EECS4312 Isolette Assignment

Juan Loja (lojag95@cse.yorku.ca)
Sadman Sakib Hasan (cse23152@cse.yorku.ca)

November 5, 2017

Prism account used for submission: cse23152@cse.yorku.ca

Requirements Document:
Temperature control for an Isolette

Revisions

Date	Revision	Description
22 October 2017	1.0	Initial requirements document

Contents

List of Figures

List of Tables

1. System Overview

The System Under Development (SUD) is a computer controller for the thermostat of an Isolette.[1] An Isolette is an incubator for for an infant that provides controlled temperature, humidity and oxygen (Fig. 1). Isolettes are used extensively in Neonatal Intensive Care Units for the care of premature infants.

This requirements document is specifically for the control of temperature. The purpose of the Isolette computer controller is to maintain the air temperature of an Isolette within a desired range. It senses the current temperature of the Isolette and turns the heat source on and off to warm the air as needed. If the temperature falls too far below or rises too far above the desired temperature range, it activates an alarm to alert the nurse. The system allows the nurse to set the desired temperature range and to set the alarm temperature range outside the desired temperature range of which the alarm should be activated. This requirements documents follows the specification in [**?**] (Appendix A) except where noted.

Figure 1: Isolette

Many babies have dies due to faulty incubators. There is thus a standard that manufacturers must satisfy. Modern incubators are equipped with alarms for air temperature, skin temperature, oxygen concentration and humidity. The alarms are both visual such

[1]The image in Fig 1 is from: `www.nufer-medical.ch`.

as red warning lamps, and audio such as beep signals. Once measured measured values exceed permitted limits as well as when faults occur in sensors. For one such incident leading to death see "Medical Devices: Use and Safety" shown in Fig. 2.

CASE 6:2 Baby dies through overheating in incubator

An underdeveloped baby was being treated in an incubator with skin temperature control. When the baby was being washed, the skin sensor was removed and left hanging outside the incubator after the washing. Thus the sensor started measuring the room temperature (approx. 25°C). The control circuits therefore increased the heat to maximum level, and the temperature in the incubator rose to more than 45°C. The baby died.

For increased safety, incubators must be constructed with an extra control circuit that prevents overheating in case the skin sensor is misplaced. The incubator in question was indeed equipped with such a safety circuit, but the circuit was defective.

Figure 2: Incubator Safety Problems [**?**, p98]

2. Goals

The high-level goals (G) of the system are:

- G1—The Infant should be kept at a safe and comfortable temperature.
- G2—The Nurse should be warned if the Infant becomes too hot or too cold.
- G3—The cost of manufacturing the computer controller for the thermostat should be as low as possible.

3. Context Diagram

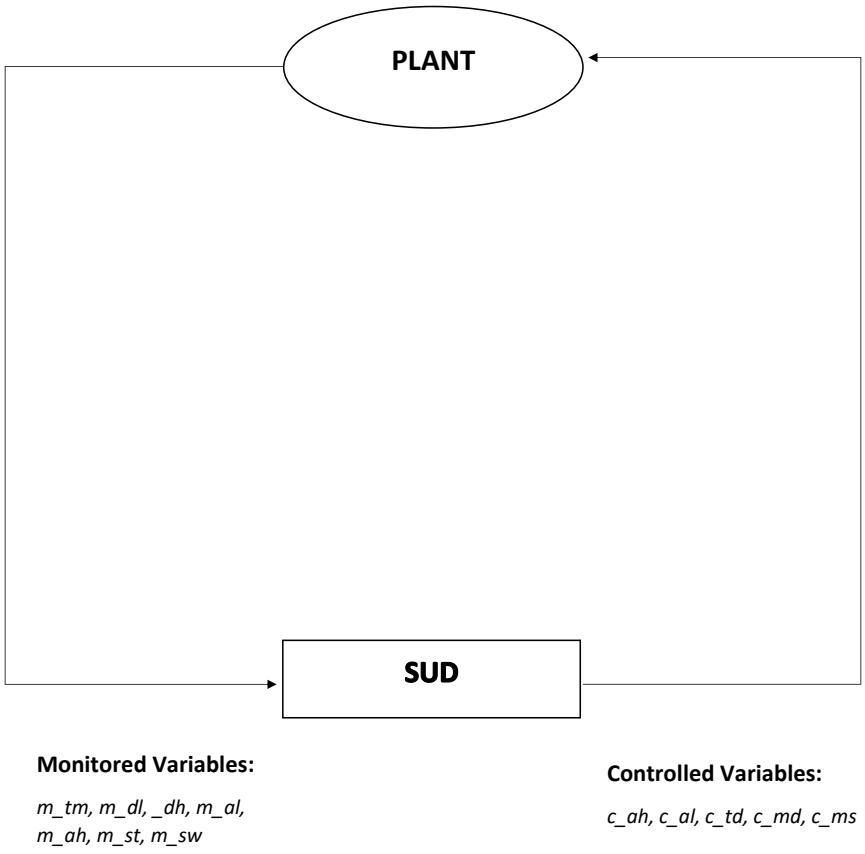

Figure 3: Context diagram for the SUD

4. Monitored Variables

The monitored variables are a subset of those described in [**?**].[2] There is a single status variable *m_st* that is *invalid* whenever any one of the operator inputs or temperature sensor are in a failed state. Otherwise types and ranges are as in [**?**].

Name	Type	Range	Units	Physical Interpretation
m_tm	$\mathbb{R}$	68 .. 105	°F	actual temperature of Isolette air temperature from sensor
m_dl	$\mathbb{Z}$	97 .. 99	°F	desired lower temperature set by operator
m_dh	$\mathbb{Z}$	98 .. 100	°F	desired higher temperature set by operator
m_al	$\mathbb{Z}$	93 .. 98	°F	lower alarm temperature set by operator
m_ah	$\mathbb{Z}$	99 .. 103	°F	higher alarm temperature set by operator
m_st	Enumerated	{valid, invalid}		status of sensor and operator settings
m_sw	Enumerated	{on, off}		switch set by operator

Table 1: Monitored Variables

[2] With some change of nomenclature. Monitored variables have an "m" prefix.

5. Controlled Variables

The controlled variables are a subset of those described in [**?**].[3] In addition, there is a mode display *c_md* and a message display *c_ms*.[4]

Name	Type	Range	Units	Physical Interpretation
c_hc	Enumerated	{on, off}		heat control: command to turn heat source on or off
c_td	$\mathbb{Z}$	$\{0\} \cup \{68 \,..\, 105\}$	°F	displayed temperature of Isolette (zero when Isolette is off)
c_al	Enumerated	{off, on}		sound alarm to call nurse
c_md	Enumerated	{off, init, normal, failed}		mode of Isolette operation (failed if $m\_st = invalid$)
c_ms	Enumerated	{ok, too_hot_alarm, too_cool_alarm, warming_up, cooling_down, system_error}		messages to display to nurse

Table 2: Controlled Variables

[3] With some change of nomenclature. Controlled variables have a "c" prefix.

[4] The mode "off" is added to that of Fig. A-4 in [**?**], and the mode transitions have been changed.

6. Mode Diagram

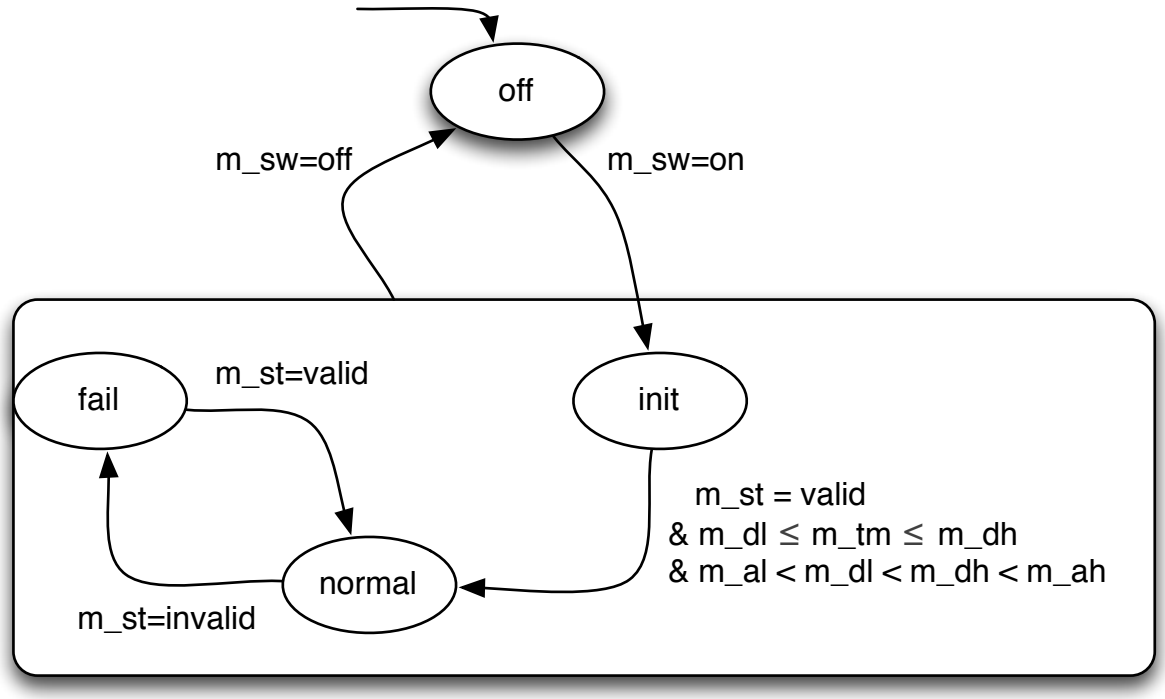

Figure 4: Mode diagram for the states

Rationale: A mode diagram denotes the possible states the system can be in. They are *abstract* variables whose output are visible to the client, in this case the nurse. In a particular state, the *guard* condition has to be satisfied in order for the mode to change.

7. R-Descriptions

The following are the R-descriptions for the System Under Description.

REQ1	The *controller* shall operate in one of four modes: *off*, *init*, *normal* and *fail*.	See statechart in Fig. 4.

Rationale: The Isolette can show four statuses to the Nurse.

- *off* mode indicates that the Isolette is switched off. If the Isolette gets switched on, move to the *init* state.
- *init* mode indicates that the Isolette has just been switched on and the temperature sensor is still not in the desired range. If the input from the nurse is valid and the temperatures are in their desired ranges then move to the *normal* state.
- *normal* mode indicates everything is under control (i.e all inputs are correct and the sensors are working fine). If something goes wrong, then move on to the *fail* state.
- *fail* mode indicates something went wrong and sound an alarm. The nurse can either then turn the Isolette off to go to the *off* state or fix the input temperature ranges to go back to the *normal* state.

REQ2	In the *normal* mode, the temperature controller shall maintain current temperature inside the Isolette within a set temperature range (the *desired* range).	The *desired* temperature range is *m_dl* .. *m_dh*. If the current temperature *m_tm* is outside this range, the controller shall turn the heater on or off via the controlled variable *m_hc* to maintain the desired state.

Rationale: The *desired temperature range* will be set by the nurse to the desired range based on the infant's weight and health. The controller shall maintain the current temperature within this range under normal operation.

The following relevant hazard was identified through the safety assessment process:

- **H1**: Prolonged exposure of Infant to unsafe heat or cold;
- *Classification*: catastrophic;
- *Probability*: $< 10^{-9}$ per hour of operation.

To ensure that probability of hazard H1 is 10^{-9} per hour of operation, the following derived safety requirement shall apply to the Isolette controller:

REQ3	In *normal* mode, the controller shall activate an alarm whenever • the current temperature falls outside the *alarm* temperature range (either through temperature fluctuation or a change in the alarm range by an operator), or • a failure is signalled in any of the input devices (temperature sensor and operator settings).	The alarm temperature range is $m\_al\,..\,m\_ah$. Monitored variable m_st in Table 1 shows "invalid" when any of the input signals fail.

Rationale: The alarm needs to go off to alert the nurse during critical situations. Most importantly, in the *normal* mode since that is when the child is first put into the Isolette. It must be ensured that the Isolette is capable of handling the child and in any case when it cannot, an alarm must go off to notify the nurse.

REQ4	Once the alarm is activated, it becomes deactivated in one of two ways: • The nurse turns off the Isolette; • The alarm has lasted for 10 seconds, and after 10 seconds or more the alarm conditions are removed.	The Isolette can be switched off by setting m_sw to off. The alarm condition can be removed when the alarm c_hc has been activated for more than 10 seconds. Refer to Table 2 and 8.

Rationale: The Alarm Temperature Range will be set by the Nurse based on the Infants weight and health. Once the alarm is activated (i.e the temperature falls beyond the range), the Infant should be removed from the Isolette and the Isolette should be turned off. If the nurse fails to accomplish that within 10 seconds, the alarm gets deactivated with the infant inside.

REQ5	If mode is *normal* and the value of the Current Temperature is greater than or equal to the Lower Alarm Ttemperature +0.5 and less than or equal to the Upper Alarm Temperature -0.5, the alarm shall be set to *off*.	When the current temperature is between +/-0.5 of the alarm temperature range, $m\_al + 0.5 <= m\_tm <= m\_ah - 0.5$ then c_al should be set to off. Refer to Table 2 and 8.

Rationale: The alarm should be turned off at the same moment that the Displayed Temperature shows a value greater than the Lower Alarm Temperature and less than the Upper Alarm Temperature.

REQ6	The Thermostat shall set the value of the Heat Control depending on the Current Temperature.	The heat control of the Isolette is the control variable *c_hc*. Refer to Table 2 and 5.

Rationale: The controlled variable *c_hc* is used by the thermostat to turn the Heat Control on and off to maintain the Current Temperature in the Isolette within the Desired Temperature Range, i.e within *m_dl* and *m_dh*. If the Current Temperature is below the Desired Low Temperature, the heat control should be set on. If the Current Temperature is above the Desired High Temperature, the heat control should be set off.

REQ7	In the *init* and *normal* modes, the displayed temperature shall be set to the value of the current temperature rounded to the nearest integer.	The displayed temperature of the Isolette is the control variable *c_td*. Refer to Table 2 and 6.

Rationale: The controlled variable *c_td* is used by the thermostat to show the Current Temperature of the Isolette. The Displayed Temperature is calculated using the mathematical floor function of the Current Temperature to avoid showing invalid temperatures to the nurse.

8. E-descriptions

The following are the environmental assumption made on the Isolette System:

ENV1	The current temperature received from the sensor is a a real number in the range 68.0 to 105.0°F.	The monitored variable *m_tm* in Table 1 specifies the range, type and unit for the Current Temperature received from the sensor.

Rationale: This is the specified range of operation of the Isolette. The lower end of this range is useful for monitoring an Isolette that is warming to the Desired Temperature Range. The upper end is set to be greater than the Higher Alarm Temperature.

ENV2	The desired and alarm temperatures received from the operator are all in increments of 1°F.	The monitored variables *m_tm*, *m_dl*, *m_dh*, *m_al* and *m_ah* set in an increment of 1°F. Refer to Table 1 to see details about the monitored inputs.

Rationale: Marketing studies have shown that customers prefer to set temperatures in 1 degree increments. A resolution 1F is sufficient to be consistent with the functionality and performance for the Isolette.

ENV3	The Lower Alarm Temperature will always be >= 93°F.	The monitored variables *m_al* denotes the Lower Alarm Temperature. Table 1 specifies the range, type and unit for the Lower Alarm Temperature set by the Nurse.

Rationale: Exposure to temperatures less than 93°F will result in hypothermia, which can lead to death within a few minutes for severely ill pre-term infants.

ENV4	The Higher Alarm Temperature will always be <= 103°F.	The monitored variables *m_ah* denotes the Higher Alarm Temperature. Table 1 specifies the range, type and unit for the Higher Alarm Temperature set by the Nurse.

Rationale: Exposure to temperatures greater than 103°F will result in hyperthermia, which can lead to cardiac arrhythmias and febrile seizures within a few minutes.

ENV5	The Lower Desired Temperature will always be >= 97°F.	The monitored variables *m_dh* denotes the Lower Desired Temperature. Table 1 specifies the range, type and unit for the Lower Desired Temperature set by the Nurse.

Rationale: Exposing the Infant to temperatures lower than 97°F may result in excessive heat loss and drop in heart rate secondary to metabolic acidosis.

9. Abstract variables needed for the Function Table

No abstract variables were used for the function tables.

10. Function Tables

Below are the function tables for each of the controlled variables:

10.1. Function Table for Mode Control: c_md

<table>
<tr><th colspan="4"></th><th>$c\_md(i)$</th></tr>
<tr><td colspan="4">$i = 0$</td><td rowspan="2">off</td></tr>
<tr><td rowspan="8">$i > 0$</td><td colspan="3">$m\_sw(i) = off$</td></tr>
<tr><td rowspan="7">$\neg(m\_sw(i) = off)$</td><td colspan="2">$c\_md(i-1) = off$</td><td>$init$</td></tr>
<tr><td rowspan="2">$c\_md(i-1) = init$</td><td>S_1</td><td>$normal$</td></tr>
<tr><td>$\neg S_1$</td><td>$c\_md(i-1)$</td></tr>
<tr><td rowspan="2">$c\_md(i-1) = normal$</td><td>$m\_st(i) = invalid$</td><td>$fail$</td></tr>
<tr><td>$m\_st(i) = valid$</td><td rowspan="2">$c\_md(i-1)$</td></tr>
<tr><td rowspan="2">$c\_md(i-1) = fail$</td><td>$m\_st(i) = invalid$</td></tr>
<tr><td>$m\_st(i) = valid$</td><td>$normal$</td></tr>
</table>

Table 3: Function Table for Mode Control

S_1	$m\_st(i) = valid \wedge$ $m\_dl(i) \leq m\_tm(i) \leq m\_dh(i) \wedge$ $m\_al(i) < m\_dl(i) < m\_dh(i) < m\_ah(i)$	This is the condition to be met for system to go from *init* to *normal*

Table 4: Definition of S_1

10.2. Function Table for Heat Control: c_hc

<table>
<tr><td colspan="4"></td><td>$c\_hc(i)$</td></tr>
<tr><td colspan="4">$i = 0$</td><td rowspan="2">off</td></tr>
<tr><td rowspan="4">$i > 0$</td><td colspan="3">$m\_sw(i) = off$</td></tr>
<tr><td rowspan="3">$\neg(m\_sw(i) = off)$</td><td colspan="2">$\neg(m\_dl(i) < m\_dh(i))$</td><td>$c\_hc(i-1)$</td></tr>
<tr><td rowspan="3">$m\_dl(i) < m\_dh(i)$</td><td>$m\_tm(i) < m\_dl(i)$</td><td>on</td></tr>
<tr><td>$m\_dl(i) <= m\_tm(i) \wedge m\_tm(i) <= m\_dh(i)$</td><td>$c\_hc(i-1)$</td></tr>
<tr><td></td><td>$m\_tm(i) > m\_dh(i)$</td><td>off</td></tr>
</table>

Table 5: Function Table for Heat Control

10.3. Function Table for Tempearature Display Control: c_td

		$c\_td(i)$
$i = 0$		0
$i > 0$	$c\_md(i-1) = off \vee c\_md(i-1) = fail$	
	$c\_md(i-1) = init \vee c\_md(i-1) = normal$	$floor(m\_tm(i) + 0.5)$

Table 6: Function Table for Temperature Display Control

10.4. Function Table for Message Display Control: c_ms

	$c\_ms(i)$
$m\_st(i) = invalid$	$system\_error$
$m\_tm(i) > m\_ah(i)$	too_hot_alarm
$m\_tm(i) < m\_al(i)$	too_cool_alarm
$m\_al(i) < m\_tm(i) < m\_dl(i)$	$warming\_up$
$m\_dh(i) < m\_tm(i) < m\_ah(i)$	$cooling\_down$
$ELSE$	ok

Table 7: Function Table for Message Display Control

10.5. Function Table for Alarm Control: c_al

<table>
<tr><td colspan="6"></td><td>$c\_al(i)$</td></tr>
<tr><td colspan="6">$i = 0$</td><td rowspan="2">off</td></tr>
<tr><td rowspan="8">$i > 0$</td><td colspan="5">S_2</td></tr>
<tr><td rowspan="7">$\neg S_2$</td><td colspan="4">S_3</td><td>$c\_al(i-1)$</td></tr>
<tr><td rowspan="6">$\neg S_3$</td><td colspan="3">S_4</td><td>on</td></tr>
<tr><td rowspan="5">$\neg S_4$</td><td colspan="2">$c\_al(i-1) = off$</td><td>$c\_al(i-1)$</td></tr>
<tr><td rowspan="4">$c\_al(i-1) = on$</td><td colspan="2">S_5</td><td rowspan="2">off</td></tr>
<tr><td rowspan="3">$\neg S_5$</td><td>$m\_sw(i) = off$</td></tr>
<tr><td>$m\_sw(i) = on$</td><td>on</td></tr>
</table>

Table 8: Function Table for Alarm Control

S_2	$c\_md(i-1) = off \vee c\_md(i-1) = init$	Mode is off or $init$. Else it is in $normal$ or $fail$ mode.
S_3	$(m\_al(i) <= m\_tm(i) \wedge m\_tm(i) < m\_al(i) + 0.5) \vee$ $(m\_ah(i) - 0.5 <= m\_tm(i) \wedge m\_tm(i) <= m\_ah(i))$	This is the Hysteresis Region.
S_4	$m\_tm(i) > m\_ah(i) \vee m\_tm(i) < m\_al(i) \vee$ $m\_st(i) = invalid$	Conditions for when the alarm is on.
S_5	$held\_for(alarm, 10)(i-1)$	Checks if alarm was on for at least 10 seconds.

Table 9: Definitions for S_2, S_3, S_4 and S_5

11. Validation

To be Done. Proof of completeness and disjointness and validation of the requirements using PVS.

Include the PVS sources in the appendix to this document but summarize the proofs here.

12. Use Cases

See Section A2 of [**?**] for some use cases. The use cases need to be adapted to the revised descriptions of the previous sections of this document. Provide one Use Case (a) informally and (b) formally in PVS.

13. Acceptance Tests

In this section, the use cases have to be converted into precise acceptance tests (using the function table to describe pre/post conditions) to be run when the design and implementation are complete. Describe one acceptance test

14. Traceability

Matrix to show which acceptance tests passed, and which R-descriptions they checked. No need to do this for this assignment.

15. Glossary

The definition of important terms is placed in this section. You are not required to complete this.

A. Appendix Title??

Appendix goes here. PVS sample below. Format so that there is no line wrapping

```
alert: THEORY
BEGIN
  delta: posreal = 0.5 % TR = 0.5 seconds
  IMPORTING Time[delta]

  p:     [DTIME -> real]  % Pressure
  alarm: [DTIME -> bool]

  hi: real
END
```