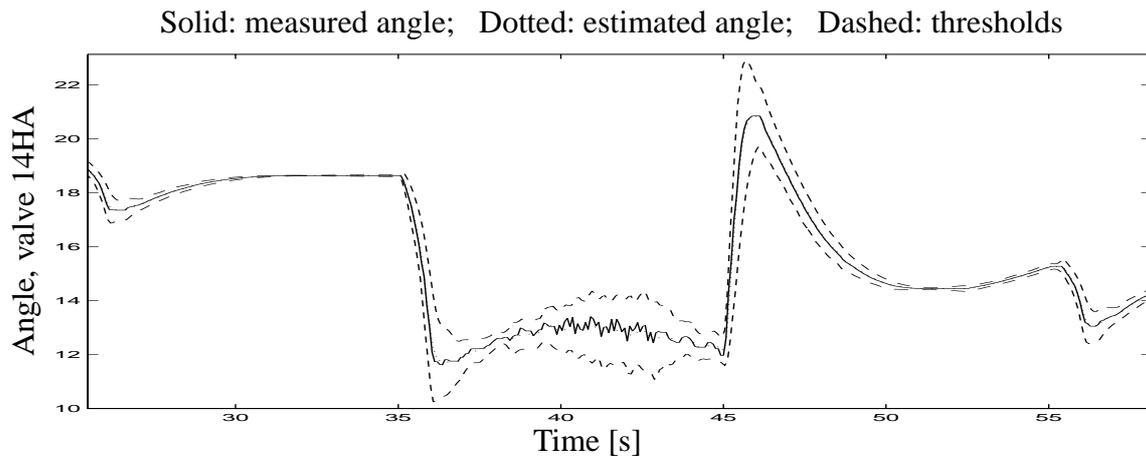
Figure 4.6: Position of valve 14HA vs time

Figure 4.6 shows how well the model of valve 14HA corresponds to Easy5 data during relatively moderate dynamics. Figure 4.7 shows the corresponding residual, R_3, and its thresholds. In Figure 4.7 it is clearly shown how the threshold varies with valve movement. Just by looking at the figure, one might think the threshold would react to a fault and be enlarged when the difference between measured and estimated position increases. However, this is not the case, since the variation of the threshold depends on control signals only, see (2.7).

Solid: residual;   Dashed: thresholds
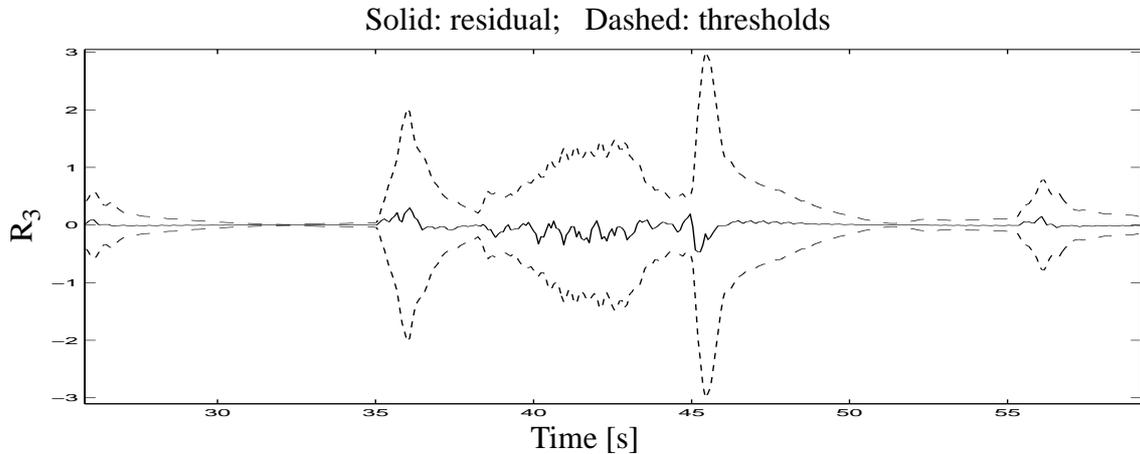
Figure 4.7: Residual R_3 and its thresholds during moderate dynamics

The thresholds seem to be unnecessary enlarged when the valve moves, but they need to be large in case of heavier dynamics, see Figure 4.8.
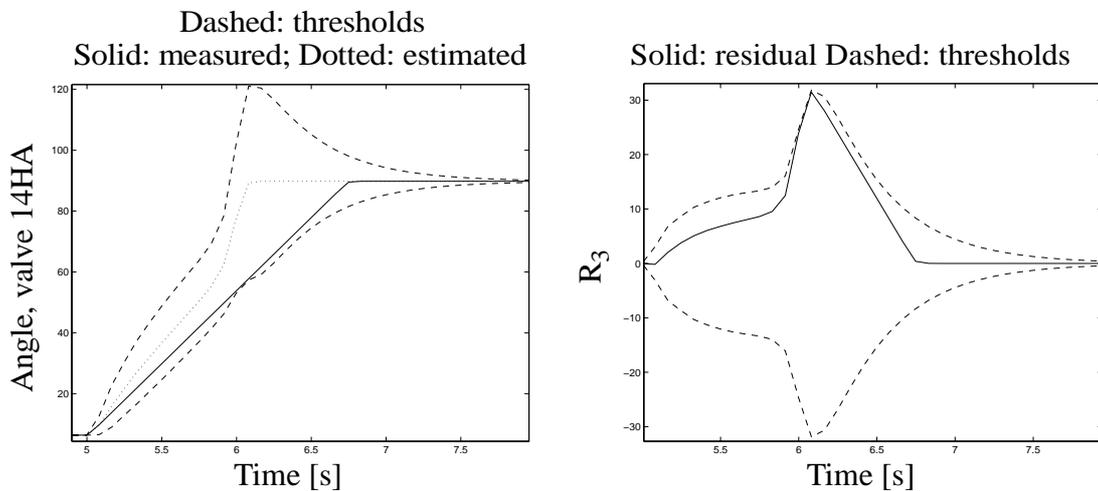
Figure 4.8: Residual R_3 and its thresholds during strong dynamics

As mentioned in Section 4.1.2 valve jamming is probably caused by a malfunctioning servo motor, which slows the valve down. Figure 4.9 shows the result of a jamming valve simulation
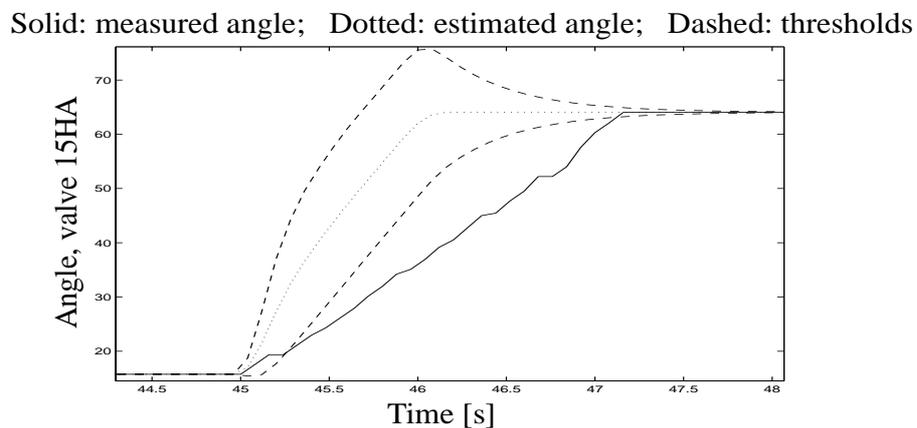
Figure 4.9: Valve 15HA jamming

4.2.4 R_6, R_7, R_8, temperature residuals

The temperature residuals compare the signals from the three temperature sensors 21HA, 19HA and 77HA. All these three signals equal each other in the Easy5-model, as discussed in Section 3.3.1, so diagnosis of the sensors is very simple to perform. In reality the temperatures seem to differ about 4 K at the most, so diagnosis should not be so complicated then either. A constant threshold slightly greater than 4 K would probably do. Diagnosis of these three temperature sensors using real measurement data has been undertaken in [7].

The residuals look like:

$$R_6 = \left| T_{19} - T_{77} \right| \tag{4.10}$$

$$R_7 = \left| T_{19} - T_{21} \right| \tag{4.11}$$

$$R_8 = \left| T_{21} - T_{77} \right| \tag{4.12}$$

with the corresponding hypothesis tests:

$$H_6^0: \qquad F_p \in M_6 = \{\Omega \backslash \{F_{T19}, F_{T77}\}\}$$
$$H_6^1: \qquad F_p \in M_6^c = \{F_{T19}, F_{T77}\}$$

$$H_7^0: \qquad F_p \in M_7 = \{\Omega \backslash \{F_{T19}, F_{T21}\}\}$$
$$H_7^1: \qquad F_p \in M_7^c = \{F_{T19}, F_{T21}\}$$

$$H_8^0: \qquad F_p \in M_8 = \{\Omega \backslash \{F_{T21}, F_{T77}\}\}$$
$$H_8^1: \qquad F_p \in M_8^c = \{F_{T21}, F_{T77}\}$$

4.2.5 R_9, cabin pressure observer

The cabin pressure is estimated using the observer (4.13).

$$\dot{\hat{P}}_{12} = \frac{RT_{13}}{V_{cab}} (\dot{m}_{16} + \dot{m}_{ca} - \dot{m}_{co}) + K_F (P_{12} - \hat{P}_{12}) \tag{4.13}$$

The flow $\dot{m}_{16}$ in (4.13) is the "measured" flow, i.e. the flow delivered by the GECU. The two flows $\dot{m}_{ca}$ and $\dot{m}_{co}$ are calculated using (3.15) and (3.17), but now the equations are fed with estimated cabin pressure, $\hat{P}_{12}$, instead of measured, P_{12}. The flow $\dot{m}_{AVS}$ is approximated with a constant.

When choosing the feedback gain K_F, the method described in Section 2.6.2 is used. That means the system is linearized around a working point, and then a linear observer design is carried out.

The obvious residual to construct here would be a comparison between estimated and measured cabin pressure, but this is not such a good idea. Cabin pressure is controlled by a PI-controller steering the two outlet valves, see Section 3.3.5. No measurement signals are available neither from the outlet valves, nor the PI-controller. This means that the real PI-controller and its valves can perform completely different from its modelled counterparts without us knowing. If for instance a leak occurs, the PI-controller of the real system will close the outlet valves a little, which forces cabin pressure back up to normal. If cabin pressure was compared, the pressures would only differ for a short time before the outlet valves had closed enough.

Any fault affecting either the true or the modelled pressure will be compensated for by the corresponding PI-controller, forcing the pressure back to the intended level. The pressure is forced back by changing the opening area of the outlet valves. Say for instance that the differential pressure sensor P_{30} constantly delivers a too small value, i.e. a negative bias sensor fault is present. The model then assumes a too low flow through valve 16HA, and estimated cabin pressure will decrease. In order to maintain the desired cabin pressure level, the modelled PI-controller will open its outlet valves a little, and due to this action the positions of the modelled and the real outlet valves now differ from each other. Summing up, what changes permanently after the introduction of a fault are the opening areas of the outlet valves, and thus comparing outlet valve opening areas is a good way to find difference between model and process behaviour.

Normally faults cannot be detected when this kind of inner control loop is present, since the output signal of the controller usually is not known. In this specific case however, the output signals of both the modelled and the true controller can be calculated, and this enables fault detection. The input signals to the true controller are ambient pressure and measured cabin pressure, while it is ambient pressure and estimated cabin pressure to the modelled one. The residual now becomes:

$$R_9 = \left| A_{co}(P_{12}, P_{amb}) - A_{co}(\hat{P}_{12}, P_{amb}) \right| \tag{4.14}$$

In (4.14) A_{co} is a model of the cabin pressure PI-controller.

The hypothesis tested with (4.14) looks like:

$$H_9^0: \qquad F_p \in M_9 = \begin{Bmatrix} F_{V14}, F_{V15}, F_{V16}, F_{V33}, F_{\Theta 14}, F_{\Theta 15} \\ F_{\Theta 16}, F_{T19}, F_{T77}, F_{T78}, F_{P30}, F_{Lav} \end{Bmatrix}$$

$$H_9^1: \qquad F_p \in M_9^c = \begin{Bmatrix} F_{PR13}, F_{Vo}, F_{T13}, F_{T21}, F_{T38}, F_{P12} \\ F_{P17}, F_{P32}, F_{Pamb}, F_{Lcp}, F_{Lcab} \end{Bmatrix}$$

How well does the cabin pressure observer correspond to the Easy5 model then? Figure 4.10 shows estimated and measured cabin pressure during the same engine dynamics used in Section 4.2.2. Estimated pressure does not follow very well during the transients, but after a while it finds its way back again.

Solid: measured pressure;   Dotted: estimated pressure;
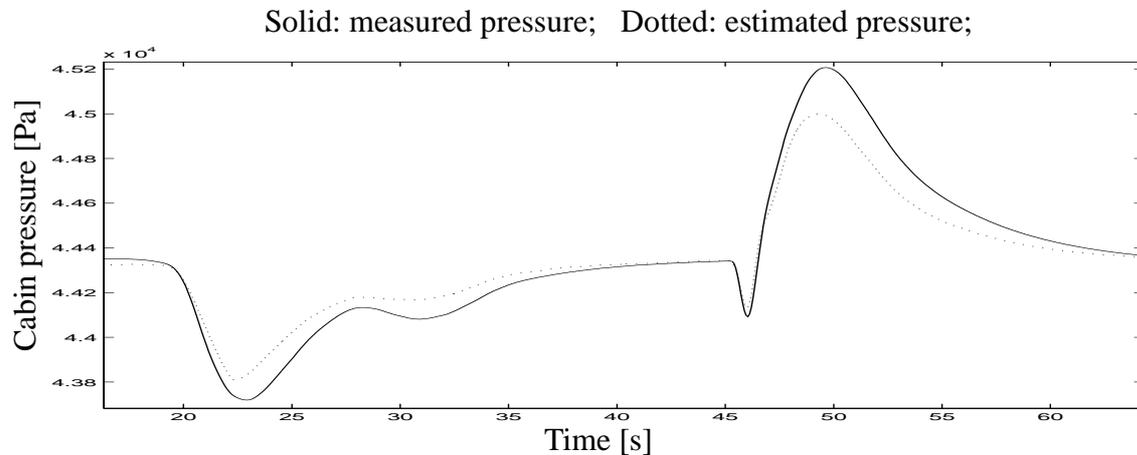
Figure 4.10: Cabin pressure during engine dynamics

To illustrate the effect of a fault on R_9 a leak in the cabin of about 13 cm^2 was gradually introduced between 25 and 26 s. The result is shown in Figure 4.11. The solid line is the outlet valve opening area of the system, i.e. $A_{co}(P_{12}, P_{amb})$, while the dotted line represents the opening area calculated by the model, $A_{co}(\hat{P}12, P_{amb})$. The thresholds are as usual represented by the dashed lines, and for this residual a constant threshold of 0.1 has been chosen.

Solid: system opening area;   Dotted: model opening area;   Dashed: thresholds
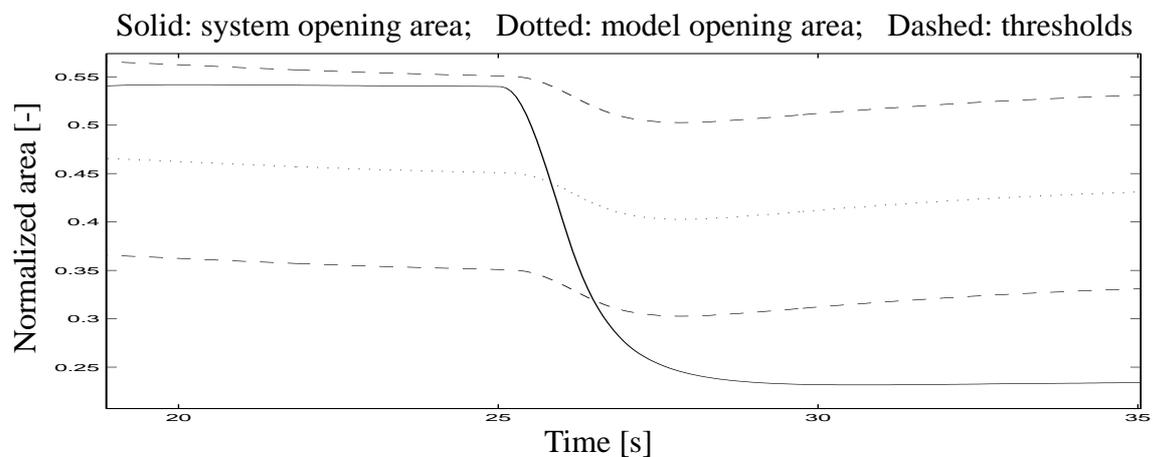
Figure 4.11: R_9 with cabin leakage

When the leak occurs the cabin pressure decreases. This is sensed by the cabin pressure controller, which starts closing the outlet valves. As can be seen in Figure 4.11, the modelled opening area also reacts a little to the leak, and this is due to the observer feedback where measured cabin pressure is included.

In Figure 4.11 the opening area of the system lies close to the upper threshold before the leak is introduced. Therefore only quite large leaks are detected, but in another operating point, the solid line might be closer to the lower threshold, and a smaller leak can be detected.

4.2.6 What could be achieved using the sensors available today?
Experience shows that moving parts often are the most weak link in all kinds of systems, so they are obviously important components to supervise. The moving parts present in the distri-

bution part of the ECS are valves, valve position sensors and mechanical pressure controllers. All moving parts, except for those situated on the AVS-branch and the position sensor of valve 14HA can be supervised with the sensors available in the system today. However, cooling of the AVS is not crucial for safe operation of the aircraft, so the AVS-branch, with its two valves, pressure controller and tube, is not that important to supervise.

Summing up, all faults presented in Section 4.1.1 except for $\mathbf{f_{T78}}$ and $\mathbf{f_{\Theta 14}}$ can be detected with the sensors available in the system today.

4.3 Diagnosis system using the new sensors

If supervision of the AVS-branch is desired even though it is not flight-safety crucial, the pressure downstream, and position of the three way valve must be measured. Then malfunctioning valves, malfunctioning pressure controller and tube leakage can be detected. If only valve 24HAM and its PI-controller was desired to supervise, a pressure sensor between the two valves on the AVS-branch is needed.

Detection of a malfunctioning valve 14HA position sensor can be achieved if a pressure sensor is installed upstream the valve. This valve is used to control cabin temperature and if it breaks down it might get very hot in the cabin, so this is an important component to supervise.

The introduction of the new pressure sensor also enables supervision of temperature sensor 78HA.

With the new pressure sensor the flow through 14HA, $\dot{m}_{14}$, can be estimated using (3.19). If equation (3.19) is combined with the two static relations (4.15) and (4.16) a new residual, R_{10} is obtained.

$$\dot{m}_{16} + \dot{m}_{AVS} = \dot{m}_{14} + \dot{m}_{cold} \tag{4.15}$$

$$\dot{m}_{14}T_{78} + \dot{m}_{cold}T_{21} = (\dot{m}_{14} + \dot{m}_{AVS})T_{38} \tag{4.16}$$

In the equations above $\dot{m}_{AVS}$ is approximated with the same constant it was approximated with in the cabin pressure observer. The flow $\dot{m}_{cold}$ represents the cold air flow from the cooling pack outlet up to where hot and cold air is mixed, see Figure 3.8. The residual R_{10} is constructed by isolating $\dot{m}_{cold}$ in (4.15), substituting it into (4.16) and finally substituting $\dot{m}_{14}$ in (4.16) with (3.19).

$$R_{10} = \frac{A_{14}P_{hot}K(P_{hot}/P_{12})}{\sqrt{RT_{78}}}(T_{78} - T_{21}) + (\dot{m}_{16} + \dot{m}_{AVS})(T_{21} - T_{38}) \tag{4.17}$$

The hypothesis tested with R_{10} looks like:

$$H_{10}^0: \qquad F_p \in M_{10} = \{\Omega \setminus \{F_{\Theta 14}, F_{T78}, F_{T21}, F_{T38}, F_{P17}, F_{P32}, F_{Phot}\}\}$$

$$H_{10}^1: \qquad F_p \in M_{10}^c = \{F_{\Theta 14}, F_{T78}, F_{T21}, F_{T38}, F_{P17}, F_{P32}, F_{Phot}\}$$

A new fault mode is also introduced with the new pressure sensor, $\mathbf{F_{Phot}}$, corresponding to a faulty sensor.

In (4.17) $\dot{m}_{AVS}$ is included, and since it is approximated with a constant a model error is introduced here. Fortunately the maximum and minimum values of $\dot{m}_{AVS}$ can be estimated, and hereby the maximum model error introduced by $\dot{m}_{AVS}$ can be obtained and used to adapt the threshold. Maximum AVS-flow is estimated using (3.16), and the minimum flow is set to one fourth of the maximum value. The threshold is also adapted with an expression of the type (2.7) reacting on the control signal to valve 14HA. The response of the threshold and residual during the usual engine dynamics is shown in Figure 4.12.

Solid: residual;   Dashed: thresholds
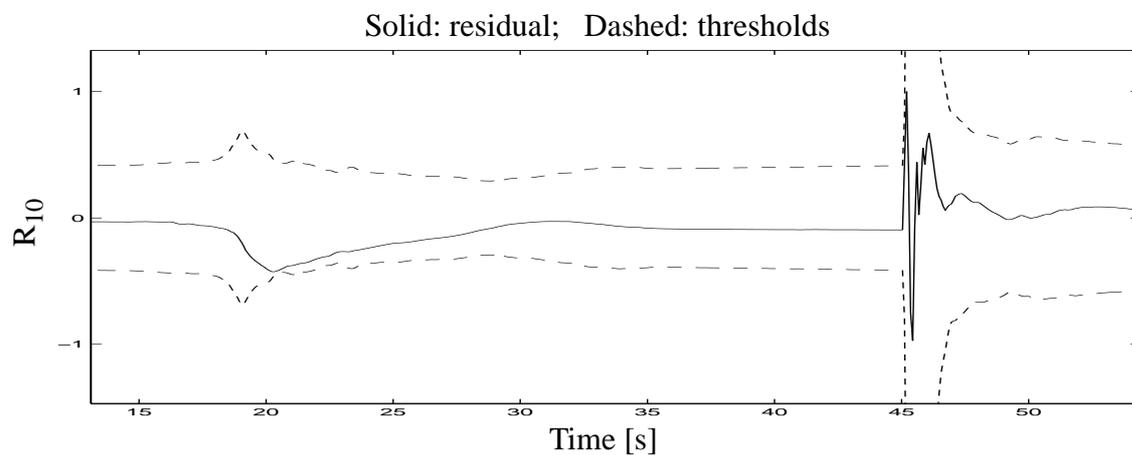
Figure 4.12: R_{10} during engine dynamics

At last the response of R_{10} to a temperature sensor offset is shown, see Figure 4.13. Between 25 and 26 s a fault of about 33 K is gradually introduced, and the residual exits its allowed area between the thresholds.

Solid: residual;   Dashed: thresholds
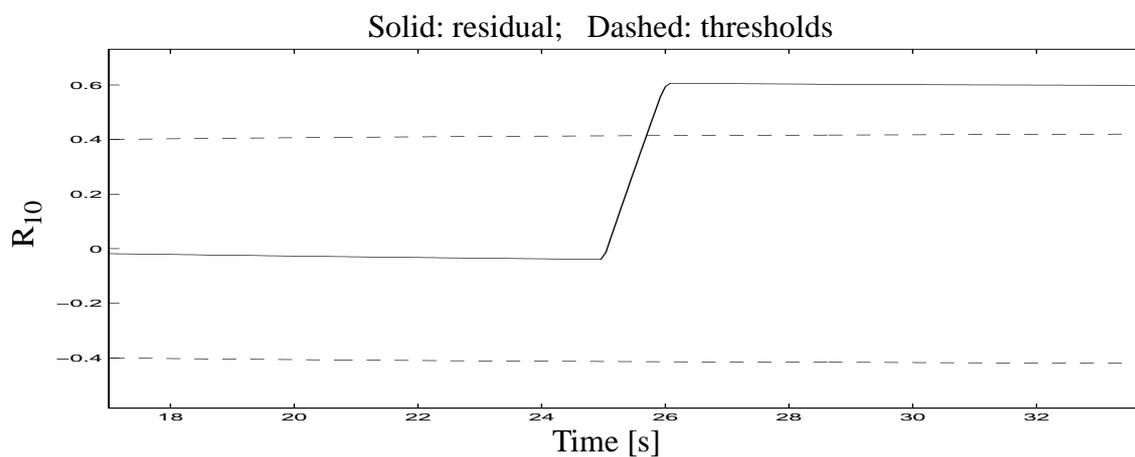
Figure 4.13: R_{10} with temperature sensor fault

Due to the introduction of R_{10} all important moving parts as well as all sensors present in the ECS distribution subsystem can now be supervised.

4.4 Decision structure

Table 2 shows all hypothesis tests presented in Section 4.2 and Section 4.3 put together in a decision structure. The structure indicates which residuals each fault mode might affect.

	NF	F_{V14}	F_{V15}	F_{V16}	F_{V33}	F_{Vo}	$F_{\Theta14}$	$F_{\Theta15}$	$F_{\Theta16}$	F_{PR13}	F_{T78}	F_{T77}	F_{T38}	F_{T21}	F_{T19}	F_{T13}	F_{Pamb}	F_{P12}	F_{P17}	F_{P30}	F_{P32}	F_{Lcp}	F_{Lav}	F_{Lcab}	F_{Phot}
R_1	0	0	0	0	X	0	0	X	0	0	0	0	0	0	0	0	X	0	X	X	0	0	X	0	0
R_2	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	X	X	0	X	X	0	0	0
R_3	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R_4	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R_5	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R_6	0	0	0	0	0	0	0	0	0	0	0	X	0	0	X	0	0	0	0	0	0	0	0	0	0
R_7	0	0	0	0	0	0	0	0	0	0	0	0	0	X	X	0	0	0	0	0	0	0	0	0	0
R_8	0	0	0	0	0	0	0	0	0	0	0	X	0	X	0	0	0	0	0	0	0	0	0	0	0
R_9	0	0	0	0	0	X	0	0	0	X	0	0	X	X	0	X	X	X	X	0	X	X	0	X	0
R_{10}	0	0	0	0	0	0	X	0	0	0	X	0	X	X	0	0	0	0	X	0	X	0	0	0	X

Table 2: Decision structure

In Section 2.5 the principles of a decision structure and how it is used was thoroughly explained, but a very brief repetition will be held here. The main thing to remember is that an X means the fault mode might affect the residual, while a 0 means it cannot. If R_2 suddenly is above its threshold, one of the five fault modes marked with X on the "R_2-line" must have caused it. If both R_1 and R_2 are above their thresholds, fault mode $\mathbf{F_{P17}}$ must have caused it.

Above the thick line between R_9 and R_{10} only sensors available today are used, while R_{10} also uses the new pressure sensor, P_{hot}.

If one studies Table 2 it is realized that only 7 out of the 24 considered fault modes can be isolated. This is however not as bad as one might first think. In the decision structure all fault modes belonging to a moving part ($\mathbf{F_{V14}}$ - $\mathbf{F_{PR13}}$) are placed to the left of the thick line between $\mathbf{F_{PR13}}$ and $\mathbf{F_{T78}}$, while sensor and leakage fault modes are to the right of the thick line. If an alarm, say R_2, is fired, a list of potential present fault modes is presented. In this case the fault modes are $\mathbf{F_{\Theta16}}$, $\mathbf{F_{P12}}$, $\mathbf{F_{P17}}$, $\mathbf{F_{P32}}$, and $\mathbf{F_{Lcp}}$, and only one of these ($\mathbf{F_{\Theta16}}$)

belongs to a moving part. Thus $\mathbf{F_{\Theta 16}}$ is the most likely fault to be present, and a service technician can start by checking this component. If the decision structure is studied one realises that almost all residuals contain only one moving part, except for R_1 and R_9, that contains two. This means that even though a whole list of possible faults often is presented to a service technician, he can still point out the one, or two, faults far most likely to have fired the alarm. This probably simplifies the investigation undertaken when an alarm is fired.

4.5 Evaluation of the diagnosis system

How well does the diagnosis system work then? It is not obvious what is meant by a well working diagnosis system, but one way of measuring the performance is to investigate how small faults it can detect. This has been carried out, and the result is presented below.

Simulations with different fault sizes in various operating points have been performed, but all possible flight cases have definitely not been investigated. Also it must be pointed out once more that this work has been carried out on a model, and not on a real ECS. Therefore the fault sizes presented below is not valid in a real ECS, but they are to be considered as hints of what fault sizes can be detected when diagnosing the Easy5-model.

The fault sizes presented below are according to a worst case scenario. In some operating points smaller faults can be detected too, but if a fault is about the size presented here it will almost för certain fire an alarm, independent of operating point.

The fault modes in Table 3 are those affecting R_1, i.e. those belonging to M_1^c in hypothesis test H_1^0 from Section 4.2.1.

$\mathbf{F_{V33}}$	$\mathbf{F_{\Theta 15}}$	$\mathbf{F_{P17}}$	$\mathbf{F_{P30}}$	$\mathbf{F_{Pamb}}$	$\mathbf{F_{Lav}}$
-	15°	10%	15%	-	-

Table 3: Fault sizes needed in R_1

It is hard to measure how much a jamming valve is jamming, so that is why no fault size is displayed under $\mathbf{F_{V33}}$, but if closing (or opening) the shut off valve 33HA takes twice the usual time the fault is probably detected.

A fault of 15° in the valve position sensor might seem a quite large fault to allow, but this is probably thanks to the big thresholds applied to R_1. As mentioned in Section 4.2.1 the merging of orifices that has to be done in R_1 introduces large model errors.

Ambient pressure sensor fault has not been simulated due to difficulties when introducing the fault. In the Easy5-model ambient pressure is defined as a global variable, since the sensor itself is not situated in the ECS. This makes it hard to change only measured ambient pressure without changing what the model believes to be the true physical ambient pressure.

The size of F_{Lav} (leak in the avionics section) that can be detected varies a lot depending on the operating point of the system. In some cases holes less than 1 cm^2 can be detected, while they cannot be detected at all no matter how big the hole is in other cases. The reason for this can be found in how merging of orifices works. (Figure 3.8 shows which orifices are involved.) Merging of orifices in series is similar to merging of parallel resistors, i.e. the resulting orifice area is less than the least of the two orifices merged, see Section 3.2.3. This means that when valve 15HA has a small opening area compared to the avionics and radar orifices, a leak hardly affects the flow at all.

$F_{\Theta 16}$	F_{P12}	F_{P17}	F_{P32}	F_{Lcp}
1°	10%	5%	5%	-

Table 4: Fault sizes needed in R_2

What was said in the previous paragraph about orifices in series also goes for F_{Lcp}, but here yet another issue is relevant. In the case of leakage in the avionics section, leaking air as well as the air flowing the intended way both ends up in the ambient, i.e. they both flow to ambient pressure. This is not the case with leakage in the cabin distribution pipe. Here leaking air flows to the ambient air, while the air flowing the intended way flows to the cabin, and the pressure is not the same in these two places. If cooling pack outlet pressure is about the same size as cabin pressure, the airflow entering the cabin is quite low. If the pipe breaks when these pressures are approximately equal a lot of air leaks, since cabin pressure is higher than ambient pressure, and leakage is then easy to detect. Under these propitious conditions holes smaller than 1 cm^2 can be detected, but under poor conditions leakage cannot be detected at all.

Residuals R_3, R_4, and R_5 only reacts to jamming valves, and as mentioned before it is hard to estimate how much they jam. However, if the jamming slows the valve down to 50% of normal speed the fault is detected.

The temperature residuals R_6, R_7, and R_8 will detect any deviation in temperature, since all three temperatures compared are represented with the same measurement signal in Easy5.

F_{PR13}	F_{Vo}	F_{T13}	F_{T21}	F_{T38}	F_{P12}	F_{P17}	F_{P32}	F_{Pamb}	F_{Lcp}	F_{Lcab}
-	-	40%	40%	40%	10%	15%	70%	-	-	100%

Table 5: Fault sizes needed in R_9

No values of detectable sizes are given for F_{PR13}, F_{Vo}, F_{Pamb} and F_{Lcp} for the reasons explained above.

In Table 5 it says that a cabin leak must be 100% if it is to be detected, and that refers to the area of the outlet valves. Thus a leak must be about the same size as the opening of the valves

if it is to be detected. The valve opening is 20 cm^2 at the most, but most of the time the valves are only about half opened.

$F_{\Theta 14}$	F_{T78}	F_{T21}	F_{T38}	F_{P17}	F_{P32}	F_{Phot}
1.5°	5%	5%	5%	20%	20%	15%

Table 6: Fault sizes needed in R_{10}

All fault sizes presented in the tables above are according to the level of model uncertainties present in the simulink model developed. If the model built was a copy of the Easy5-model, faults of infinitesimal size would be detected, so the fault sizes necessary for detection are actually a measurement of the model uncertainties present.

Chapter 5

Discussion

The purpose of this thesis was to investigate which faults in the distribution part of the ECS can be detected with the sensors available today, using model based diagnosis, and to clarify where new ones could be useful in order to design an improved diagnosis system. To do this a model of the ECS distribution section was built, and by means of it a diagnosis system was constructed. When this was done it was also clarified which faults could be detected using the sensors available today. The remaining faults important to detect were sorted out, and the model was expanded with new sensors in order to enable detection of those faults. The conclusions drawn are presented below.

5.1 Conclusion

All faults important to detect, except for one (see Table 2), can be detected with the sensors available in the system today. If a new pressure sensor is installed upstream valve 14HA, the last important fault can be detected as well. Thus almost all error prone components can be supervised using only available sensors, but it is to be noted that this goes for the distribution subsystem of the ECS only. The rest of the ECS contains very few sensors, and if diagnosis is to be performed there as well several new sensors are probably needed. For instance the pressure sensor suggested to be introduced in this thesis would most likely be useful.

With the new pressure sensor all faults considered in this thesis can be detected, even though some of them must be quite large in various operating points before the impact on the residual is enough to fire an alarm.

If the Gripen had been equipped with the extended diagnosis system presented here during the years it has been operative, 95% of the faults occurred in the ECS distribution section would have been detected. This corresponds to about 40% of all faults having occurred in the entire

ECS. This is of course a theoretical result, but it shows the potential of the technique. More information about which faults that have occurred in the ECS can be found in [11].

Only 7 of the 24 fault modes considered can be isolated (i.e. exclusively pointed out) with the diagnosis system developed, see Table 2. However, if only those faults that actually have occurred are considered (i.e. those to the left of the first thick line in Table 2), 5 out of 9 can be isolated. (The two fault modes $\mathbf{F_{V33}}$ and $\mathbf{F_{\Theta 15}}$ cannot be separated from each other. Neither can $\mathbf{F_{PR13}}$ and $\mathbf{F_{V0}}$.) Therefore the performance of the diagnosis system is not as bad as one might first think, when only 7 out of 24 fault modes can be isolated. A service technician investigating a generated alarm is given a whole list of possible faults, but he can still say which (or which two) is far the most likely to have caused the alarm.

When designing a diagnosis system it is important to model as many faults as possible (even those not very likely to occur) that might have an effect on the residuals. Because, if an alarm is fired, and all possible fault modes on the resulting list are checked without finding anything, people will start losing faith in the system. Also if a diagnosis system like this one is implemented and works very well, service technicians might start losing their fault localization skills. Then it can be hard finding the fault responsible for an alarm, if it is not one of those suggested by the diagnosis system.

5.2 Future work

If a diagnosis system like this one is to be implemented in the Gripen, a lot of work remains, and most of the work behind this thesis must be redone. Since this work has been carried out on a model, none of the parameters presented, such as thresholds or detectable fault sizes, are relevant in a real system. What can be used is the principles of the model, i.e. for instance what physical quantities can be estimated using the control and measurement signals provided in the ECS.

How well the model corresponds to measurement data from a real ECS has not been properly investigated. It has been tested on a very small amount of data, and that did not turn out very well, but no conclusions can be drawn from this test only. In [7] model based diagnosis has been carried out on a subsystem of the ECS distribution section, and the flow models used there corresponds very well to measurement data from an ECS rig. The flow models used in [7] are of the type (3.3), so the flow models used in this thesis, (3.1), might have to be replaced by (3.3). This would be a good thing, since (3.3) are easier to simulate than (3.1). Merging of orifices also works better when (3.3) is applied to measurement data compared to when (3.1) is applied to Easy5 data. Thus the greatest model error in the diagnosis system developed here might be reduced if the models are changed when implemented.

There are also components in the ECS that are not included in the Easy5-model, such as the defroster and cabin safety valve. These must be included, but that is probably quite easily done. The introduction of these components will affect the cabin pressure observer. The safety valve can probably be supervised, since it has an effect on R_9. The defroster flow is mechanically controlled by the pilot and completely unknown, but it is relatively small and is not very likely to significantly disturb the cabin pressure estimation. However, if it does, there are at least two ways to solve the problem. The first alternative is to simply measure the defroster flow, and the second one is to sense when the defroster is engaged and then shut off the diagnosis system.

Another potential improvement is the fault models. The longer the aircraft is operative, the more information about how faults occur is gathered, and perhaps this information can be used to obtain more restrictive fault models than the general one used here, i.e. (4.1).

If the model was revised and validated against the ECS rig, it would be very interesting to install the model only, without its thresholds, in one of the test aircrafts and log the residuals. Then it would be sorted out how well the model works under realistic conditions, because even the rig is a bit idealistic. If this turned out well, the data collected could be used to set thresholds, and later on the system could be implemented in production aircraft.

References

[1]   Nyberg M, Frisk E, *Diagnosis and supervision of technical processes*, Linköpings tekniska högskola (course literature)

[2]   Blom G, *Sannolikhetsteori och statistikteori med tillämpningar,* Studentlitteratur 1989

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

[4]   *Saab military aircraft's lärarutbildning 1994 - JAS39 Luftsystem Materialgrupp 36,* 1994-04-20 (Saab internal document)

[5]   *SRS for the GECU in JAS39,* 00-08-31 (Saab internal document)

[6]   Nilsson J, Master thesis: *Diagnosis on a principal environmental control system,* Linköpings tekniska högskola, LiTH-ISY-EX-3067

[7]   Svensson B, Master thesis: *Diagnosis on the JAS39 Gripen environmental control system,* Linköpings tekniska högskola, LiTH-ISY-EX-3148

[8]   *ECS technology course presented to Saab Scania AB,* Hymatic, January 1995 (Saab internal document)

[9]   Easy5-model, file: js39b_ebs_ecs_4a (Saab internal document)

[10]   Nordling C, Österman J, *Physics handbook, for science and engineering,* Studentlitteratur 1995, fifth edition

[11]   Åkerlund O, *Underlag för att bestämma de mest angelägna felen att detektera och isolera,* Reg no F-2000-0231 (Saab internal document)