

# EECS4312 Isolette Assignment

Juan Loja (lojag95@cse.yorku.ca)

Sadman Sakib Hasan (cse23152@cse.yorku.ca)

November 4, 2017

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

©This document is not for public distribution. This document may only be used by EECS4312 students registered at York University. By downloading this document from the department, registered York students agree to keep this document (and all documents associated with assignments, projects or laboratories) private for their personal use, and may not communicate it to anyone else.

Students must obey York regulations on academic honesty requiring that students do the work of the Lab on their own, and not cheat by sharing with others or using and/or submitting the work of others. If you use *github* or similar repository for your work, the repository must be private. Placing your work in the public domain infringes on academic integrity. Github offers unlimited private repositories to students: <https://education.github.com/pack>.

# Requirements Document:

## Temperature control for an Isolette

### Revisions

Date	Revision	Description
22 October 2017	1.0	Initial requirements document

## Contents

<b>1. System Overview</b>	<b>5</b>
<b>2. Goals</b>	<b>6</b>
<b>3. Context Diagram</b>	<b>7</b>
<b>4. Monitored Variables</b>	<b>8</b>
<b>5. Controlled Variables</b>	<b>9</b>
<b>6. Mode Diagram</b>	<b>10</b>
<b>7. R-Descriptions</b>	<b>11</b>
<b>8. E-descriptions</b>	<b>14</b>
<b>9. Abstract variables needed for the Function Table</b>	<b>15</b>
<b>10. Function Tables</b>	<b>15</b>
10.1. Function Table for heat control: <i>c_hc</i> . . . . .	16
<b>11. Validation</b>	<b>17</b>
<b>12. Use Cases</b>	<b>18</b>
<b>13. Acceptance Tests</b>	<b>19</b>
<b>14. Traceability</b>	<b>20</b>
<b>15. Glossary</b>	<b>20</b>
<b>A. Appendix Title??</b>	<b>21</b>

## List of Figures

1. Isolette . . . . .	5
2. Incubator Safety Problems [?, p98] . . . . .	6
3. Context diagram for the SUD . . . . .	7
4. Mode diagram for the states . . . . .	10

## List of Tables

1.	Monitored Variables . . . . .	8
2.	Controlled Variables . . . . .	9

## 1. System Overview

The System Under Development (SUD) is a computer controller for the thermostat of an Isolette.<sup>1</sup> 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 died 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

---

<sup>1</sup>The image in Fig 1 is from: [www.nufer-medical.ch](http://www.nufer-medical.ch).

as red warning lamps, and audio such as beep signals. Once 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

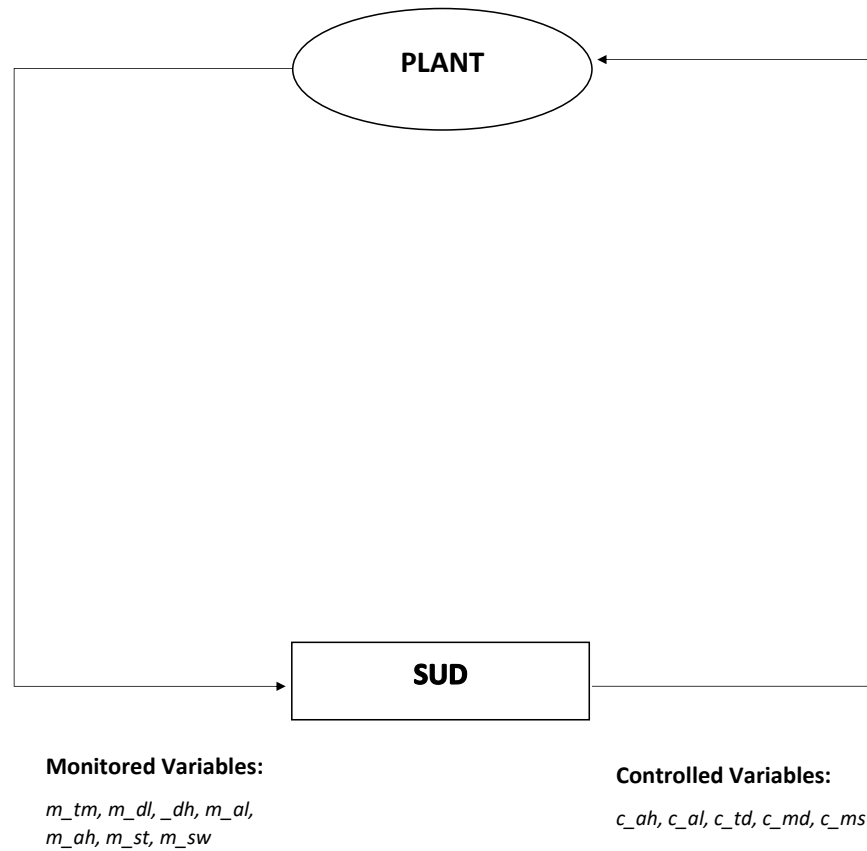


Figure 3: Context diagram for the SUD

## 4. Monitored Variables

The monitored variables are a subset of those described in [?].<sup>2</sup> 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

---

<sup>2</sup>With some change of nomenclature. Monitored variables have an “m” prefix.



## 5. Controlled Variables

The controlled variables are a subset of those described in [?].<sup>3</sup> In addition, there is a mode display  $c\_md$  and a message display  $c\_ms$ .<sup>4</sup>

Name	Type	Range	Units	Physical Interpretation
$c\_hc$	Enumerated	{on, off}		heat control: command to turn heat source on or off
$c\_td$	$\mathbb{Z}$	$\{0\} \cup \{68 \dots 105\}$	$^{\circ}\text{F}$	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 $m\_st = \text{invalid}$ )
$c\_ms$	Enumerated	{ok, too_hot_alarm, too_cool_alarm, warming_up, cooling_down, system_error}		messages to display to nurse

Table 2: Controlled Variables

<sup>3</sup>With some change of nomenclature. Controlled variables have a “c” prefix.

<sup>4</sup>The mode “off” is added to that of Fig. A-4 in [?], and the mode transitions have been changed.

## 6. Mode Diagram

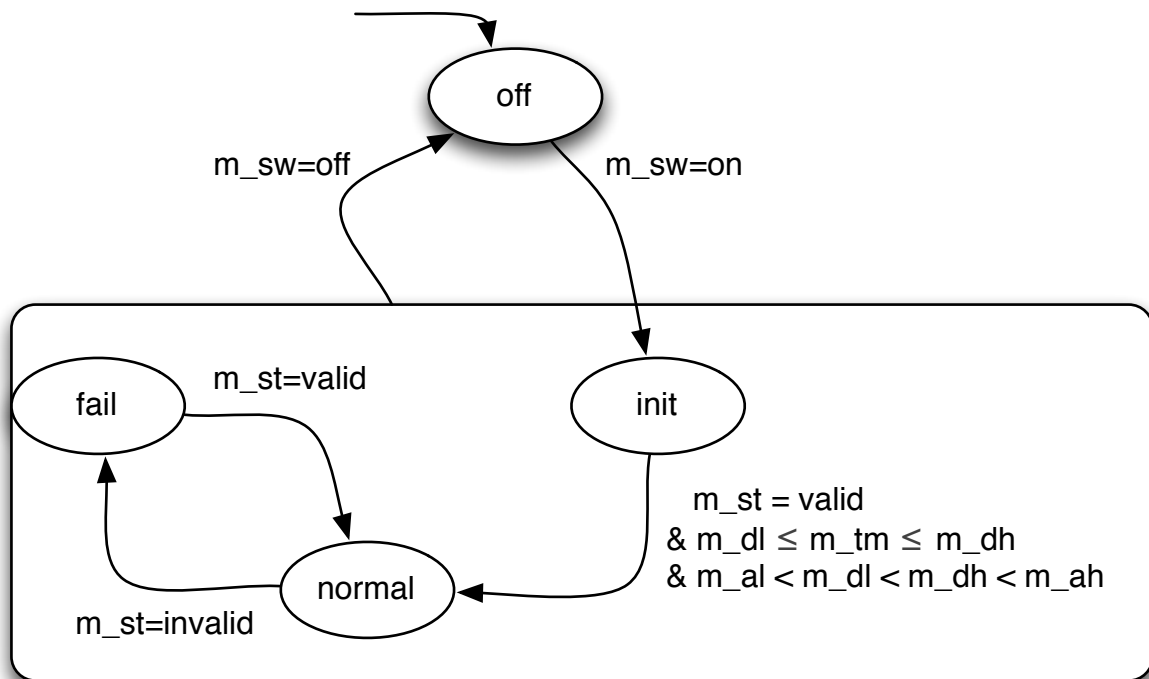


Figure 4: Mode diagram for the states

**Rationale:** NEED RATIONALE HERE

## 7. R-Descriptions

We have already elicited the following R-descriptions.

REQ1	The <i>controller</i> shall operate in one of four modes: <i>off</i> , <i>init</i> , <i>normal</i> and <i>fail</i> .	See statechart in Fig. ??.
------	--	----------------------------

REQ2	In the <i>normal</i> mode, the temperature controller shall maintain current temperature inside the Isolette within a set temperature range (the <i>desired</i> range).	The <i>desired</i> temperature range is $m\_dl \dots m\_dh$ . 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	<p>In <i>normal</i> mode, the controller shall activate an alarm whenever</p> <ul style="list-style-type: none"> <li>the current temperature falls outside the <i>alarm</i> temperature range (either through temperature fluctuation or a change in the alarm range by an operator), or</li> <li>a failure is signalled in any of the input devices (temperature sensor and operator settings).</li> </ul>	<p>The alarm temperature range is <i>m_al..m_ah</i>. Monitored variable <i>m_st</i> shows “invalid” when any of the input signals fail.</p>
------	---	---

REQ4	<p>Once the alarm is activated, it becomes deactivated in one of two ways:</p> <ul style="list-style-type: none"> <li>The nurse turns off the Isolette;</li> <li>The alarm has lasted for 10 seconds, and after 10 seconds or more the alarm conditions are removed.</li> </ul>	<p>Refer to the relevant tables of monitored and/or controlled variables and function tables.</p>
------	---	---

On the next page, you must add the next three most important R-Descriptions. Provide a brief rationale for each R-Description. Include any remaining R-Descriptions in an appendix to this document.

Additional three R-Descriptions with brief rational (one page)

## 8. E-descriptions

ENV1	The current temperature received from the sensor is a a real number in the range 68.0 to 105.0°F.	??
------	---	----

ENV5	The desired and alarm temperatures received from the operator are all in increments of 1°F.	Refer to the relevant tables of monitored and/or controlled variables and function tables.
------	---	--

Provide the next 3 most important E-descriptions on this page. The the rest in the appendix.

## 9. Abstract variables needed for the Function Table

No abstract variables were used for the function tables.

## 10. Function Tables

Starting on the next page, provide one function table for each control variable (in Table 2). Each control variable should have its own sub-section heading and its own page.

## 10.1. Function Table for heat control: c\_hc

Function table goes here on this page. Other function tables each on their own page



## 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
```