Annex 7.1.A
The Air Control Case Study

Simin Nadjm-Tehrani
Dept. of Computer & Information Science, Linköping University,
S-581 83 Linköping, Sweden, e-mail: simin@ida.liu.se

1 Introduction

This report presents the current work on the air control case study provided by SAAB Aircraft AB in the first of the SYRF project. The case study was presented to the project partners in terms of a 4 page textual specification and an implemented code for a controller in the ASA development environment. The purpose of the case study is to serve identifying relevant problems in modelling, implementing, testing and verification of synchronous programs embedded in physical environments, and to serve as a test case for the approaches proposed in the project.

The textual specification document provided a mixture of operational description, global requirements, and implementation oriented descriptions of a control system. In the current report we restructure the original information, separating the requirements specifications from the design specifications, induce some new requirements, and add additional models and assumptions about the physical environment of the control. Another work package in the project will report on the reengineering of the implementation suggested by SAAB and shows how the controller can be modelled by a mixture of synchronous languages: Argos for hierarchical breakdown, Esterel for conditional activation of parallel modules and Lustre for continuous control blocks.

The report is organized as follows: section 2 describes the architecture of the system and the interface between software and hardware. Section 3 covers global requirements specifications, and section 4 presents the functional specification of the system — the first design specification. Section 5 decomposes the requirements with respect to the suggested design. Section 6 provides a first attempt at modelling the physical environment and makes explicit certain assumptions, leading to a set of differential and algebraic equations.

2 System architecture

The case study consists of a climatic chamber with a control system which regulates and monitors the flow and the temperature of air which is circulating in the chamber.

Figure 1 presents the component model and physical interfaces between the software controller and the chamber hardware.

The chamber is to be ventilated through the inlet and outlet and has a given volume. It has two sensors for measuring the internal air temperature and the mass flow rate. The external interface consists primarily of an on/off button, two analog knobs for setting the values for required temperature and flow, as well as warning signals in terms of a light and a sound. It also includes lights for signifying some of its internal modes of operation (wait, work, or block). This may appear to be outside the realms of a component and interface specification (mixing the design related mode names) but has been kept for compatibility with the original specification.

Unfortunately, the original architectural specification says nothing about the actuators. In the functional part of the document one can see that the heater and fan can be turned on and off. It is also implicit that their output effect can be adjusted in an analog manner, but there is no other information about the nature of control signals or the range of values. Section 6 attempts to fill this gap by making certain assumptions.

3 Requirements specification

The overall requirement of the system is to keep the chamber's temperature and flow within given values, and to warn the operators if this goal is not achievevable due to encountering problems.

On the face of it, these are safety and liveness properties. The system will not allow variable values to go outside a given bound (nothing bad happens), and the system warns if its operating assumptions are not met (something good happens).

One may even consider the "if and only if" version to the the second property: the system warns only if it is justified (false alarms are not desirable).

In section 5 we will revisit the requirements and make them more specific, but before that, we consider the suggested design.

4 Functional specification

The functional specification assumes a particular design. Here we restate the elements of design as listed in the original document (except for different groupings and minor adjustments), and for the sake of consistency, use

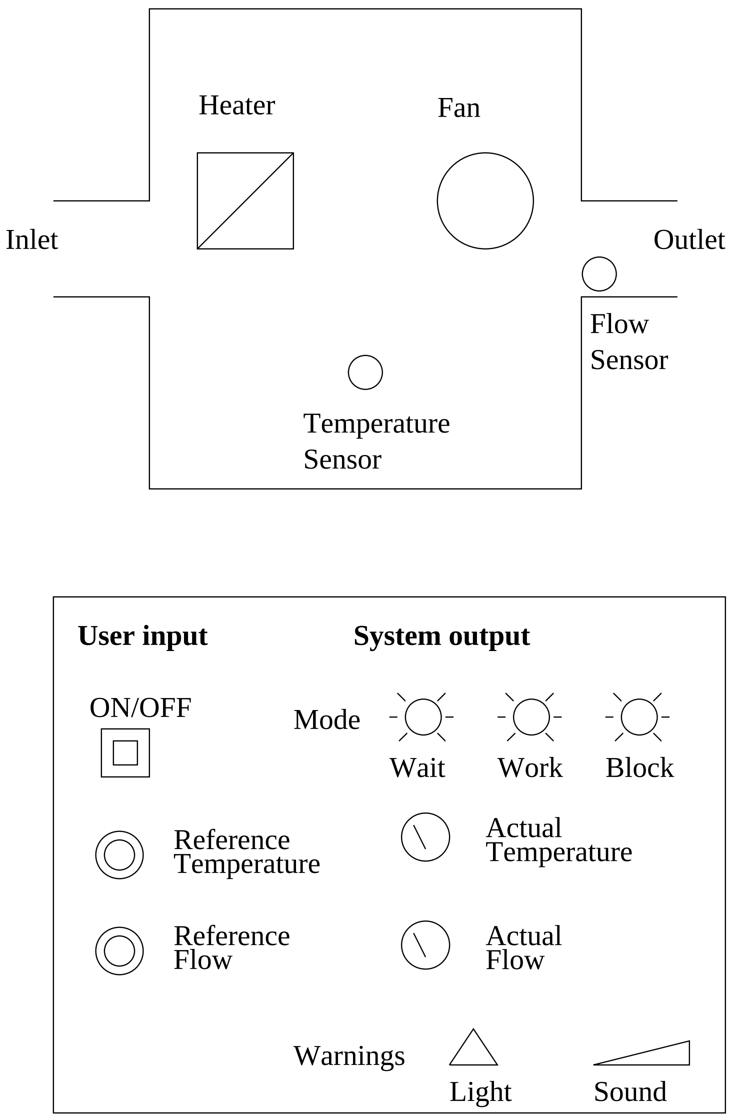

Figure 1: The hardware components of the aircontrol system and its external interface

the same variable names. These elements of design can be summarized as follows.

temperature control

- At start up, a requested temperature *optreq* is selected and the heater is turned on. It is possible to choose *optreq* in the interval $[treqmin, treqmax]$, where $treqmin$ is greater than the (lowest) outside air temperature *envtemp*. Any other chosen values outside the above interval are automatically adjusted up (down) to the lower (upper) limit respectively.

- Let $T_{min} = optreq - 2\Delta_{temp}$ and $T_{max} = optreq + 2\Delta_{temp}$. Then the system is considered to be in the **wait** mode while the actual temperature (*chamtact*) is not within those limits.

- The system will be in the **sol** mode (read solution mode) from the time the temperature hits the reagion $T_{min} \leq chamtact \leq T_{max}$ until it leaves the mode. The system makes a transition to the **work** mode when $\mid chamtact - optreq \mid \leq \Delta_{temp}$ is fullfilled. The time taken for the system to enter and leave the **sol** mode is expected to be a given fixed time called *solution_time*.

ventilation control

- The ventilation or the mass flow rate is measured by the time it takes to exchange one volume of air.

- At start up, a requested flow time *optvent* is selected and the fan is turned on. This chosen time for the rate of air change should be in the interval $[tventmin, tventmax]$. Other chosen values are automatically adjusted upwards (downwards) to these limits respectively.

- Ventilation is regulated so that the air in the chamber is changed at least once every *optvent*.

- The observed rate of change *flowtime* is based on a measure of the air flow *chamflow* delivered by the sensor.

monitoring

- The continuously measured values of *chamtact* and *chamflow* are to be displayed on the control panel.

- Three lamps indicate being in the system modes **wait, work** and **block** respectively.

- A warning by light and sound shall be activated whenever $\mid chamtact - optreq \mid > \Delta_{temp}$ after being in the **sol** mode for a duration of *solution_time*.

- The warning light is activated if $flowtime > Xoptvent$ for some fixed ratio X.

- When in **work** mode, if $\mid chamtact - optreq \mid > 2\Delta_{temp}$, or the derivative of the temperature, based on *chamtact* exceeds a maximum value $tgrad$, then the mode shall change to the **block** mode.

- When in **block** mode, the heater is immediately turned off, the warning light and the light indicating the **block** mode are activated , and the fan is active for another *tblock* seconds before it is turned off. It shall not be possible to influence the system by changing *optreq* or *optvent*. The system must be turned off before restart.

- If *optreq* is changed such that $optreq > chamtact + \Delta_{temp}$ the system makes a transition to the **wait** mode, and the heater is turned on (if not on?).

- If *optreq* is changed such that $optreq < chamtact - \Delta_{temp}$, the system is changed to **wait** mode, the heater is turned off and the fan will continue to work (turned on if not on?).

5 More detailed requirements

In this section we refine the overall requirements as stated in section 3 by reference to the above functional design. Satisfying he following requirements can thus be the goal of system verification, i.e. the verification of the closed loop system.

- The controller shall arrive at the **sol** mode within a given time bound (say t_1 seconds).

- In the **sol** mode, while the reference values remain constant, the temperature and flow shall converge towards the chosen reference values, and *chamact* shall remain within $2\Delta_{temp}$ from *optreq*. Warning by sound and light is not issued unless *chamact* is outside $[optreq - \Delta_{temp}, optreq + \Delta_{temp}]$ efter *solution_time* has elapsed since entering the mode.

- In the **work** mode, while the reference values remain constant, the temperature shall remain within the given bounds. That is, *chambact* remains in the interval $[optreq - \Delta_{temp}, optreq + \Delta_{temp}]$, and $flowtime > Xoptvent$.

- The mode **block** is entered if and only if the derivative of *chamact* exceeds *tgrad*, or if *chamact* falls outside $[optreq - \Delta_{temp}, optreq + \Delta_{temp}]$ while *optreq* remains constant.

5.1 Comments and classifications

The property associated with the **sol** mode ensures that false alarms are not issued provided that a reasonable value for *solution_time* has been determined. That is, if *solution_time* is chosen appropriately with respect to the heater characteristics and the assumption on variation of the external air temperature, then the warning is not issued unnecessarily.

The last property implies that the system will never enter the **block** mode unless the outside temperature and flow change beyond reasonable bounds. That is, the contoller transits to the **block** mode if and only if a shut down is justified, due to exceeding *tgrad*, or if the reference values are not maintainable when the external input lies outside a reasonable range.

The first property is obviously a bounded liveness property. The properties connected with the **sol** and **work** modes are, however, typical convergence (stability) properties easier proved within the framework of control theory. Reaching the block mode is not desirable, making that a safety property under normal operating conditions, but also essential if things go wrong (making it a conditional liveness property).

It should be clear that a formal verification of all of these properties requires a mathematical model of the physical environment.

6 Physical environment

In this section we state some assumptions and partially model the physical environment.

6.1 Heat-flow inter-relationships

Heat and flow mutually affect each other in non-trivial ways [1]. In a first coarse model of the climatic chamber we include the effects of flow on the heating process but ignore the effects in the opposite direction. The motivation being that the primary concern of the ventilation system is keeping the temperature within given bounds (this may be induced from the global requirements and the nature of warnings).

Next, we make a simplification concerning how flow affects heat. We decide not to consider the air flow effects with respect to the heat transfer factor of the heater (i.e. how velocity of the moving air will affect heating of the air). We only consider the cooling effect as a result of the air exchange caused by the fan with respect to heat generation.

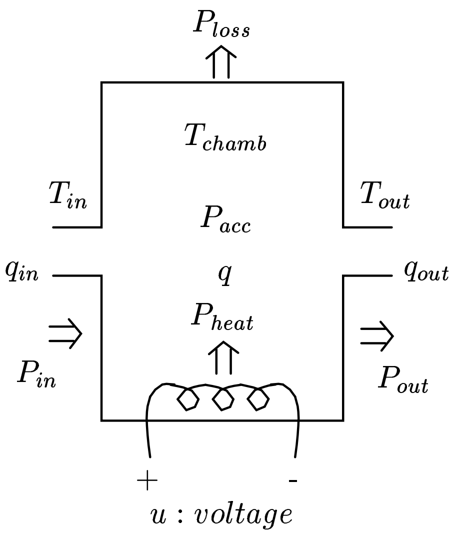

Figure 2: The variables appearing in the heat model of the chamber.

6.2 Assumptions on flow

The flow of mass and volume are related by air density, i.e. $q\,\rho = \dot{m}$, where q $[m^3/s]$ denotes volume flow, ρ $[kg/m^3]$ is a density factor (normally a function f of temperature T), and $\dot{m}$ $[kg/s]$ is the mass flow. Since the design document mostly discusses "the time it takes for exchange of air", it is not clear whether one can measure volume flow or mass flow. No more information about the sensor is available.

The first assumption that we make is that the air pressure in the chamber remains constant relative to the external air pressure. This implies mass balance: that input and output mass flows are equal, $\dot{m}_{in} = \dot{m}_{out}$, which further leads to a similar assumption on volume flow. The latter can, however, be assumed provided that density as a function of temperature can be approximated to a constant factor. That is, assuming $f(T) = k_\rho$, we can further assume that $q_{in} = q_{out}$. Note that the fan can change the value of the chamber flow q, but the assumptions above constrain the in and out flows to stay in a constant relation: more specifically $q = q_{in} = q_{out}$.

We make no further assumptions on the input to the flow actuator (the fan), the range of the angular velocity, whether the fan is driven by voltage, etc. We simply assume that a given (reference) flow can be obtained within a bounded time with an appropriate regulator. This places the emphasis on the physical model of the heating process.

6.3 Model of the heating process

The heater produces heat which is accumulated in the chamber to an extent which depends on the flow. Figure 2 presents the variables appearing in the heat process model.

Based on the earlier assumptions the heat model will have three inputs: the air flow (q), the control signal to the heater (u), and the outside air temperature (T_{in}). The main state variable is the chamber temperature (T_{chamb}) which can be measured by the temperature sensor and delivered to the heat controller. However, to see how the final model is arrived at we start by stating the energy conservation principle:

$$P_{in} + P_{heat} - P_{out} - P_{loss} = P_{acc} \tag{1}$$

where the sum of heat power is stated to be constant, i.e. the incoming power (P_{in}), that resulting from the heater activation (P_{heat}), the outgoing power (P_{out}), and the power lost through the walls of the chamber (P_{loss}) are assumed to give the accumulated heat power in the chamber (P_{acc}).

We now state the relation between each element and the input/output variables, and some model coefficients (all the k-terms):

$$\begin{aligned}
P_{in} &= q_{in}\, T_{in}\, k_{in} \\
P_{heat} &= u^2\, k_{heat} \\
P_{out} &= q_{out}\, T_{out}\, k_{out} \\
P_{loss} &= T_{chamb}\, k_{loss} \\
P_{acc} &= \dot{T}_{chamb}\, k_{chamb}
\end{aligned}$$

Making a further assumption that $T_{chamb} = T_{out}$, using the earlier assumption $q = q_{in} = q_{out}$, and using equation 1, we can now simplify the set of formulas to the following equation defining the chamber temperature:

$$\begin{aligned}
&\dot{T}_{chamb} = 1/k_{chamb} \\
&\quad (\quad q\, T_{in}\, k_{in} + \\
&\qquad u^2\, k_{heat} - \\
&\qquad T_{chamb}(q\, k_{out} - k_{loss})
\end{aligned}$$

It is interesting to see that despite several simplifying assumptions the model is highly non-linear. So, formally proving the properties of the hybrid model consisting of the synchronous controller and this chamber model is a challenge for hybrid system verification.

7 Future works

The work on this case study will continue by studying the requirements for completeness in cooperation with domain experts. Further, integrated proof methods which combine the proof techniques from respective areas (computer science and control theory) need to be determined. This requires determining how to decompose the requirements specifications to a granularity whereby the systematic combination of proof techniques is possible. Some interesting properties of the system when controlled by the synchronous controller are then subjected to formal proofs.

References

[1] H. Alvarez. *Energiteknik, Del I.* Studentlitteratur, Lund, Sweden, 1990.