Isolette Requirements

(SAnToS Lab Version)

Adapted from DOT/FAA/AR-08/32
(DRAFT – PLEASE DO NOT DISTRIBUTE)

October 11, 2024

Contents

Chapter 1

System Overview

The system being specified is the Thermostat of an Isolette.[1] An Isolette is an incubator for an Infant that provides controlled temperature, humidity, and oxygen (if necessary). Isolettes are used extensively in Neonatal Intensive Care Units for the care of premature infants.

The purpose of the Isolette Thermostat 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.

1.1 System Content

The operational context of the Isolette Thermostat is shown in Figure 1.1.

The Thermostat interacts directly with three entities that are part of the Isolette:

- The Temperature Sensor provides the Current Temperature of the air in the Isolette to the Thermostat.
- The Heat Source heats the Air in the Isolette. It is turned on and off by the Heat Control.
- The Operator Interface provides the Operator Settings for the Thermostat and receives Operator Feedback from the Thermostat.

The Thermostat also interacts indirectly with other entities outside of the Isolette:

- The Nurse who uses the Operator Interface to enter the Operator Settings and view the Operator Feedback.
- The Air in the Isolette.
- The Infant that is placed in the Isolette and is warmed by the Air.

[1] To simplify this example, the Operator Interface is treated as an external entity outside of the Thermostat.

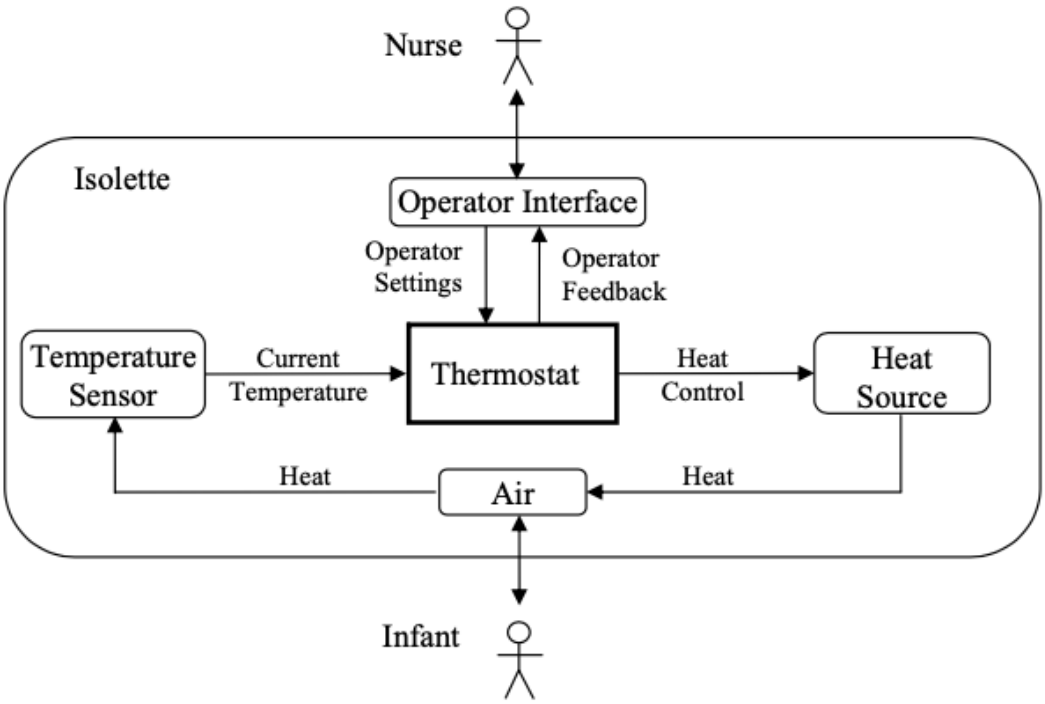

Figure 1.1: Context Diagram for the Isolette Thermostat

1.2 System 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 Thermostat should be as low as possible.

Chapter 2

Operational Concepts

The following use and exception cases describe how the operators interact with the Isolette and the Thermostat. A summary of the use and exception cases is provided in Table 2.1. The actors and their primary goals are shown in Table 2.2.

2.1 Use Case: Normal Operation of Isolette

This use case describes the normal operation of the Isolette by the Nurse.

- Related System Goals: G1 and G2
- Primary Actor: Nurse
- Precondition:
  - Infant is ready to be placed in the Isolette
  - Isolette and Thermostat are turned off
- Postcondition:
  - Infant is removed from the Isolette
  - Isolette and Thermostat are turned off
- Main Success Scenario
  1. Nurse turns on the Isolette
  2. Isolette turns on the Thermostat
  3. Thermostat initializes and enters its normal mode of operation (exception case 1) (UC 2.5, Section 5.1.2, and Section 5.2.2)
  4. Nurse configures the Isolette for the needs of the Infant (2.2)
  5. Nurse waits until the Current Temperature is within the Desired Temperature Range (2.6 and 5.1.1)

ID	Primary Actor	Title and Description
2.1	Nurse	*Normal Operation of Isolette:* Describes the normal operation of the Isolette by the Nurse
2.2	Nurse	*Configure the Isolette:* Describes how the Nurse configures the Isolette and Thermostat for the Infant
2.3	Thermostat	*Maintain Desired Temperature:* Describes how the Thermostat turns the Heat Source on and off to maintain the Current Temperature in the Isolette within the Desired Temperature Range
2.4	Thermostat	*Failure to Maintain Safe Temperature:* Describes how the Thermostat and the Nurse respond when the Isolette is unable to maintain the Current Temperature within the Alarm Temperature Range
2.5	Thermostat	*Respond to Thermostat Failure:* Describes how the Thermostat and the Nurse respond when the Thermostat detects an internal failure
2.6	Nurse	*Failure to Maintain Desired Temperature:* Describes how the Nurse deals with an Isolette that cannot keep the Current Temperature within the Desired Temperature Range but can keep the Current Temperature within the Alarm Temperature Range

Table 2.1: Summary of Isolette Thermostat Use and Exception Cases

Actor	Primary Goals of the Actor
Nurse	Provide the Infant with proper nursing care, including keeping the Infant warm
Infant	Be comfortable and healthy
Isolette	Hold the Infant and maintain the Current Temperature within the Desired Temperature Range
Thermostat	Maintain Current Temperature in the Isolette within the Desired Temperature Range

Table 2.2: Isolette Thermostat Primary Actors and Goals

6. Nurse places the Infant in the Isolette
7. Isolette maintains Desired Temperature (2.3)
8. Nurse confirms that the Current Temperature is in the Desired Temperature Range during rounds (2.6 and 5.1.1)
9. Nurse removes Infant
10. Nurse turns off the Isolette
11. Isolette turns off the Thermostat

- Exception Case 1:

  1. Alarm is activated because Current Temperature is outside the Alarm Temperature Range (5.2.3)
  2. Nurse ignores the Alarm[1]
  3. Continue with Main Success Scenario, step 4.

2.2 Use Case: Configure The Isolette

This use case describes how the Nurse configures the Isolette and Thermostat for the Infant.

- Related System Goals: G1 and G2
- Primary Actor: Nurse
- Precondition: The Isolette and Thermostat are turned on
- Postcondition:
  - The Desired Temperature Range is set for the needs of the Infant
  - The Alarm Temperature Range is set for the needs of the Infant
  - The Current Temperature in the Isolette is in the Desired Temperature Range
- Main Success Scenario:

  1. Nurse sets the Alarm Temperature Range for the Infant (5.2.1)
  2. Nurse sets the Desired Temperature Range for the Infant (5.1.1)
  3. Thermostat maintains Desired Temperature Range (2.3)

[1] In the interest of simplicity, the functionality to turn the Alarm off is not specified. As an exercise, the reader might want to consider what changes would be necessary to add this capability to the example.

2.3 Use Case: Maintain Desired Temperature

This use case describes how the Thermostat turns the Heat Source on and off to maintain the Current Temperature in the Isolette within the Desired Temperature Range.

- Related System Goals: G1
- Primary Actor: Thermostat
- Precondition: Isolette and Thermostat are turned on
- Postcondition:
  - Isolette and Thermostat are turned on
  - Current Temperature is in the Desired Temperature Range
- Main Success Scenario:
  1. Current Temperature falls below the Desired Temperature Range
  2. Thermostat turns the Heat Source on to warm up the Isolette (5.1.3)
  3. Current Temperature rises above the Desired Temperature Range
  4. Thermostat turns the Heat Source off to cool the Isolette (5.1.3)
  5. Repeat steps 1 through 4

2.4 Exception Case: Failure To Maintain Safe Temperature

This exception case describes how the Thermostat and Nurse respond when the Isolette is unable to maintain Current Temperature within the Alarm Temperature Range.

- Related System Goals: G2
- Primary Actor: Thermostat
- Precondition:
  - The Isolette and Thermostat are turned on
  - The Current Temperature is within the Alarm Temperature Range
  - The Alarm is off
- Postcondition:
  - The Isolette and Thermostat are turned on
  - The Current Temperature is within the Desired Temperature Range
  - The Alarm is off
- Main Success Scenario:
  1. Current Temperature falls below or rises above the Alarm Temperature Range

2. Thermostat activates the Alarm (5.2.3)
3. Nurse responds to the Alarm and sees that the Display Temperature is in the Alarm Temperature Range (5.1.1)
4. Nurse removes Infant from the Isolette
5. Nurse corrects the problem, e.g., closing an open door (alternate course 1)
6. Nurse waits until the Display Temperature is within the Desired Temperature Range (2.6 and 5.1.1)
7. Nurse places Infant back in the Isolette

- Alternate Course 1:

1. Nurse is unable to correct the problem
2. Nurse obtains another Isolette
3. Nurse starts normal operation of the new Isolette (2.1)

2.5 Exception Case: Respond To Thermostat Failure

This exception case describes how the Thermostat and the Nurse respond when the Thermostat detects an internal failure.

- Related System Goals: G2
- Primary Actor: Thermostat
- Precondition:
  - The Isolette and Thermostat are turned on
  - The Thermostat status is on
  - The Alarm is off
- Postcondition:
  - The Isolette and Thermostat are turned on
  - The Current Temperature is in the Desired Temperature Range
  - The Alarm is off
- Main Success Scenario:

1. Thermostat detects an internal failure (5.1.4 and 5.2.4)
2. Thermostat enters the FAILED mode (5.1.2 and 5.2.2)
3. Thermostat sets its Displayed Status to failed (5.1.1 and 5.2.1)
4. Thermostat activates the Alarm
5. Nurse responds to the Alarm and sees that the Thermostat is failed
6. Nurse removes Infant from the Isolette
7. Nurse obtains another Isolette
8. Nurse starts normal operation of the new Isolette (2.1)

2.6 Exception Case: Failure To Maintain Desired Temperature

This exception case describes how the Nurse handles an Isolette that cannot keep the Current Temperature within the Desired Temperature Range, but can keep the Current Temperature within the Alarm Temperature Range.

- Related System Goals: G1
- Primary Actor: Nurse
- Precondition:
  - The Isolette and Thermostat are turned on
  - The Current Temperature is not within the Desired Temperature Range
  - The Current Temperature is within the Alarm Temperature Range
- Postcondition:
  - The Isolette and Thermostat are turned on
  - The Current Temperature is in the Desired Temperature Range
- Main Success Scenario:
  1. Nurse attempts to correct the problem, e.g., closing an open door
  2. Nurse waits until the Current Temperature of the Isolette is within the Desired Temperature Range (alternate course 1) (5.1.1)
  3. Return to calling scenario
- Alternate Course 1:
  1. Display Temperature fails to enter the Desired Temperature Range (5.1.1)
  2. Nurse removes Infant from the Isolette
  3. Nurse obtains another Isolette
  4. Nurse starts normal operation of the new Isolette (2.1)
  5. Return to calling scenario

Chapter 3

External Entities

The following sections describe the external entities with which the Thermostat directly interacts: the Temperature Sensor, the Operator Interface, and the Heat Source. The monitored and controlled variables associated with each entity are listed, along with any environmental assumptions made about the entity. An Isolette external entity is also defined to specify environmental assumptions that span more than one external entity.

3.1 Isolette

An Isolette is an incubator for an Infant that provides controlled temperature, humidity, and oxygen (if necessary). It encompasses the Thermostat, the Temperature Sensor, the Operator Interface, and the Heat Source. The following environmental assumptions are made by the Thermostat about the Isolette

- EA-IS-1: When the Heat Source is turned on and the Isolette is properly shut, the Current Temperature will increase at a rate of no more than 1°F per minute.

  Rationale: If the Current Temperature can increase at a rate of more than 1°F per minute, the Thermostat may not be able to turn the Heat Source off quickly enough to maintain the Desired Temperature Range unless the allowed latency specified for the Heat Control is reduced.

- EA-IS-2: When the Heat Source is turned off and the Isolette is properly shut, the Current Temperature will decrease at a rate of no more than 1°F per minute.

  Rationale: If the Current Temperature can decrease at a rate of more than 1°F per minute, the Thermostat may not be able to turn the Heat Source on quickly enough to maintain the Desired Temperature Range unless the allowed latency specified for the Heat Control is reduced.

3.2 Temperature Sensor

The Temperature Sensor provides the Current Temperature of the Air in the Isolette to the Thermostat. The monitored variables are shown in table 3.1.

Name	Type	Range	Units	Physical Interpretation
Current Temperature	Real	[68.0..105.0]	°F	Current air temperature inside Isolette
	Current	•Invalid, Valid		

Table 3.1: Thermostat Monitored Variables for Temperature Sensor

Name	Type	Range	Units	Physical Interpretation
Heat Control	Enumerated	Off, On		Command to turn Heat Source on and off

Table 3.2: Thermostat Controlled Variables for Heat Source

- Table 3.1 denotes initial value

The following environmental assumptions are made:

- EA-TS-1: The Current Temperature will be provided to the Thermostat in degrees Fahrenheit

  Rationale: Consistency with environmental-assumption Operator Interface EA-OI-1

- EA-TS-2: The Current Temperature will be sensed to an accuracy of ±0.1°F.

  Rationale: An accuracy of 0.1°F is necessary to ensure the Thermostat can turn the Heat Source on and off quickly enough to maintain the Desired Temperature Range.

- EA-TS-3: The Current Temperature will cover the range of at least 68.0° to 105.0°F.

  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 greater than the Upper Alarm Temperature to ensure that the Current Temperature will be sensed across the entire Alarm Temperature Range.

3.3 Heat Source

The Heat Source heats the Air in the Isolette. It is turned on and off by changing the value of the Heat Control controlled variable. The controlled variables are shown in table 3.2. No environmental assumptions are made.

3.4 Operator Interface

The Operator Interface provides the Operator Settings for the Thermostat and receives Operator Feedback from the Thermostat. The environmental assumptions associated with the Operator Interface are quite strong, which simplifies the manage Operator Interface Function. If these assumptions were not satisfied by the Operator Interface external entity, the Manage Operator Interface Function would need to be strengthened to ensure consistent inputs to the Thermostat. The monitored and controlled variables are shown in tables 3.3 and 3.4, respectively.

- Table 3.3 denotes initial value

The following environmental assumptions are made:

Name	Type	Range	Units	Physical Interpretation
Operator Settings				Thermostat settings provided by operator
Desired Temperature Range				Desired range of Isolette temperature
Lower Desired Temperature	Integer	[97..99]	°F	Lower value of Desired Temperature Range
	Status	•Invalid, Valid		
Upper Desired Temperature	Integer	[98..100]	°F	Upper value of Desired Temperature Range
	Status	•Invalid, Valid		
Alarm Temperature Range				Active Alarm when outside of this range
Lower Alarm Temperature	Integer	[93..98]	°F	Lower value of Alarm Temperature Range
	Status	•Invalid, Valid		
Upper Alarm Temperature	Integer	[98..100]	°F	Upper value of Alarm Temperature Range
	Status	•Invalid, Valid		

Table 3.3: Thermostat Monitored Variables for Operator Interface

Name	Type	Range	Units	Physical Interpretation
Operator Feedback				Information provided back to the operator
Regulator Status	Enumerated	Init, On, Failed		Status of the Thermostat Regulator Function
Monitor Status	Enumerated	Init, On, Failed		Status of the Thermostat Monitor Function
Display Temperature	Integer	[68..105]	°F	Displayed temperature of Isolette
Alarm	Enumerated	Off, On		Command to turn Alarm on or off

Table 3.4: Thermostat Controlled Variables for Operator Interface

- EA-OI-1: All temperatures will be entered and displayed in degrees Fahrenheit.

  Rationale: Minimize the complexity of this example. An actual system would probably support Celsius or perhaps both Fahrenheit and Celsius

- EA4-OI-2: All temperatures will be set and displayed by the operators in increments of 1°F.

  Rationale: Marketing studies have shown that customers prefer to set temperatures in 1 degree increments. A resolution 1°F is sufficient to be consistent with the functional and performance requirements specified in the rest of the document.

- EA-OI-3: The Lower Alarm Temperature will always be ≥93°F.

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

- EA-OI-4: The Lower Alarm Temperature will always be less than or equal to the Lower Desired Temperature of -1°F.

  Rationale: If the Lower Alarm Temperature is greater than or equal to the Lower Desired Temperature, the Alarm could be activated while the Current Temperature is still in the Desired Temperature Range.

- EA-OI-5: The Lower Desired Temperature will always be ≥97°F. 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.

- EA-OI-6: The Lower Desired Temperature will always be less than or equal to the Upper Desired Temperature of -1°F.

  Rationale: If the Lower Desired Temperature is greater than or equal to the Upper Desired Temperature, it is unclear if the Heat Source should be on or off. This may result in excessive cycling of the Heat Source.

- EA-OI-7: The Upper Desired Temperature will always be $\leq$100°F. Rationale: Exposing the Infant to temperatures greater than 100°F may result in an incorrect diagnosis of fever resulting in aggressive evaluation (blood culture and lumbar puncture) and treatment for infection.

- EA-OI-8: The Upper Alarm Temperature will always be greater than or equal to the Upper Desired Temperature of 1°F.

  Rationale: If the Upper Alarm Temperature is less than or equal to the Upper Desired Temperature, the Alarm could be activated while the Current Temperature is still in the Desired Temperature Range.

- EA-OI-9: The Upper Alarm Temperature will always be $\leq$103°F.

  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.

- EA-OI-9: The Display Temperature will cover the range of at least 68.0° to 105.0°F.

  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 maximum Upper Alarm Temperature.

Chapter 4

Safety Requirements

The following relevant hazards were 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 requirements are levied on the Isolette Thermostat:

- SR-1: The Isolette shall include an independent regulator function that maintains the Current Temperature inside the Isolette within the Desired Temperature Range.

  Rationale: The Desired Temperature Range will be set by the Nurse to the ideal range based on the Infant's weight and health. The regulator should maintain the Current Temperature within this range under normal operation.

  Allowed probability of failure: $< 10^{-5}$ per hour

- SR-2: The Isolette shall include an independent monitor function that activates an Alarm within a maximum of 5 seconds whenever

  - the Current Temperature falls below or rises above the Alarm Temperature Range.
  - the Current Temperature or the Alarm Temperature Range is flagged as invalid.
  - an internal failure has been detected in the monitor function.

  Rationale: The Alarm Temperature Range will be set by the Nurse based on the Infant's weight and health. The Infant should be removed from the Isolette within 15 seconds after the Current Temperature falls below or rises above this range. With the normal monitoring provided by the Nurse, this can be accomplished within 10 seconds, leaving 5 seconds for the system to activate the Alarm. Activating the Alarm in less time is desirable.

  If the Current Temperature or the Alarm Temperature Range provided to the monitor function are flagged as invalid or if an internal failure is detected in the monitor function, the monitor function should not be trusted to perform correctly.

  Allowed probability of failure: $< 10^{-5}$ per hour.

Chapter 5

Thermostat System Function

The Thermostat performs two logically independent functions. The first regulates the Current Temperature in the Isolette so it is maintained within the Desired Temperature Range. The second monitors the Current Temperature in the Isolette and activates an Alarm if it falls below or rises above the Alarm Temperature Range.

The high-level requirements for the Thermostat Function are as follows:

- REQ-TH-1: The Thermostat shall set the value of the Heat Control.

  Rationale: A primary function of the Thermostat is to turn the Heat Control on and off to maintain the Current Temperature in the Isolette within the Desired Temperature Range, which is required by SR-1.

- REQ-TH-2: The Thermostat Function shall set the value of the Regulator Status.

  Rationale: SR-1 requires the Thermostat to provide an independent regulator function. The status of this function is provided to the Operator Interface by the Thermostat. The Operator Interface will use the Regulator Status and the Monitor Status to report the overall status of the Thermostat, which is required by SR-1.

- REQ-TH-3: The Thermostat shall set the value of the Display Temperature.

  Rationale: The Current Temperature is displayed on the Operator Interface to provide the operators with an additional means to confirm the Isolette is maintaining the temperature correctly. This value is provided by the Thermostat to the Operator Interface as the Display Temperature.

- REQ-TH-4: The Thermostat shall set the value of the Alarm Control.

  Rationale: A primary Thermostat Function is to activate the Alarm if the Isolette is unable to maintain the Current Temperature within the Alarm Temperature Range, which is required by SR-2.

- REQ-TH-5: The Thermostat shall set the value of the Monitor Status.

  Rationale: SR-2 requires the Thermostat to provide an independent monitor function. The status of this function must be provided to the Operator Interface, which will use it and the status of the regulator function to report the overall status of the thermostat.

The Thermostat Function is allocated into subfunctions as shown in figure 5.1.

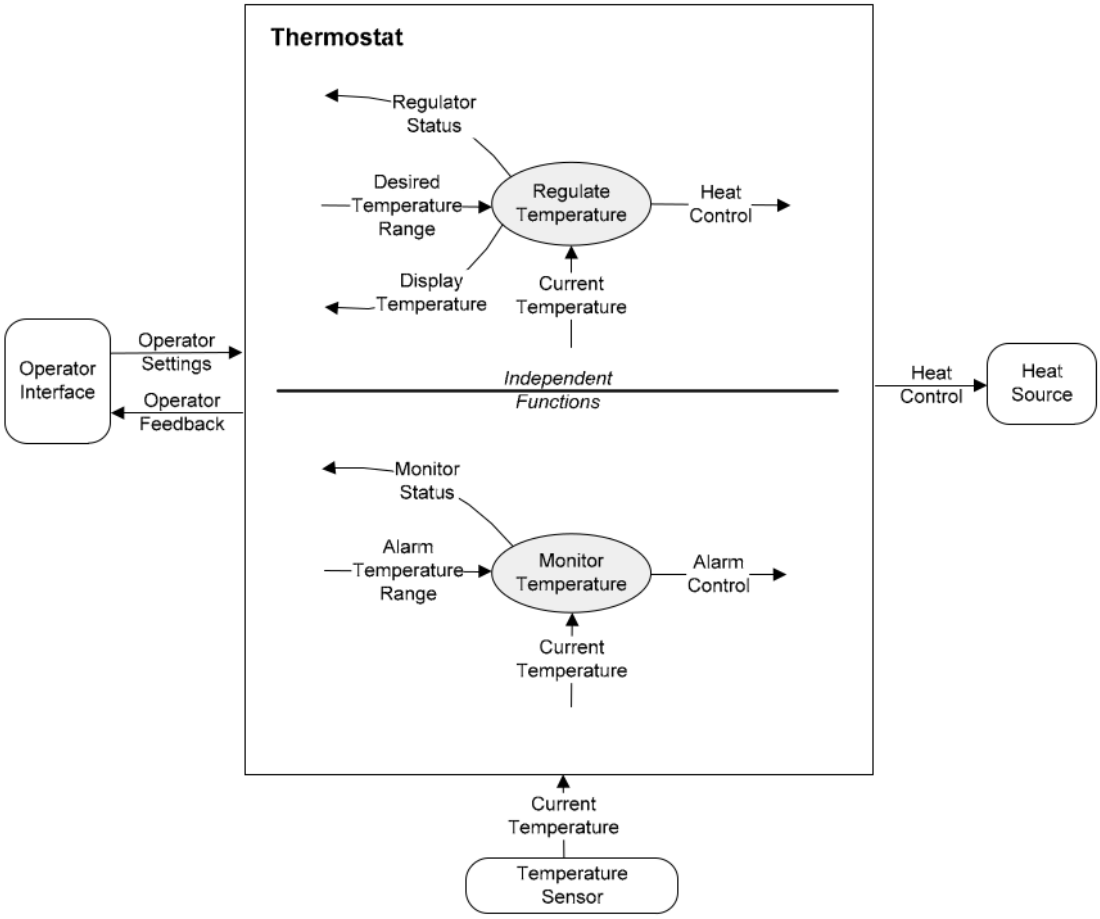

Figure 5.1: Thermostat Dependency Diagram

5.1 Regulate Temperature Function

The Regulate Temperature Function compares the Current Temperature from the Temperature Sensor with the Desired Temperature Range provided by the Operator Interface and turns the Heat Source on or off to keep the Current Temperature within the Desired Temperature Range. It also provides the Display Temperature and the Regulator Status back to the Operator Interface.

The high-level requirements for the Regulate Temperature Function are as follows:

- REQ-RT-1: The Regulate Temperature Function shall set the value of the Heat Control.

  Rationale: The primary function of the Regulate Temperature Function is to turn the Heat

Control on and off to maintain the Current Temperature in the Isolette within the Desired Temperature Range, as required by SR-1.

- REQ-RT-2: The Regulate Temperature Function shall set the value of the Regulator Status.

  Rationale: The status of the Regulate Temperature Function is provided to the Operator Interface so it can use the status of the Regulate Temperature and Monitor Temperature Functions to report the overall status of the Thermostat, as required by SR-1.

- REQ-RT-3: The Regulate Temperature Function shall set the value of the Display Temperature.

  Rationale: The Current Temperature of the Isolette is displayed on the Operator Interface to provide the operators with an additional means to confirm that the Isolette is maintaining the temperature correctly. This value is provided by the Regulate Temperature Function to the Operator Interface as the Display Temperature.

The Regulate Temperature Function is allocated into subfunctions in figure 5.2.

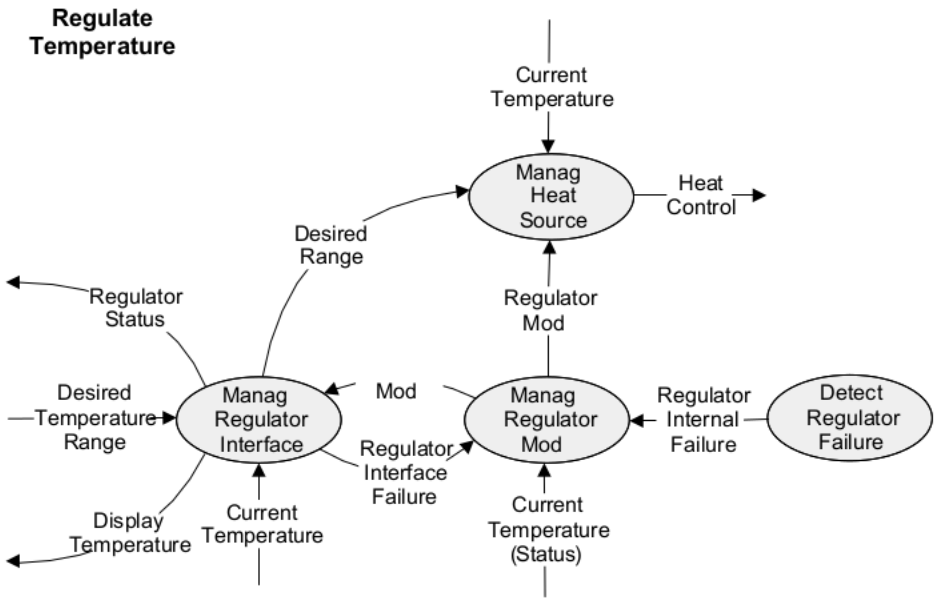

Figure 5.2: Regulate Temperature Dependency Diagram

The internal variables for the Regulate Temperature Function are shown in table 5.1.

5.1.1 Manage Regulator Interface Function

The Manage Regulator Interface Function defines the interaction with the Operator Interface external entity. These include obtaining the Desired Range, reporting back the status of the Regulate Temperature Function, and reporting back the Display Temperature. The constants are shown in table 5.2.

The requirements for the Regulator Status controlled variable are as follows:

Name	Type	Range	Units	Physical Interpretation
Desired Temperature				Desired range of Isolette temperature
Lower Desired Temperature	Integer	[96..101]	°F	Lower value of desired range
Upper Desired Temperature	Integer	[97..102]	°F	Upper value of desired range
Regulator Interface Failure	Boolean	False, True		Indicates an operator interface
Regulator Internal Failure	Boolean	False, True		Indicates an internal failure
Regulator Mode	Enumerated	Init		Initializing following power-up
		NORMAL		Normal mode of operation
		FAILED		Internal failure detected

Table 5.1: The Regulate Temperature Internal Variables

Name	Type	Range	Units	Physical Interpretation
Max Operator Response Time	Real	0.5	Sec	This time an operation will tolerate between an operator request or a change in the Thermostat state and the visible response
Rationale: A trade study has shown that this lag should be no more than 0.5 second.				

Table 5.2: Manage Regulator Interface Function Constants

- REQ-MRI-1: If the Regulator Mode is INIT, the Regulator Status shall be set to Init.
- REQ-MRI-2: If the Regulator Mode is NORMAL, the Regulator Status shall be set to On.
- REQ-MRI-3: If the Regulator Mode is FAILED, the Regulator Status shall be set to Failed.

  Latency: < Max Operator Response Time Tolerance: N/A

The requirements for the Display Temperature controlled variable are as follows:

- REQ-MRI-4: If the Regulator Mode is NORMAL, the Display Temperature shall be set to the value of the Current Temperature rounded to the nearest integer.

  Rationale: Displaying the rounded value of the Current Temperature provides the the most accurate display of the Current Temperature possible using an integer display. When combined with the accuracy of the Temperature Sensor (EA-TS-2), the Display Temperature should be within 0.6°F of the actual value.

- REQ-MRI-5: If the Regulator Mode is not NORMAL, the value of the Display Temperature is UNSPECIFIED.

  Rationale: In modes other than NORMAL, the value of Display Temperature is not meaningful and should not be used.

  Latency: < Max Operator Response Time

  Tolerance: ±0.6°F

The requirements for the Regulator Interface Failure internal variable are as follows:

- REQ-MRI-6: If the Status attribute of the Lower Desired Temperature or the Upper Desired Temperature is Invalid, the Regulator Interface Failure shall be set to True.

Name	Type	Range	Units	Physical Interpretation
Regulator Init Timeout	Real	1.0	Sec	The time allowed for initialization of the Regulate Temperature Function before declaring failure
Rationale: A trade study has shown that users become impatient if the Thermostat requires more than one second to initialize.				

Table 5.3: The Manage Regulator Mode Function Constants

Name	Type	Definition
Regulator Status	Boolean	NOT (Regulator Interface Failure OR Regulator Internal Failure) AND Current Temperature.Status = Valid

Table 5.4: The Manage Regulator Mode Function Definitions

- REQ-MRI-7: If the Status attribute of the Lower Desired Temperature and the Upper Desired Temperature is Valid, the Regulator Interface Failure shall be set to False.

  Rationale: The Regulator Interface Failure internal variable indicates if any errors have occurred in sensing the Operator Interface monitored variables needed by the Regulate Temperature Function. Note that its initial value on power-up will always be True since the Status of the Lower Desired Temperature and the Upper Desired Temperature are initially Invalid.

The requirements for the Desired Range internal variable are as follows:

- REQ-MRI-8: If the Regulator Interface Failure is False, the Desired Range shall be set to the Desired Temperature Range.

- REQ-MRI-9: If the Regulator Interface Failure is True, the Desired Range is UNSPECIFIED.

  Rationale: The Desired Range is only meaningful when there is not a Regulator Interface Failure. If there is, its value should not be used, and it can be set to any value.

5.1.2 Manage Regulator Mode Function

The Manage Regulator Mode Function determines the mode of the Regulate Temperature Function. The constants and definitions are shown in tables 5.3 and 5.4, respectively.

The requirements for the Regulator Mode internal variable are as follows:

- The modes and transitions of the Manage Regulator Mode Function are specified in the state transition diagram shown in figure 5.3. Each transition is a separate requirement and is assigned a unique identifier (e.g., Req MRM 1). All transitions are assumed to occur in negligible time.

  Rationale: (Req MRM 3 and Req MRM 4) Once the regulator has failed, the only way for it to re-enter normal operation is for it to be powered off and on. This ensures that the operators are made aware of any transient failures that the regulator may be experiencing.

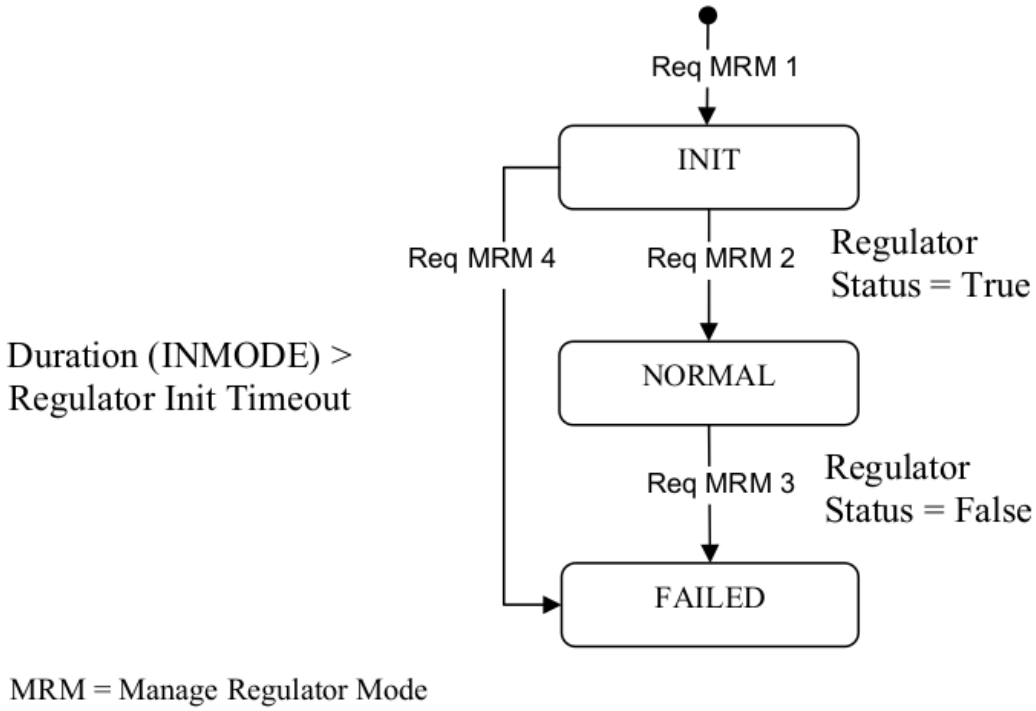

Figure 5.3: Regulate Temperature Mode Transition Diagram

5.1.3 Manage Heat Source Function

The Manage Heat Source Function turns the Heat Source on and off to maintain the Current Temperature of the Isolette within the Desired Temperature Range. The constants are shown in table 5.5.

The requirements for the Heat Control controlled variable are as follows:

- REQ-MHS-1: If the Regulator Mode is INIT, the Heat Control shall be set to Off.

  Rationale: A regulator that is initializing cannot regulate the Current Temperature of the Isolette and the Heat Control should be turned off.

- REQ-MHS-2: If the Regulator Mode is NORMAL and the Current Temperature is less than the Lower Desired Temperature, the Heat Control shall be set to On.

- REQ-MHS-3: If the Regulator Mode is NORMAL and the Current Temperature is greater than the Upper Desired Temperature, the Heat Control shall be set to Off.

- REQ-MHS-4: If the Regulator Mode is NORMAL and the Current Temperature is greater than or equal to the Lower Desired Temperature and less than or equal to the Upper Desired Temperature, the value of the Heat Control shall not be changed.

  Rationale: When the Isolette is warming towards the Upper Desired Temperature, the Heat Source should be left on until the Upper Desired Temperature is reached. In a similar fashion,

Name	Type	Range	Units	Physical Interpretation
Allowed Heat Source Latency	Real	6.0	Sec	The maximum time by which the Heat Source must be turned on or off to ensure acceptable Operation of the Isolette system
Since a closed Isolette will warm or cool at a maximum rate of 1°F per minute (EA-IS1 and EA-IS2), turning the Heat Source on or off within 6 seconds ensures that the Current Temperature will not have changed by more than 0.1°F, the required accuracy and resolution of the Temperature Sensor (EA-TS2).				

Table 5.5: The Manage Heat Source Function Constants

if the Isolette is cooling towards the Lower Desired Temperature, the Heat Source should be left off until the Lower Desired Temperature is reached.

- REQ-MHS-5: If the Regulator Mode is FAILED, the Heat Control shall be set to Off.

  Rationale: In failed mode, the regulator cannot regulate the Current Temperature of the Isolette and the Heat Control should be turned off.

  Latency: < Allowed Heat Source Latency

  Tolerance: N/A

5.1.4 Detect Regulator Failure Function

The Detect Regulator Failure Function identifies internal failures, (e.g., a memory check failure) in the Regulate Temperature Function. It defines a single Boolean-valued internal variable, Regulator Internal Failure, which is set to True if an internal failure is detected.

The requirements for Regulator Internal Failure variable are implementation-specific and cannot be specified until an implementation platform is chosen.

5.2 Monitor Temperature Function

The Monitor Temperature Function compares the Current Temperature from the Temperature Sensor with the Alarm Temperature Range provided by the Operator Interface and turns the Alarm Control on or off to Alert The Nurse if the Current Temperature falls below or rises above the safe range. It also provides the Monitor Status back to the Operator Interface.

The high-level requirements for the Monitor Temperature Function are as follows:

- REQ-MT-1: The Monitor Temperature Function shall set the value of the Alarm Control.

  Rationale: The primary function of the Monitor Temperature Function is to raise an alarm if the Isolette is unable to maintain the Current Temperature within the Alarm Temperature Range, as required by safety requirement SR-2.

- REQ-MT-2: The Monitor Temperature Function shall set the value of the Monitor Status.

  Rationale: Safety requirement SR-2 requires the Thermostat to provide an independent monitor function. The status of this function must be provided to the Operator Interface, which

will use it and the status of the Regulate Temperature Function to report the overall status of the Thermostat, as required by safety requirement SR-2.

The Monitor Temperature Function is allocated into subfunctions as shown in figure 5.4.

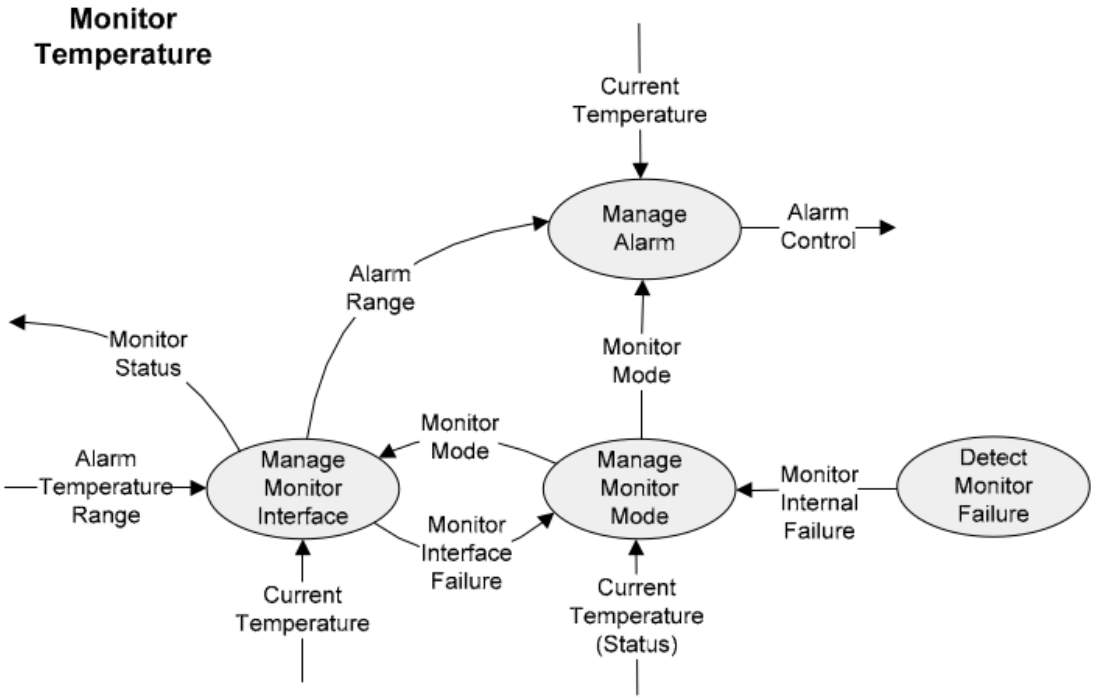

Figure 5.4: Monitor Temperature Dependency Diagram

The Monitor Temperature internal variables are shown in table 5.6.

5.2.1 Manage Monitor Interface Function

The Manage Monitor Interface function defines the interaction with the Operator Interface external entity. These include obtaining the Alarm Range and reporting back the status of the Monitor Temperature Function. The constants are shown in table 5.7.

The requirements for the Monitor Status controlled variable are as follows:

- REQ-MMI-1: If the Manage Monitor Interface mode is INIT, the Monitor Status shall be set to Init.
- REQ-MMI-2: If the Manage Monitor Interface mode is NORMAL, the Monitor Status shall be set to On.
- REQ-MMI-3: If the Manage Monitor Interface mode is FAILED, the Monitor Status shall be set to Failed.

  Latency: < Max Operator Response Time

  Tolerance: N/A

Name	Type	Range	Units	Physical Interpretation
Alarm Range				Safe range of Isolette temperature
Lower Alarm Temperature	Integer	[96..101]	°F	Lower value of alarm range
Upper Alarm Temperature	Integer	[97..102]	°F	Upper value of alarm range
Monitor Interface Failure	Boolean	False, True		Indicates an operator interface failure
Monitor Internal Failure	Boolean	False, True		Indicates an internal failure
Monitor Mode	Enumerated	Init		Initializing following power-up
		NORMAL		Normal mode of operation
		FAILED		Internal failure detected

Table 5.6: Monitor Temperature Internal Variables

Name	Type	Range	Units	Physical Interpretation
Max Operator Response Time	Real	0.5	Sec	This time an operation will tolerate between an operator request or a change in the Thermostat state and the visible response
Rationale: A trade study has shown that this lag should be no more than 0.5 second.				

Table 5.7: The Manage Monitor Interface Function Constants

The requirements for Monitor Interface Failure internal variable are as follows:

- REQ-MMI-4: If the Status attribute of the Lower Alarm Temperature or the Upper Alarm Temperature is Invalid, the Monitor Interface Failure shall be set to True.
- REQ-MMI-5: If the Status attribute of the Lower Alarm Temperature and the Upper Alarm Temperature is Valid, the Monitor Interface Failure shall be set to False.

  Rationale: The Monitor Interface Failure internal variable indicates if any errors have occurred in sensing the Operator Interface monitored variables needed by the Manage Temperature Function. Note that its initial value on power-up will always be True since the Status attribute of the Lower Alarm Temperature and the Upper Alarm Temperature will initially be Invalid.

The requirements for Alarm Range Internal variable are as follows:

- REQ-MMI-6: If the Monitor Interface Failure is False, the Alarm Range variable shall be set to the Desired Temperature Range.
- REQ-MMI-7: If the Monitor Interface Failure is True, the Alarm Range variable is UNSPECIFIED.

  Rationale: The Alarm Range variable is only meaningful when there is not a Monitor Interface Failure. If there is, its value should not used and it can be set to any value.

5.2.2 Manage Monitor Mode Function

The Manage Monitor Mode Function determines the mode of the Monitor Temperature Function. The constants and definitions are shown in tables 5.8 and 5.9, respectively.

The requirements for the Regulator Mode internal variable are as follows:

Name	Type	Range	Units	Physical Interpretation
Monitor Initialization Timeout	Real	1.0	Sec	The time allowed for initialization of the Monitor Temperature Function before declaring failure
Rationale: A trade study has shown that users become impatient if the Thermostat requires more than one second to initialize.				

Table 5.8: The Manage Monitor Mode Function Constants

Name	Type	Definition
Monitor Status	Boolean	NOT (Monitor Interface Failure OR Monitor Internal Failure) AND Current Temperature.Status = Valid

Table 5.9: The Manage Monitor Mode Function Definitions

- The modes and transitions of the Manage Regulator Mode Function are specified in the state transition diagram shown in figure 5.5. Each transition is a separate requirement and is assigned a unique identifier (e.g., Req MRM 1). All transitions are assumed to occur in negligible time.

  Rationale: (Req MRM 3 and Req MRM 4) Once the regulator has failed, the only way for it to re-enter normal operation is for it to be powered off and on. This ensures that the operators are made aware of any transient failures that the regulator may be experiencing.

5.2.3 Manage Alarm Function

The Manage Alarm Function turns the Alarm Control on when the Current Temperature of the Isolette falls below or rises above the Alarm Temperature Range.

The requirements for the Alarm Control controlled variable are as follows:

- REQ-MA-1: If the Monitor Mode is INIT, the Alarm Control shall be set to Off.

  Rationale: A monitor that is initializing should not activate the alarm unless it enters the FAILED mode.

- REQ-MA-2: If the Monitor Mode is NORMAL and the Current Temperature is less than the Lower Alarm Temperature or greater than the Upper Alarm Temperature, the Alarm Control shall be set to On.

- REQ-MA-3: If the Monitor Mode is NORMAL and the Current Temperature is greater than or equal to the Lower Alarm Temperature and less than the Lower Alarm Temperature +0.5°, or the Current Temperature is greater than the Upper Alarm Temperature -0.5° and less than or equal to the Upper Alarm Temperature, the value of the Alarm Control shall not be changed.

  Rationale: This provides a hysteresis that prevents transient alarms, see figure 5.6.

- REQ-MA-4: If the Monitor Mode is NORMAL and the value of the Current Temperature is greater than or equal to the Lower Alarm Temperature +0.5° and less than or equal to the Upper Alarm Temperature -0.5°, the Alarm Control shall be set to Off.

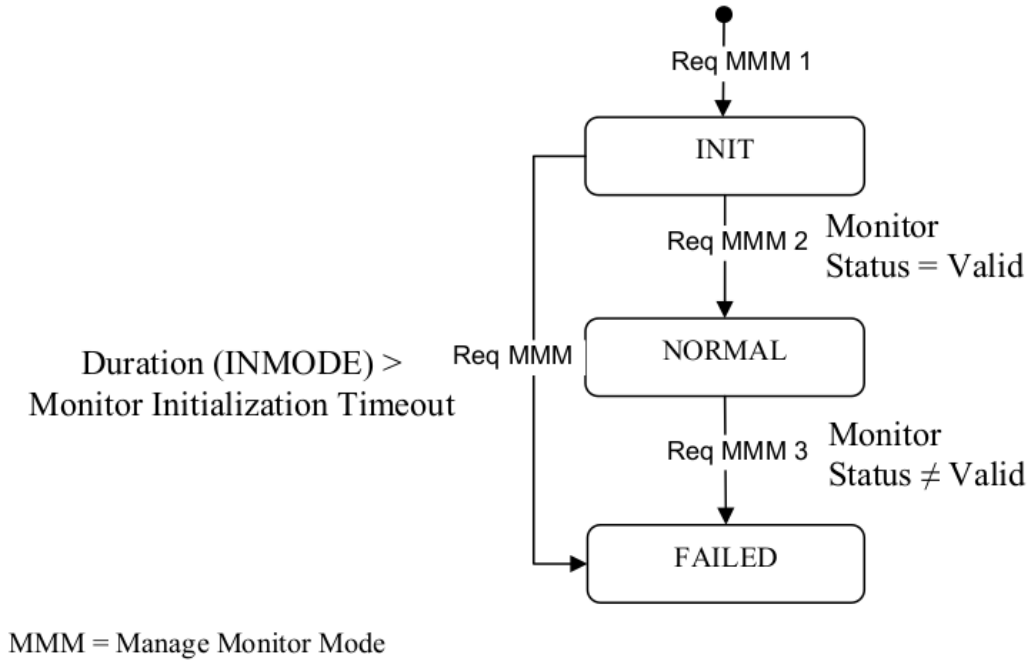

Figure A-6. Monitor Temperature Mode Transition Diagram

Figure 5.5: Monitor Temperature Mode Transition Diagram

Rationale: This turns the alarm 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.

- REQ-MA-5: If the Monitor Mode is FAILED, the Alarm Control shall be set to On.

  Rationale: A failed monitor cannot monitor the Current Temperature of the Isolette and the Alarm should be turned on.

  Latency: <5 seconds

  Tolerance: N/A

  Rationale: Required by SR-2.

5.2.4 Detect Monitor Failure Function

The Detect Monitor Failure Function identifies internal failures, (e.g., a memory check failure) in the Monitor Temperature Function. It defines a single Boolean-valued internal variable, Monitor Internal Failure, which is set to True if an internal failure is detected.

The requirements for Monitor Internal Failure variable are implementation-specific and cannot be specified until an implementation platform is chosen.

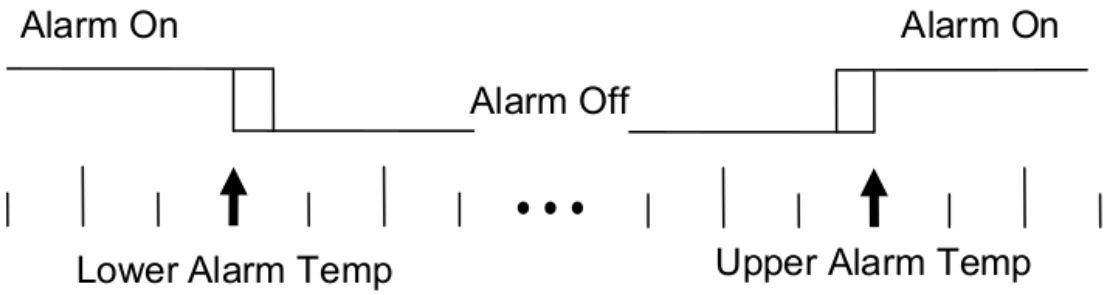

Figure 5.6: Transient Alarm Hyperesis