Designing a safety-critical system for the control of temperature and humidity in hazardous environments

Benjamin Tozer
Department of Electrical Engineering
University of New Brunswick
Fredericton, Canada
btozer1@unb.ca

Myah Bowal
Department of Electrical Engineering
University of New Brunswick
Fredericton, Canada
myah.bowal@unb.ca

Nicholas McLean
Department of Electrical Engineering
University of New Brunswick
Fredericton, Canada
mclean.nick765@unb.ca

Md Mohitul Haque
Department of Electrical Engineering
University of New Brunswick
Fredericton, Canada
mohitul.haque@unb.ca

***Abstract*— This document details the design of a safety-critical system that will ensure that a toxic biological agent is quarantined within its greenhouse. Included is an analysis of factors, design of a prototype, hazard identification, and analysis (including Fault Tree Analysis; Failure Modes and Effects Analysis; Event Tree Analysis; Risk Analysis; and Failure Modes and Effects Testing). Also detailed are mishap mitigation measures that are used to improve the reliability of the prototype. Additionally, a final comparison between this design and with relevant standards is included.**

Keywords—Safety-critical system design

I. Introduction

Critical temperature and humidity controls in hazardous environments contain a significant amount of risk, that can cause severe mishap to the surrounding environment and human population. The safety-critical application analyzed is required to monitor and control the temperature and humidity of a confined experimental greenhouse which is considered a safety-critical biologically hazardous environment. The greenhouse contains a specific non-disclosed plant that happens to be infested with insects (scale-dawn) causing the plants' leaves to turn yellow and slowly die. In hopes of preventing the non-disclosed plants from these insects a biological agent has been developed that can control the dangerous insects. This biological agent has no significant information tied to it, but it may be harmful to humans, therefore release into the surrounding environment could have the potential to set off an epidemic. This epidemic could cause death of many humans as well as harm other aspects of the environment.

To try and mitigate the risks of this catastrophic event from occurring, a detailed approach must be followed to ensure nothing is harmed. The approach represented is required to contain a considerable number of components. An accurate temperature and humidity control mechanism is essential to sustain a precise range of temperature and humidity. The temperature must be consistently dispersed throughout the controlled greenhouse space between the range of 30-40 degrees Celsius. The humidity must present a value between 50-70%. If these two aspects cannot be maintained an unmanageable diminish/growth of the unknown biological agent posing a harmful effect on humans and the surrounding environment may be released. Bacteria has been well determined to exponentially grow with an increase in temperature. With this risk in mind, a wireless remote-controlled system is needed to increase or decrease both the humidity and the temperature. This will allow the biological agent to be safely controlled from a distance without the need of physically entering the controlled greenhouse environment. The system will also be equipped with a wireless temperature/humidity sensing distribution system. In hopes of controlling the insect population a control mechanism has been installed as well as space access control allowing trained personnel safely into the environment when necessary.

II. Design

A. System Description

The system's temperature has to be maintained between 30°C and 40°C and its humidity is to be maintained between 50% to 70%.

Table 1 displays the equipment used for the prototype. Numbers in brackets indicate values that have increased after mishap mitigation techniques have been implemented.

Table.1. Equipment List

Device name	Quantity
Mbed LPS1768 board	2 (+1)
Relays (Sunfounder relay module)	1 module packaged with 5 relays (3 were used)
Heater-Resistor 25 OHM 50W	1
DC brushless QuietTek 12V fan	2
Sensors-DHT11 (temperature and humidity)	2 (+1)
LED for population control mechanism and access control	2
Power supply JKL1200500	1
Power supply (backup, model number soldered)	1 (+1)
Current sensor	3 (+3)

Vibration sensor	2 (+2)

In this system, the Mbed LPC1768 is used as the main CPU. It is based on 32-bit ARM® Cortex™-M3 core. The Mbed is used to control the entire system. It reads data from the sensors and controls the effectors and population control mechanism. It is equipped with USB, Ethernet, FLASH memory and the flexibility of several peripheral interfaces. It also has many libraries that can be used to implement mishap mitigation techniques and sensors. It also has sufficient I/O ports to implement the sensors and actuators of the rest of the system. Fig.1 displays the pin diagram of this model [1].

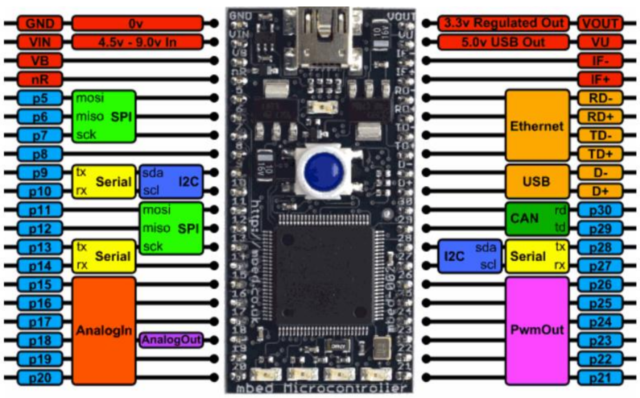


Fig. 1. Pin diagram of Mbed LPC1768 [1]

In fig.2, the flow diagram of the microcontroller operation is shown.

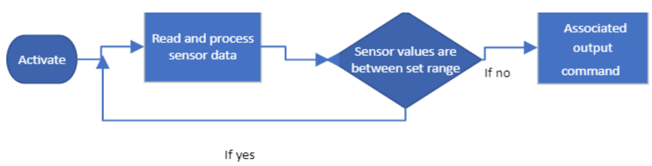


Fig. 2. Flow diagram of Mbed operation

A secondary LPC1768 board has been implemented as a backup.

Relays are used in this system as a method of providing power to the actuators. These actuators include a 25 OHM heater-resistor is used to increase the heat the greenhouse. 12VDC fans, one for increasing input airflow (IN) and another to increase output airflow (OUT) are used to both regulate the humidity and temperature. The fan IN is used to decrease the temperature or increase the humidity. The fan OUT is used decrease the humidity. Together, these three actuators are enough to regulate the temperature and humidity within the greenhouse.

The power supply used in this system is the JKL1200500. It was primarily chosen due to its availability and the familiarity of the design team with the model. As a backup, another power supply was used (soldered serial number). It was selected due to its availability.

A DHT11 sensor is used to sense the temperature and humidity within the greenhouse. It is a digital smart-sensor, however, the LPS1768 board has libraries that simplify the communication between the sensor and the microcontroller.

Two LEDs are used, each with a different purpose. One is to indicate that the agent population control mechanism has been actuated. This was chosen as it was an easy way to indicate the culling of the fictional agents (which could theoretically be killed by light of a specific wavelength). The other LED is to indicate to incoming personnel that the containment door to the greenhouse is not to be opened. This prevents further mishap which would happen if the agent were to escape containment.

In addition to the simplex components, current sensors and vibration sensors are used as a mishap mitigation technique to monitor the DC fans and the resistive heater. Fig. 3 shows all of these elements combined into a single, fail-operate system.

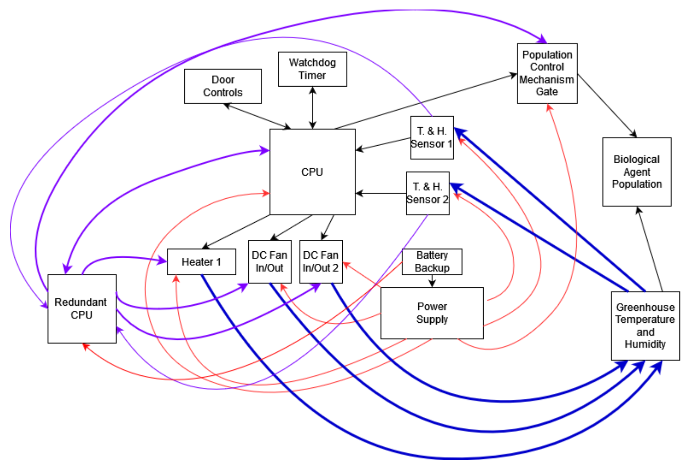


Fig. 3. Fail-operate system

B. *Mishap Mitigation Measurements*

The following section details the mishap mitigation techniques that have been implemented into the prototype design.

End-around tests for the I/O pins are implemented in the design. This involves having four of the LPC1768 output signals (three actuators and the agent control mechanism) immediately looping back to an input pin in the LPC1768. This will test for faults in both the input and output pins of the embed board. Wrap-around tests for the three actuators are implemented. This was done by adding a current sensor to the output of each DC fan as well as to the resistive heater. A proportional level of current to the input indicates that these devices are operating.

Memory checks are done in-software by writing (alternating 1's and 0's) to each memory block individually and then reading that block to verify that it stored that information correctly. A watchdog timer is implemented internal to the LPC1768. This involves watchdog timer libraries and a reset to the timer inside the main loop of the program. A try-catch block has been implemented in the software. This involves wrapping the main loop of the program in a try-catch block so that errors are caught. Register checks are done by in-software by having the MCU solve a complicated equation with a known solution and then compare it with the result to make sure that they are consistent.

Vibration sensors are used on both DC fans to verify that they are spinning when required and to ensure that the fans are not failing on. Power interlocks to the actuators are implemented by the use of normally-open relays as inputs to all three actuators. This is to isolate these actuators if they were to fail on. Various elements of redundancy have also been added. See section 2.C.

C. Other Specific Safety Features

In addition to the mishap mitigation techniques implemented above, the following features have been added to the system as an additional layer of safety.
To add a layer of redundancy, another LPC1768 board is used as a backup. It will have communication with the other MCU to know when to turn on. It will also be able to control all three actuators, the agent control mechanism, and the zone access control indicator. However, it will not have access to a computer for operator live monitoring. It will also only have access to one sensor compared to the two of the primary board. Another important element of redundancy is the backup power supply. This is a device with a high probability of failure, so redundancy for this particular component is extremely important. An additional sensor has also been used to reduce the risk of sensing errors. These three elements are individual elements with high degree of failure probability which is why they were selected to have redundant components.

III. Design Evaluation

See Appendices A-F for FMEA/FMECA, FTA, ETA, RA, and FMET analyses for both the simplex and fail-operate systems.

IV. Conclusions

A. Evaluation of System with Respect to Standards

System factor assessment indictates that the highest-level mishap will result in a pandemic and massive environmental damage, which would be considered catastrophic. IEC 61508: Community Impact defines this level of impact as a Safety Integrity Level 4. And the corresponding acceptable probability of this happening should be within the $\geq 10^{-9}\ to < 10^{-8}$ occurrences per hour.

Additionally, comparing this to Safety Integrity Level 2 as indicated by the MIL-STD-882D, the probability should be within $\geq 10^{-7}\ to < 10^{-6}$ occurrences per hour.
Risk analysis done to the Fault Tree Analysis (see Appendix F) indicates that the mishap probability of the fail-operate system is $6.4\text{x}10^{-10}$. This is acceptable risk for both standards.

B. Final Comments

The mishap mitigation techniques designed for this safety critical system were sufficient to reduce the probability of a mishap from $6.6\text{x}10^{-9}$ to $6.4\text{x}10^{-10}$ occurences per hour.

Acknowledgments

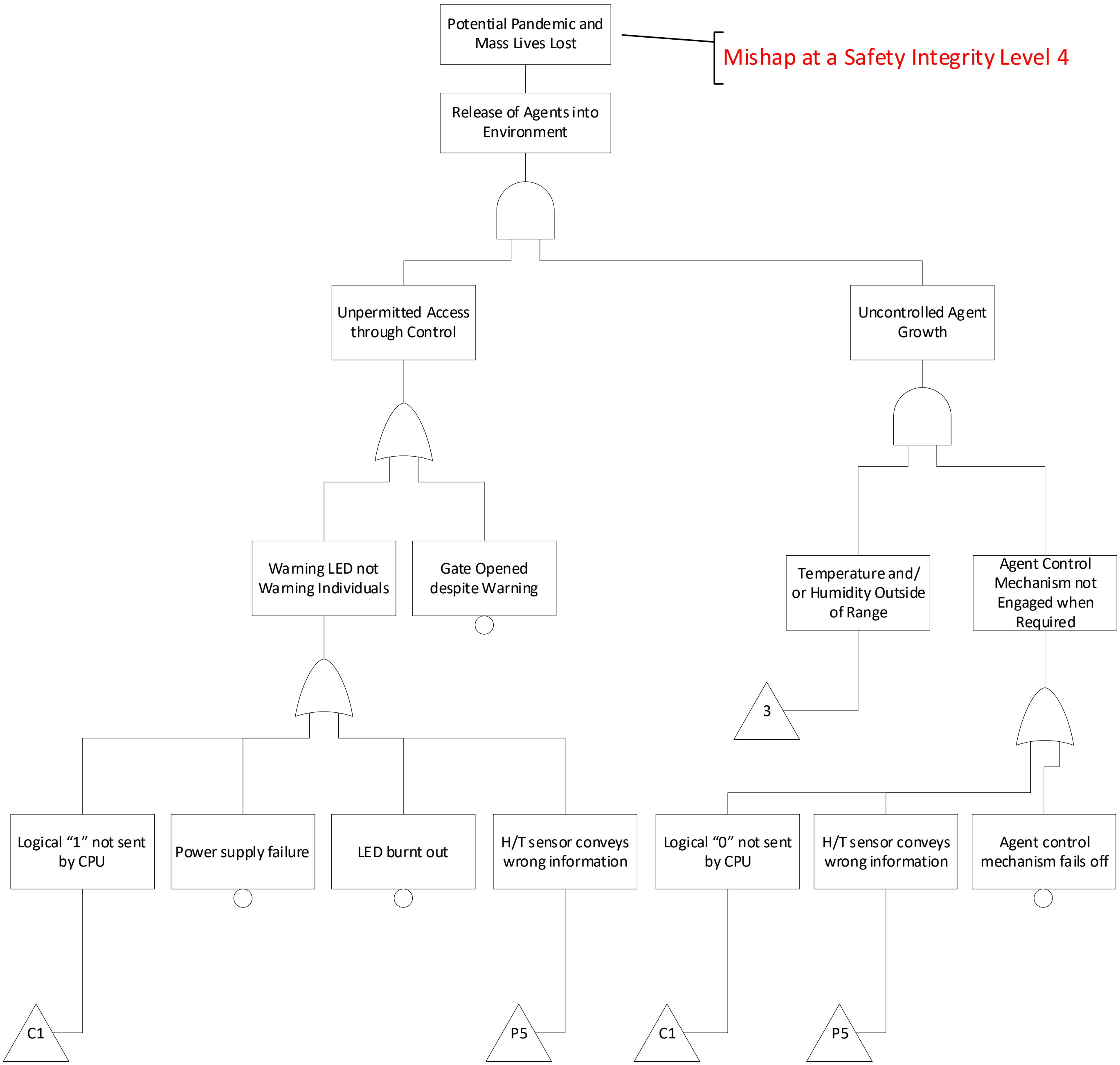
Thanks to Dr. Castillo.

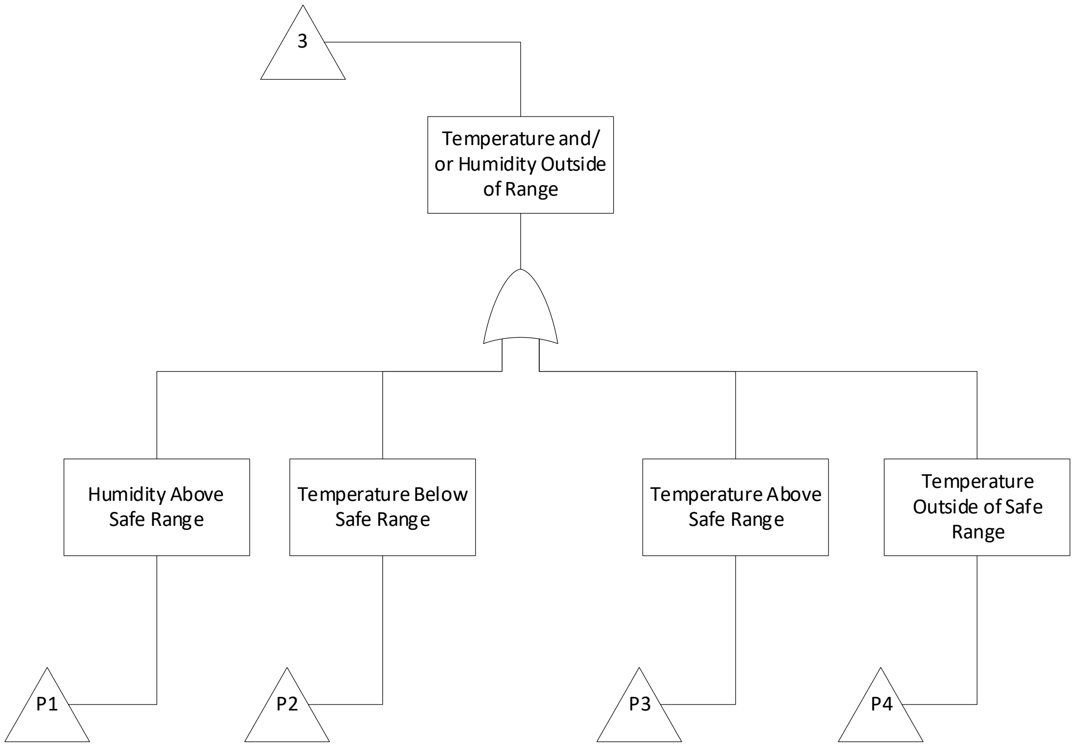
References

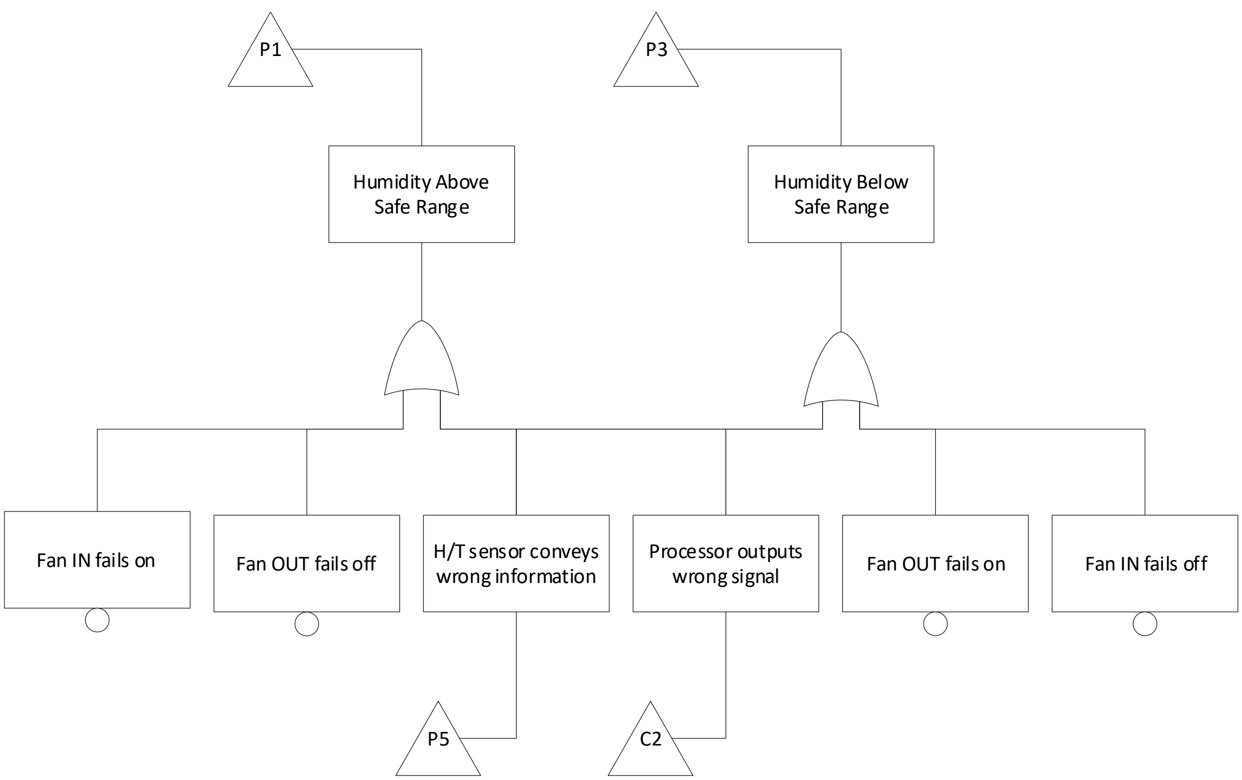
[1] https://os.mbed.com/platforms/mbed-LPC1768/

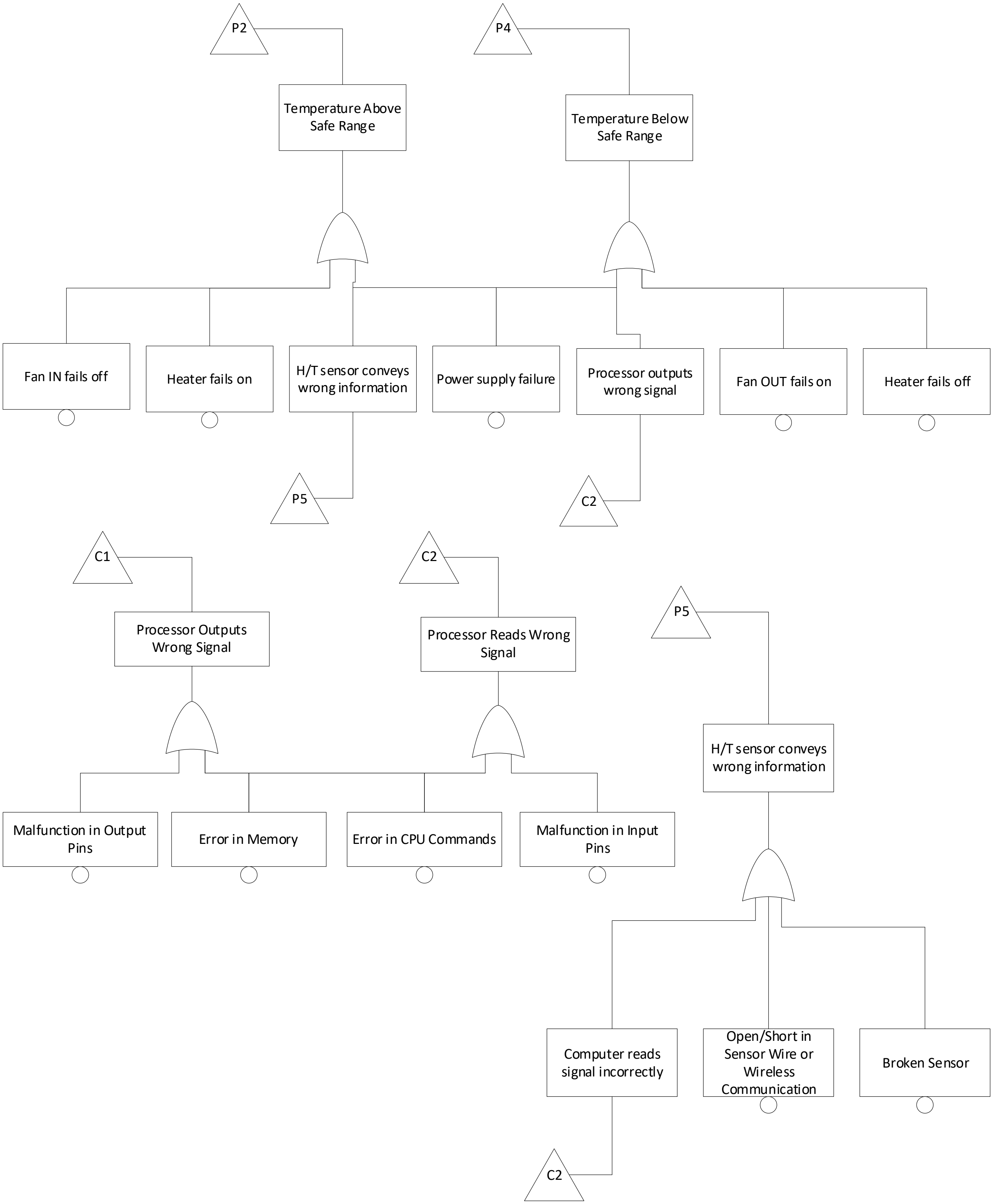
APPENDIX A: FAULT TREE ANALYSIS (SIMPLEX AND FAIL-OPERATE)

A.1: Simplex FTA

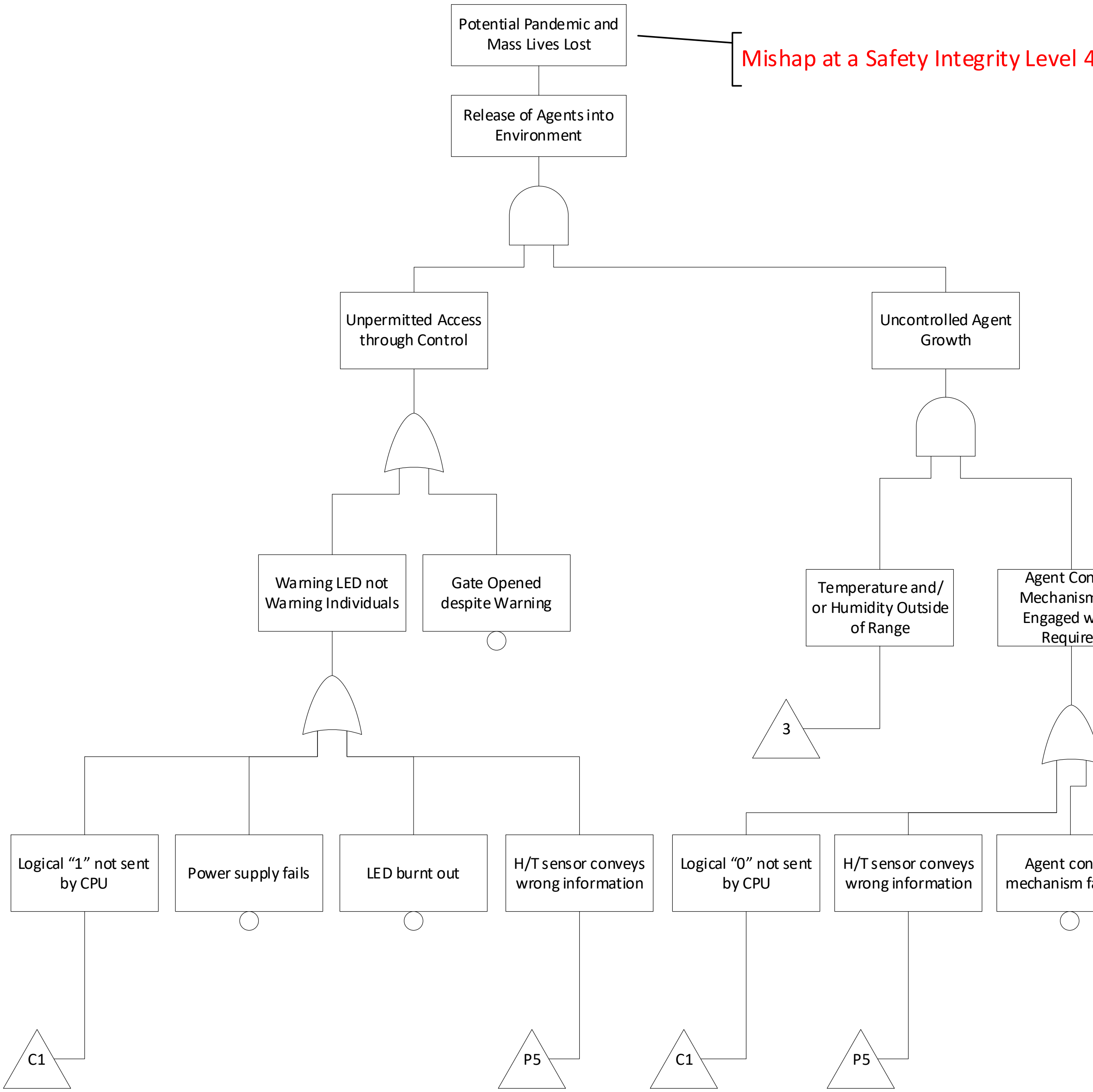



3
Temperature and/ or Humidity Outside of Range
Humidity Above Safe Range
Temperature Below Safe Range
Temperature Above Safe Range
Temperature Outside of Safe Range
P1
P2
P3
P4

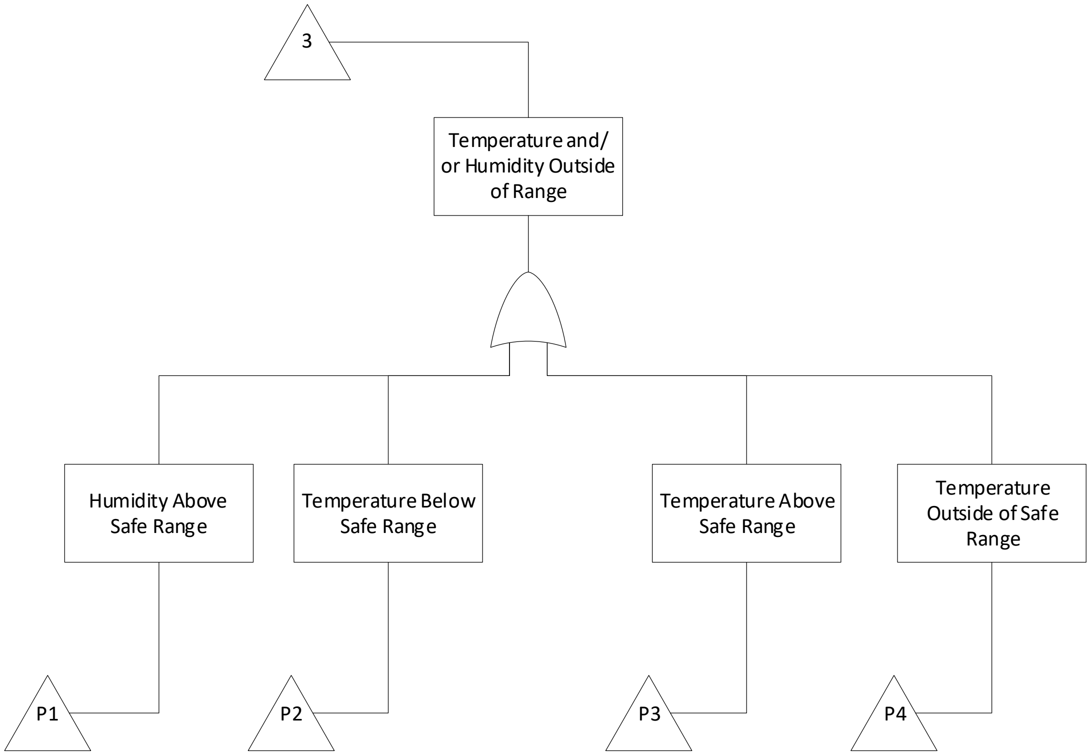

P1
P3
Humidity Above Safe Range
Humidity Below Safe Range
Fan IN fails on
Fan OUT fails off
H/T sensor conveys wrong information
Processor outputs wrong signal
Fan OUT fails on
Fan IN fails off
P5
C2

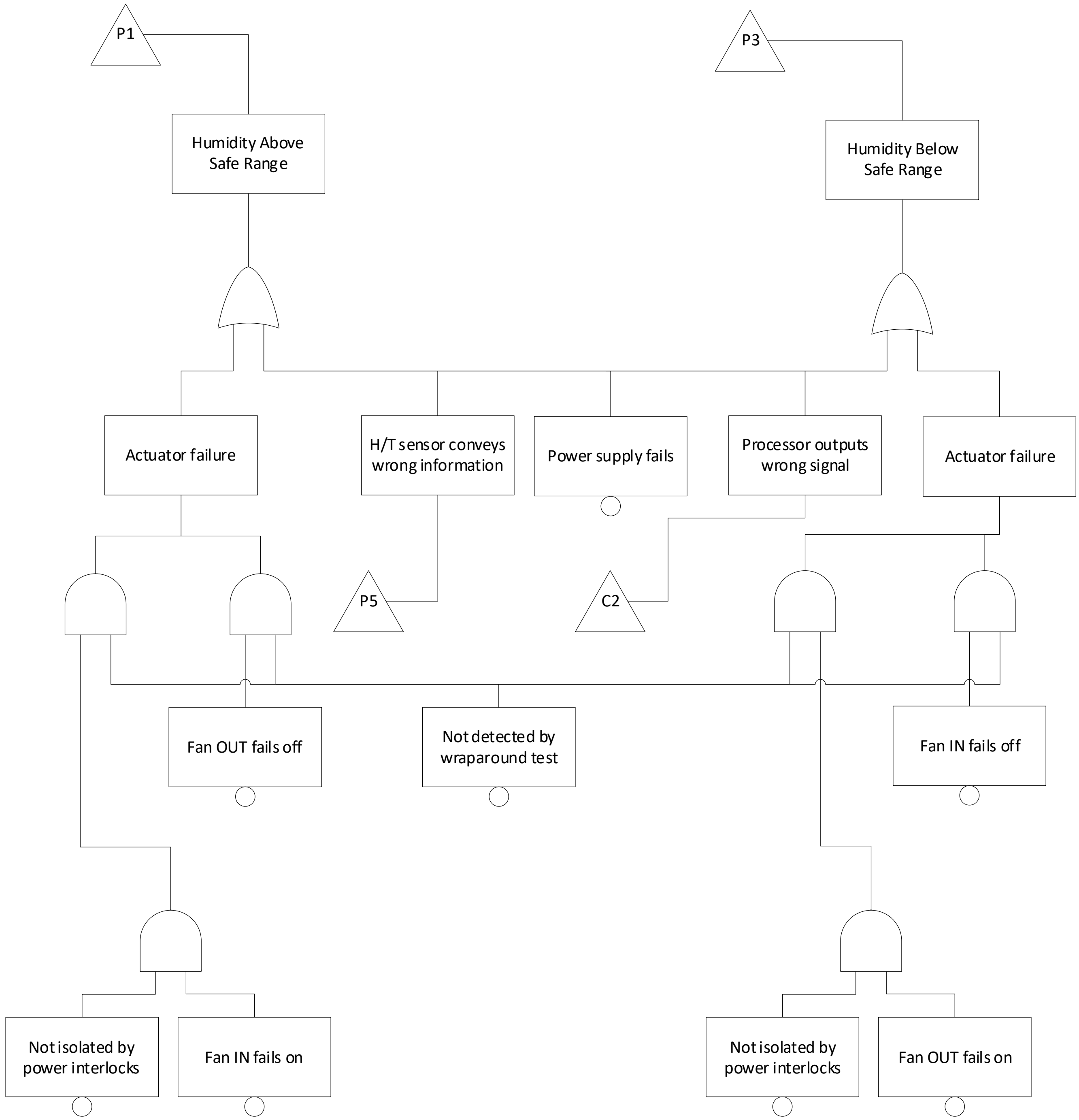

P2
Temperature Above Safe Range
P4
Temperature Below Safe Range
Fan IN fails off
Heater fails on
H/T sensor conveys wrong information
Power supply failure
Processor outputs wrong signal
Fan OUT fails on
Heater fails off
P5
C2
C1
Processor Outputs Wrong Signal
C2
Processor Reads Wrong Signal
P5
H/T sensor conveys wrong information
Malfunction in Output Pins
Error in Memory
Error in CPU Commands
Malfunction in Input Pins
Computer reads signal incorrectly
Open/Short in Sensor Wire or Wireless Communication
Broken Sensor
C2

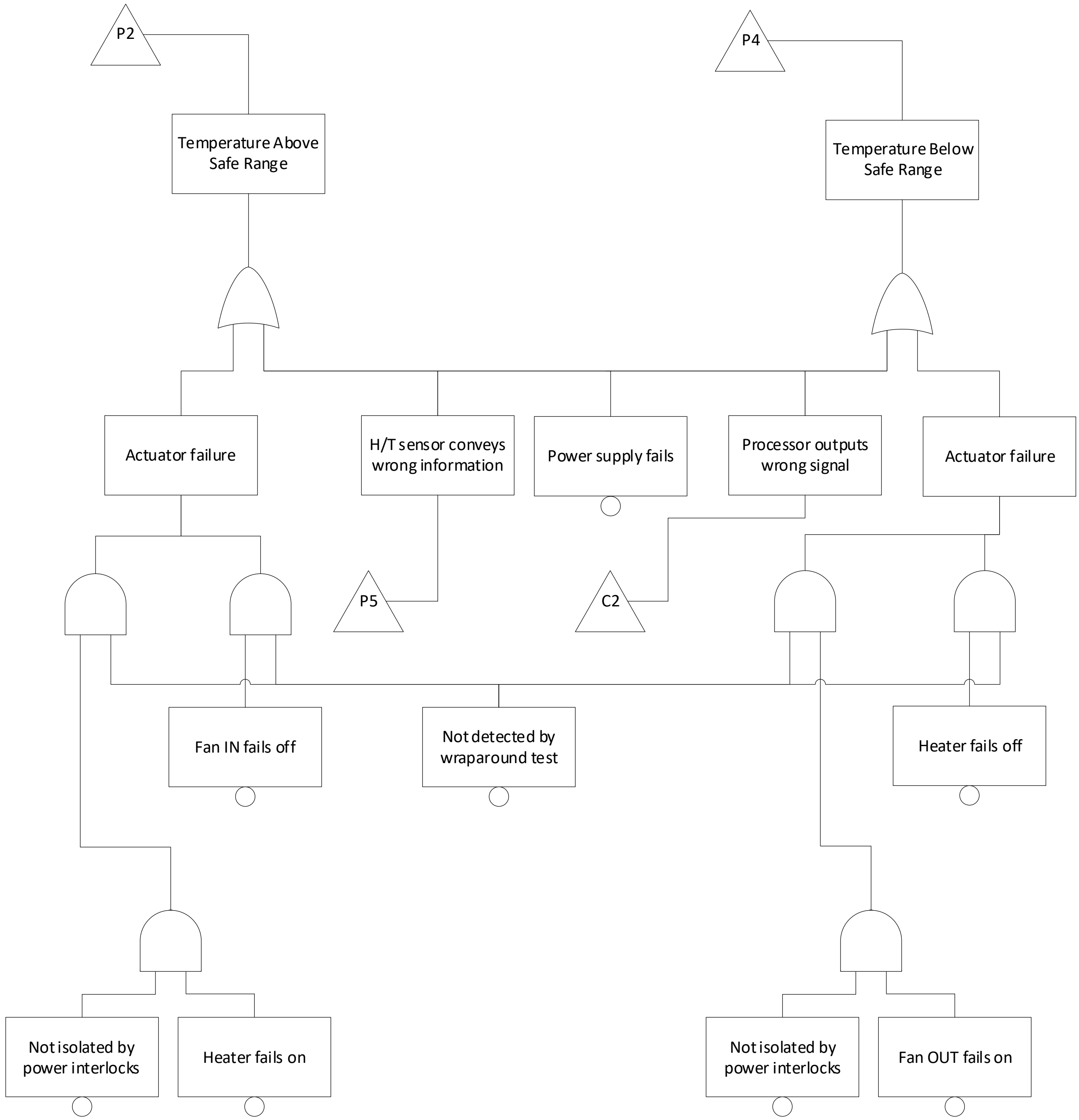
A.2: Fail-Operate FTA



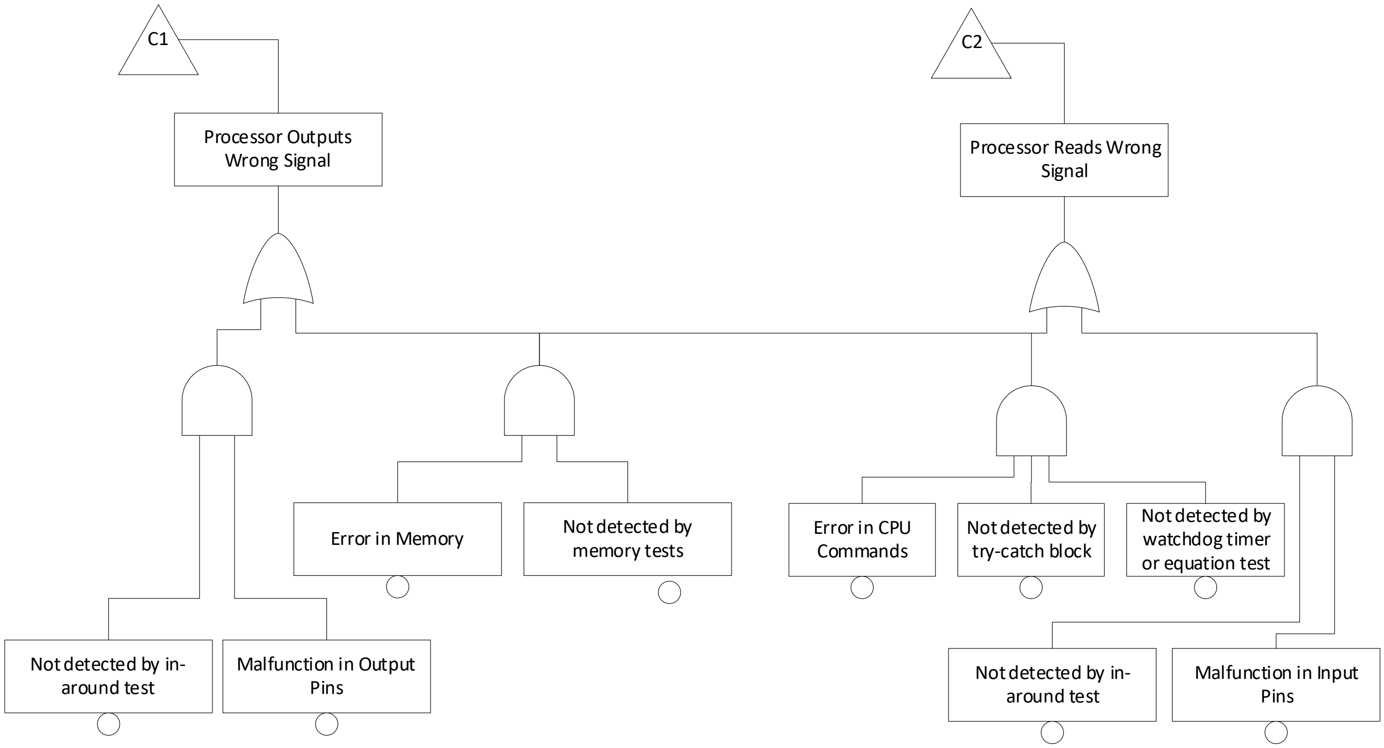
A.2: Fail-Operate FTA (Continued)

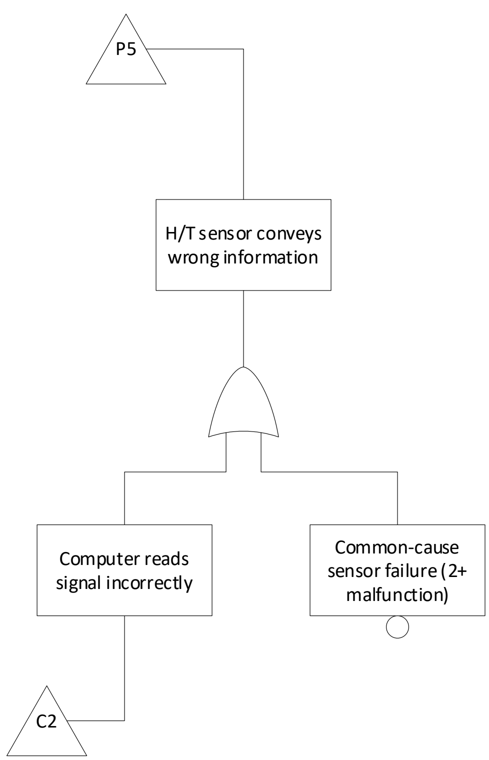



P1
Humidity Above Safe Range
P3
Humidity Below Safe Range
Actuator failure
H/T sensor conveys wrong information
Power supply fails
Processor outputs wrong signal
Actuator failure
P5
C2
Fan OUT fails off
Not detected by wraparound test
Fan IN fails off
Not isolated by power interlocks
Fan IN fails on
Not isolated by power interlocks
Fan OUT fails on



P2
P4
Temperature Above Safe Range
Temperature Below Safe Range
Actuator failure
H/T sensor conveys wrong information
Power supply fails
Processor outputs wrong signal
Actuator failure
P5
C2
Fan IN fails off
Not detected by wraparound test
Heater fails off
Not isolated by power interlocks
Heater fails on
Not isolated by power interlocks
Fan OUT fails on


C1
Processor Outputs Wrong Signal
C2
Processor Reads Wrong Signal
Error in Memory
Not detected by memory tests
Error in CPU Commands
Not detected by try-catch block
Not detected by watchdog timer or equation test
Not detected by in-around test
Malfunction in Output Pins
Not detected by in-around test
Malfunction in Input Pins


P5
H/T sensor conveys wrong information
Computer reads signal incorrectly
Common-cause sensor failure (2+ malfunction)
C2

Appendix B: Failure Mode and Effects Analysis

B.1: Simplex FMEA

Component	Failure Mode	Failure Effect
Temperature & Humidity Sensor	Temperature reads low	Temperature falsely increased resulting in possible unchecked growth of agent (no response)
	Temperature reads high	Temperature falsely decreased resulting in possible mass death of agent (no response)
	Humidity reads low	Humidity falsely increased resulting in possible unchecked growth of agent (no response)
	Humidity reads high	Humidity falsely decreased resulting in possible mass death of agent (no response)
Heater	Fail on	Possible unchecked growth of agent (no response)
	Fail off	Possible mass death of agent (no response)
Fan In/Out	Fail on In	Possible unchecked growth of agent (no response)
	Fail on Out	Possible mass death of agent (no response)
	Fail off In	Possible mass death of agent (no response)
	Fail off Out	Possible unchecked growth of agent (no response)
Power Supply	Short power outage	Possible unchecked growth or mass death of agent (no response) Access door locked (NH)
	Long power outage	Possible unchecked growth or mass death of agent (no response) Access door locked (NH)
Door Controls	Fail unlocked	Possible unauthorized access to facility (no response)
	Fail locked	No access to facility (NH)
Population control mechanism gate	Fail open	Mass death of agent (no response)
	Fail closed	Possible unchecked growth of agent (no response)
CPU	Memory failure	Possible unchecked growth or mass death of agent (no response)
	Incorrect output to actuators	Possible unchecked growth or mass death of agent (no response)
	Incorrect interpretation of sensor data	Possible unchecked growth or mass death of agent (no response)
	Falsely conveys door all clear	Possible unauthorized access to facility (no response)
	Falsely conveys door warning signal	No access to facility (NH)

B.2: Fail-Operate FMEA

Component	Failure Mode	Failure Effect
Temperature & Humidity Sensor	Temperature reads low	Redundant sensor corrects failure (NH)
	Temperature reads high	Redundant sensor corrects failure (NH)
	Humidity reads low	Redundant sensor corrects failure (NH)
	Humidity reads high	Redundant sensor corrects failure (NH)
Heater	Fail on	Wrap-around test catches failure and population control mechanism is used to kill the agent and move the system to a safe state
	Fail off	Wrap-around test catches failure and population control mechanism is used to kill the agent and move the system to a safe state
Fan In/Out	Fail on In	Wrap-around test catches failure and power is disconnected. Redundant fan corrects failure (NH)
	Fail on Out	Wrap-around test catches failure and power is disconnected. Redundant fan corrects failure (NH)
	Fail off In	Wrap-around test catches failure. Redundant fan corrects failure (NH)
	Fail off Out	Wrap-around test catches failure. Redundant fan corrects failure (NH)
Power Supply	Short power outage	Back-up power supply is activated (NH)
	Long power outage	Back-up power supply is activated (NH)
Door Controls	Fail unlocked	Possible unauthorized access to facility (no response)
	Fail locked	No access to facility (NH)
Population control mechanism gate	Fail open	Mass death of agent (no response)
	Fail closed	Possible unchecked growth of agent (no response)
CPU	Memory failure	Detected by memory test, failed locations isolated (NH)
	Incorrect output to actuators	Detected by end-around test and rectified (NH)
	Incorrect interpretation of sensor data	Discrepancy detected between the two sensors; correct information determined (NH)
	Falsely conveys door all clear	Possible unauthorized access to facility (no response)
	Falsely conveys door warning signal	No access to facility (NH)

Appendix C: Failure Modes Effect and Criticality Analysis

C.1: Fail-Operate FMECA

Component	Failure Mode	Failure Effect	Mishap Severity	Failure Probability
Temperature & Humidity Sensor	Temperature reads low	Temperature falsely increased resulting in possible unchecked growth of agent (no response)	III	C
	Temperature reads high	Temperature falsely decreased resulting in possible mass death of agent (no response)	IV	C
	Humidity reads low	Humidity falsely increased resulting in possible unchecked growth of agent (no response)	III	C
	Humidity reads high	Humidity falsely decreased resulting in possible mass death of agent (no response)	IV	C
Heater	Fail on	Possible unchecked growth of agent (no response)	III	E
	Fail off	Possible mass death of agent (no response)	IV	E
Fan In/Out	Fail on In	Possible unchecked growth of agent (no response)	III	D
	Fail on Out	Possible mass death of agent (no response)	IV	D
	Fail off In	Possible mass death of agent (no response)	IV	D
	Fail off Out	Possible unchecked growth of agent (no response)	III	D
Power Supply	Short power outage	Possible unchecked growth or mass death of agent (no response) Access door locked (NH)	III	C
	Long power outage	Possible unchecked growth or mass death of agent (no response) Access door locked (NH)	III	C
Door Controls	Fail unlocked	Possible unauthorized access to facility (no response)	I	B
	Fail locked	No access to facility (NH)		C
Population control mechanism gate	Fail open	Mass death of agent (no response)	IV	B
	Fail closed	Possible unchecked growth of agent (no response)	III	B
CPU	Memory failure	Possible unchecked growth or mass death of agent (no response)	III	D
	Incorrect output to actuators	Possible unchecked growth or mass death of agent (no response)	III	D
	Incorrect interpretation of sensor data	Possible unchecked growth or mass death of agent (no response)	III	D
	Falsely conveys door all clear	Possible unauthorized access to facility (no response)	I	D
	Falsely conveys door warning signal	No access to facility (NH)		

C.2: Fail-Operate FMECA

Component	Failure Mode	Failure Effect	Mishap Severity	Failure Probability
Temperature & Humidity Sensor	Temperature reads low Temperature reads high Humidity reads low Humidity reads high	Redundant sensor corrects failure (NH) Redundant sensor corrects failure (NH) Redundant sensor corrects failure (NH) Redundant sensor corrects failure (NH)		
Heater	Fail on Fail off	Wrap-around test catches failure and population control mechanism is used to kill the agent and move the system to a safe state Wrap-around test catches failure and population control mechanism is used to kill the agent and move the system to a safe state	IV IV	E E
Fan In/Out	Fail on In Fail on Out Fail off In Fail off Out	Wrap-around test catches failure and power is disconnected. Redundant fan corrects failure (NH) Wrap-around test catches failure and power is disconnected. Redundant fan corrects failure (NH) Wrap-around test catches failure. Redundant fan corrects failure (NH) Wrap-around test catches failure. Redundant fan corrects failure (NH)		
Power Supply	Short power outage Long power outage	Back-up power supply is activated (NH) Back-up power supply is activated (NH)		
Door Controls	Fail unlocked Fail locked	Possible unauthorized access to facility (no response) No access to facility (NH)	I	D
Population control mechanism gate	Fail open Fail closed	Mass death of agent (no response) Possible unchecked growth of agent (no response)	IV III	D D
CPU	Memory failure Incorrect output to actuators	Detected by memory test, failed locations isolated (NH) Detected by end-around test and rectified (NH)		

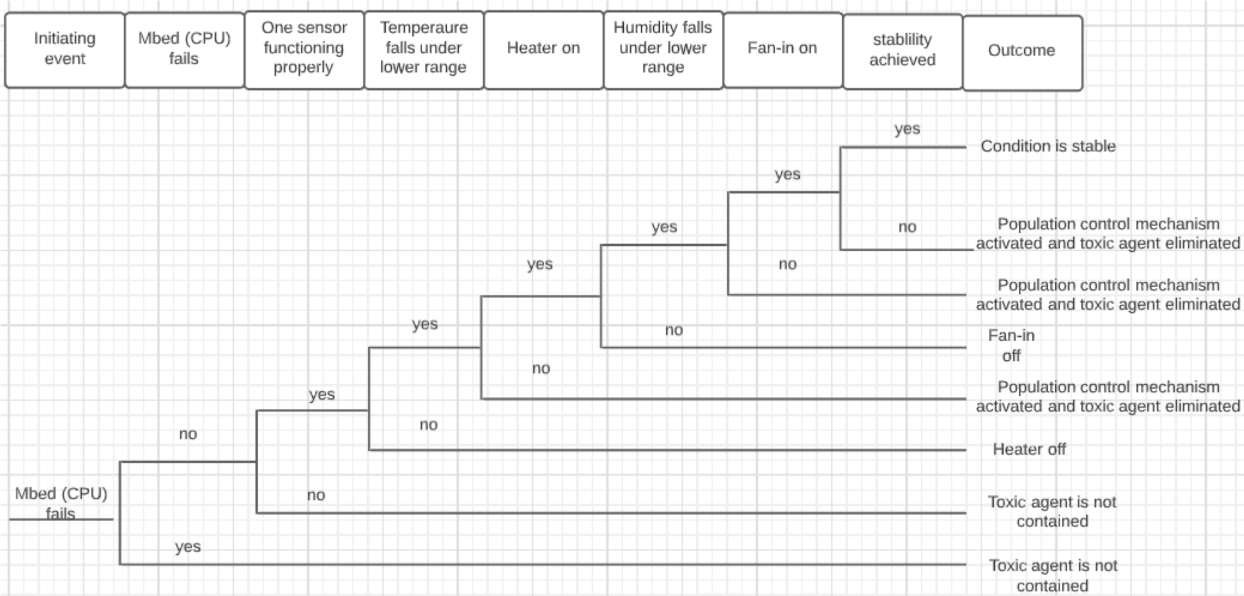
	Incorrect interpretation of sensor data Falsely conveys door all clear Falsely conveys door warning signal	Discrepancy detected between the two sensors; correct information determined (NH) Possible unauthorized access to facility (no response) No access to facility (NH)	I	D

Appendix D: Failure Modes and Effects Testing

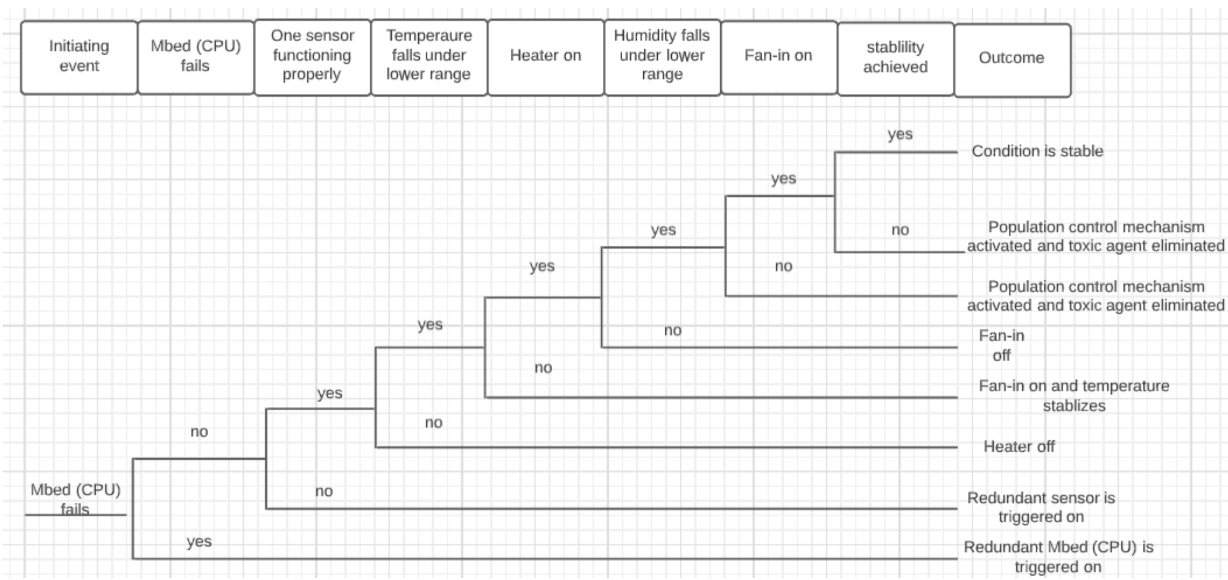
Component	Failure Mode	Failure Simulation Test	Result
Temperature & Humidity Sensor	Temperature reads low	Short one sensor’s temperature output to GND	TBD
	Temperature reads high	Short one sensor’s temperature output to VCC	TBD
	Humidity reads low	Short one sensor’s humidity output to GND	TBD
	Humidity reads high	Short one sensor’s humidity output to VCC	TBD
Heater	Fail on	Apply VCC to the resistor input	TBD
	Fail off	Disconnect power from resistor	TBD
Fan In/Out	Fail on In	Short input to VCC	TBD
	Fail on Out	Short input to VCC	TBD
	Fail off In	Disconnect power from fan	TBD
	Fail off Out	Disconnect power from fan	TBD
Power Supply	Short power outage	Temporarily disconnect main power supply	TBD
	Long power outage	Disconnect main power supply	TBD
CPU	Memory failure	Force a flag to the memory test using software	TBD
	Incorrect output to actuators	Externally fix output to actuators	TBD
	Incorrect interpretation of sensor data	Set sensor data input to an incorrect value	TBD
	Falsely conveys door warning signal	Disconnect power from door LED and induce a failure that would lead to a warning signal	TBD

Appendix E: Event Tree Analysis

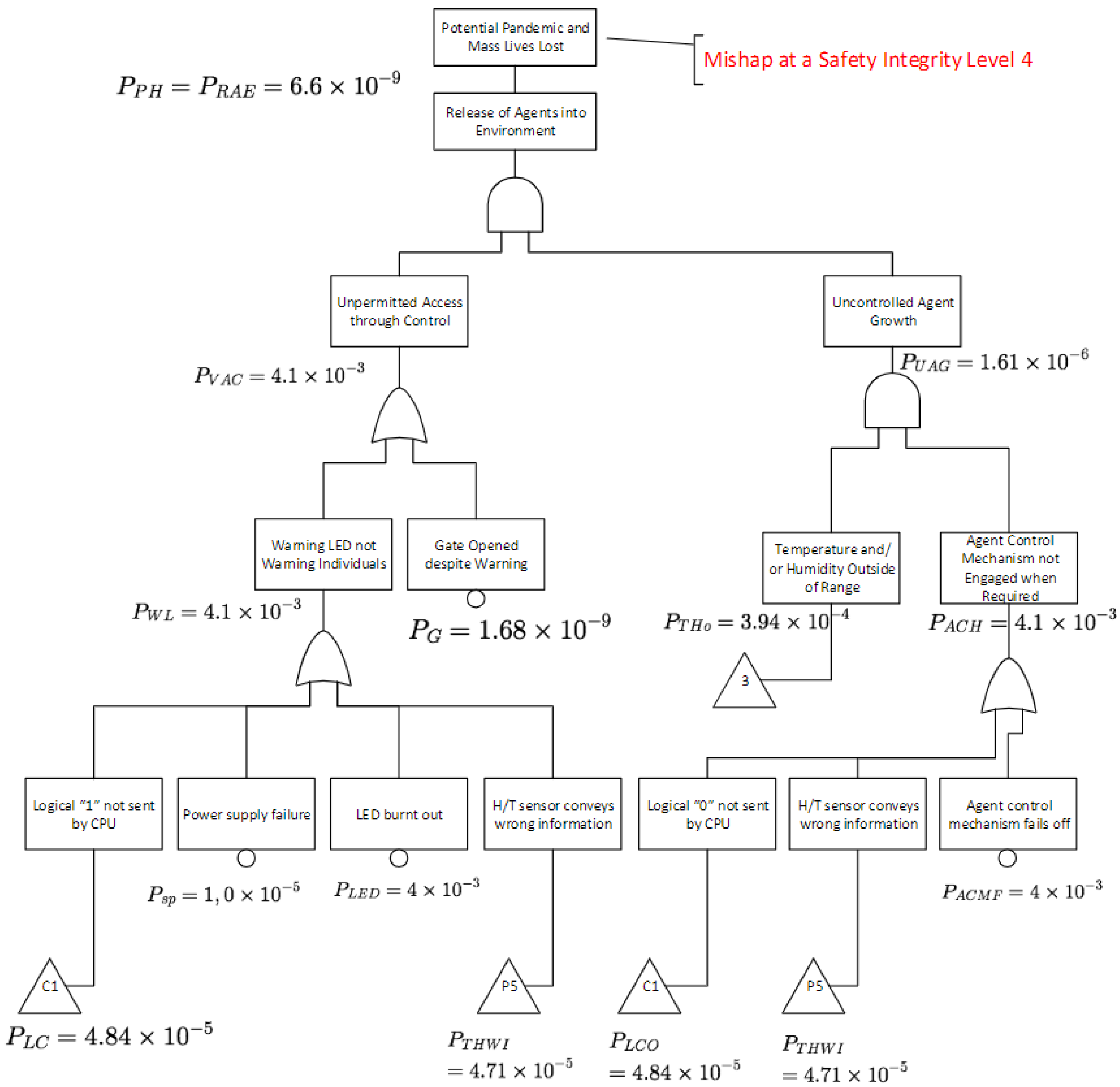
E.1: Simplex ETA



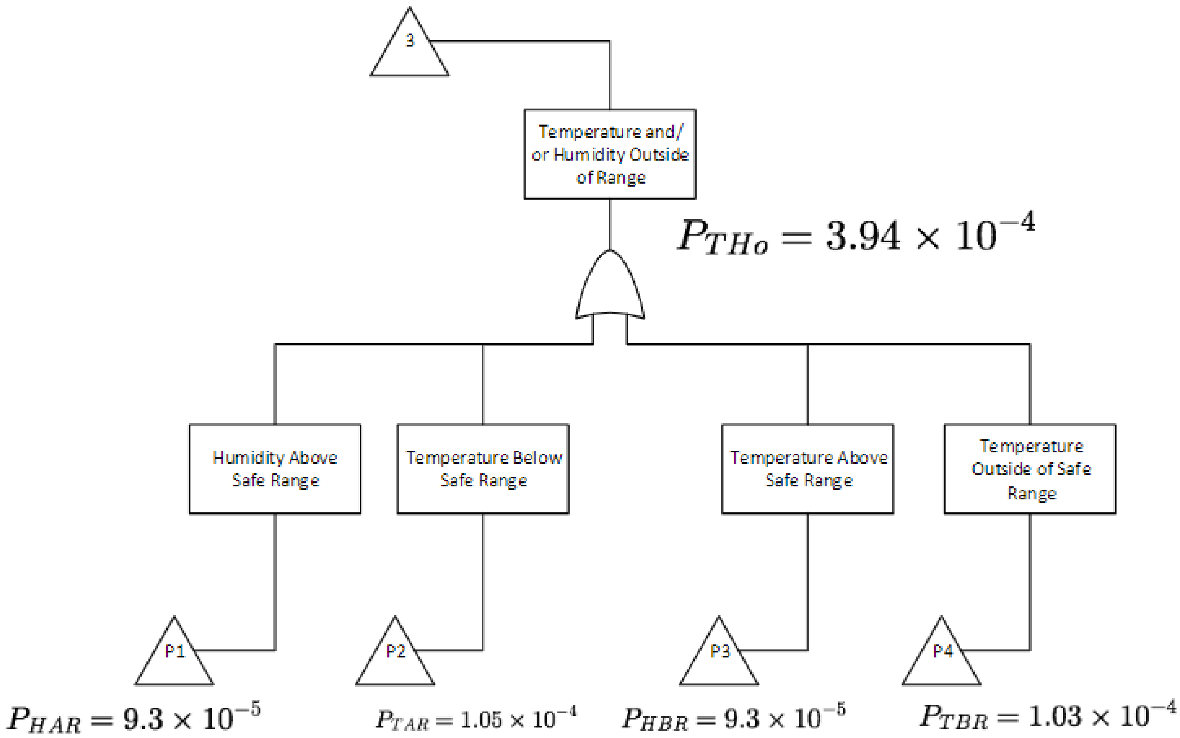
E.2: Fail-Operate ETA

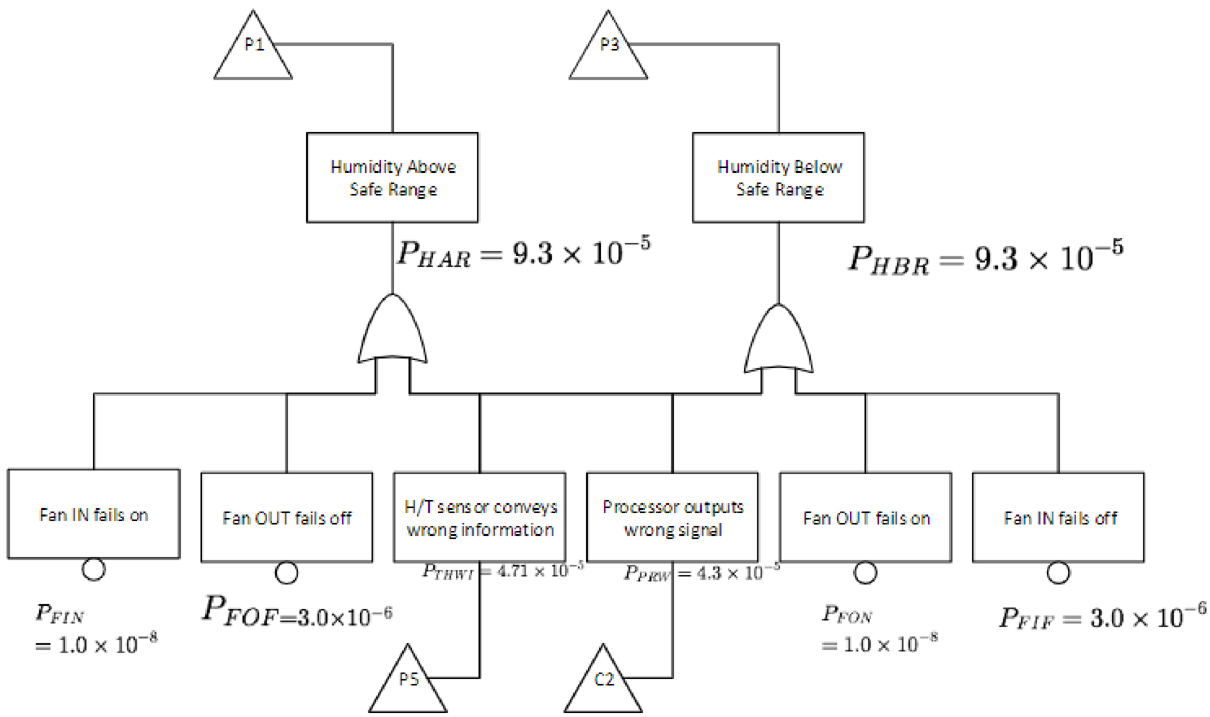


F.1: Simplex RA

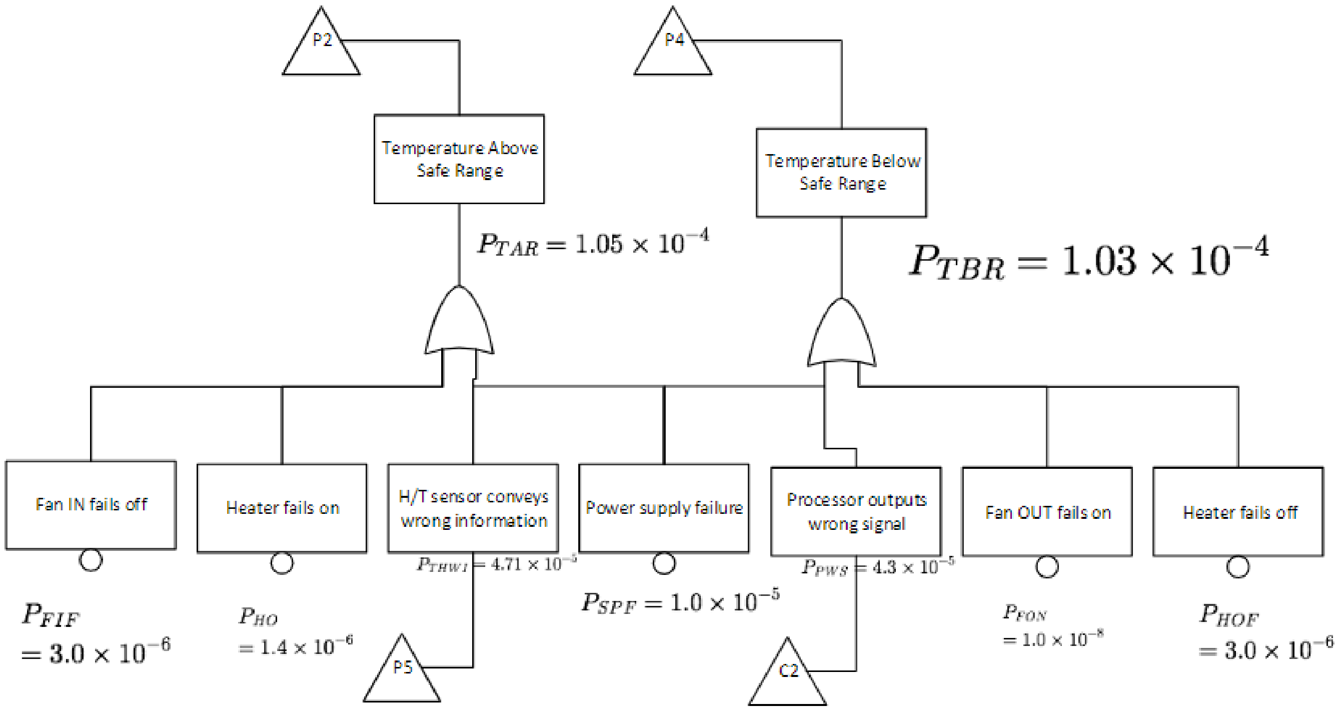


F.1: Simplex RA (Continued)

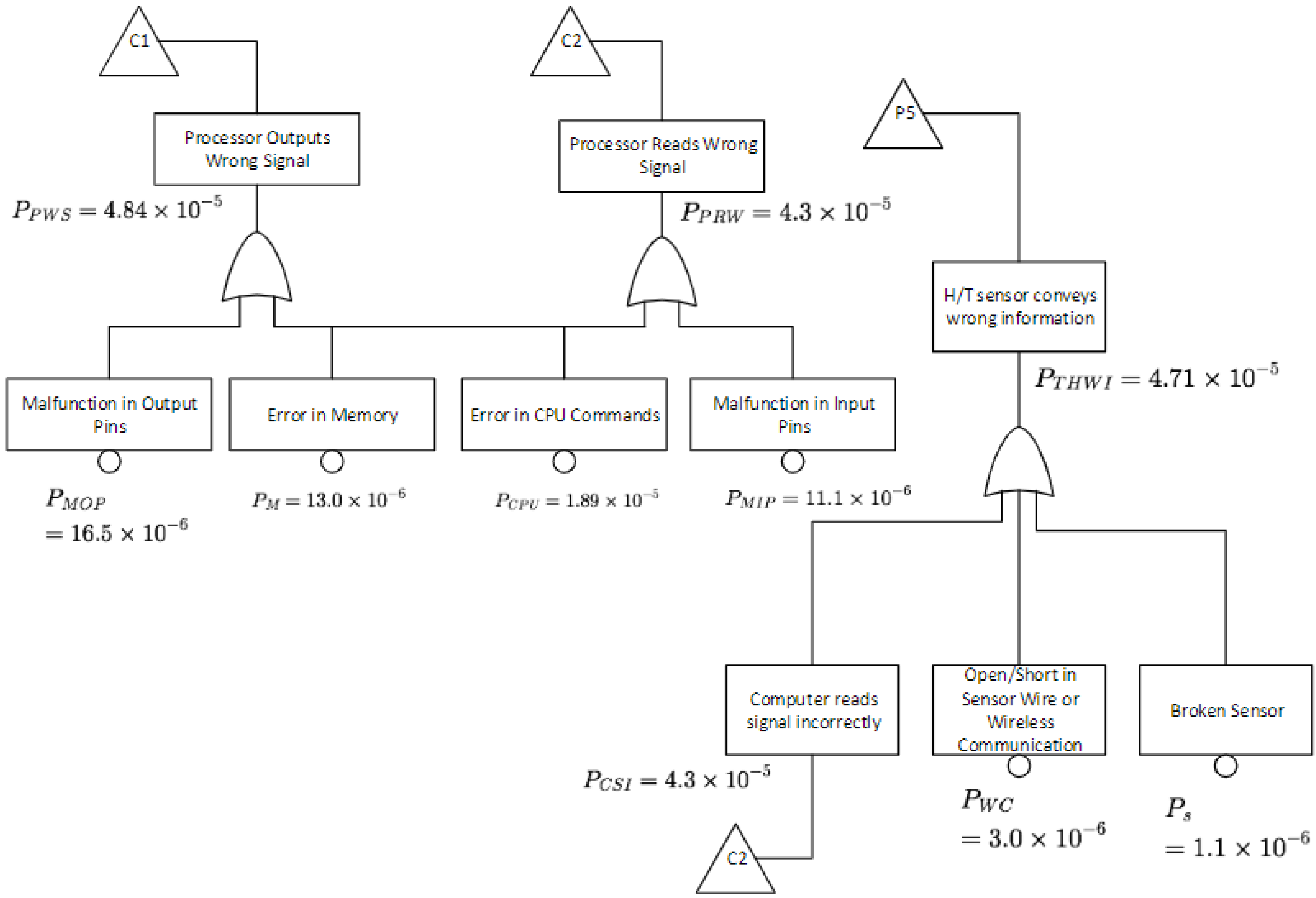




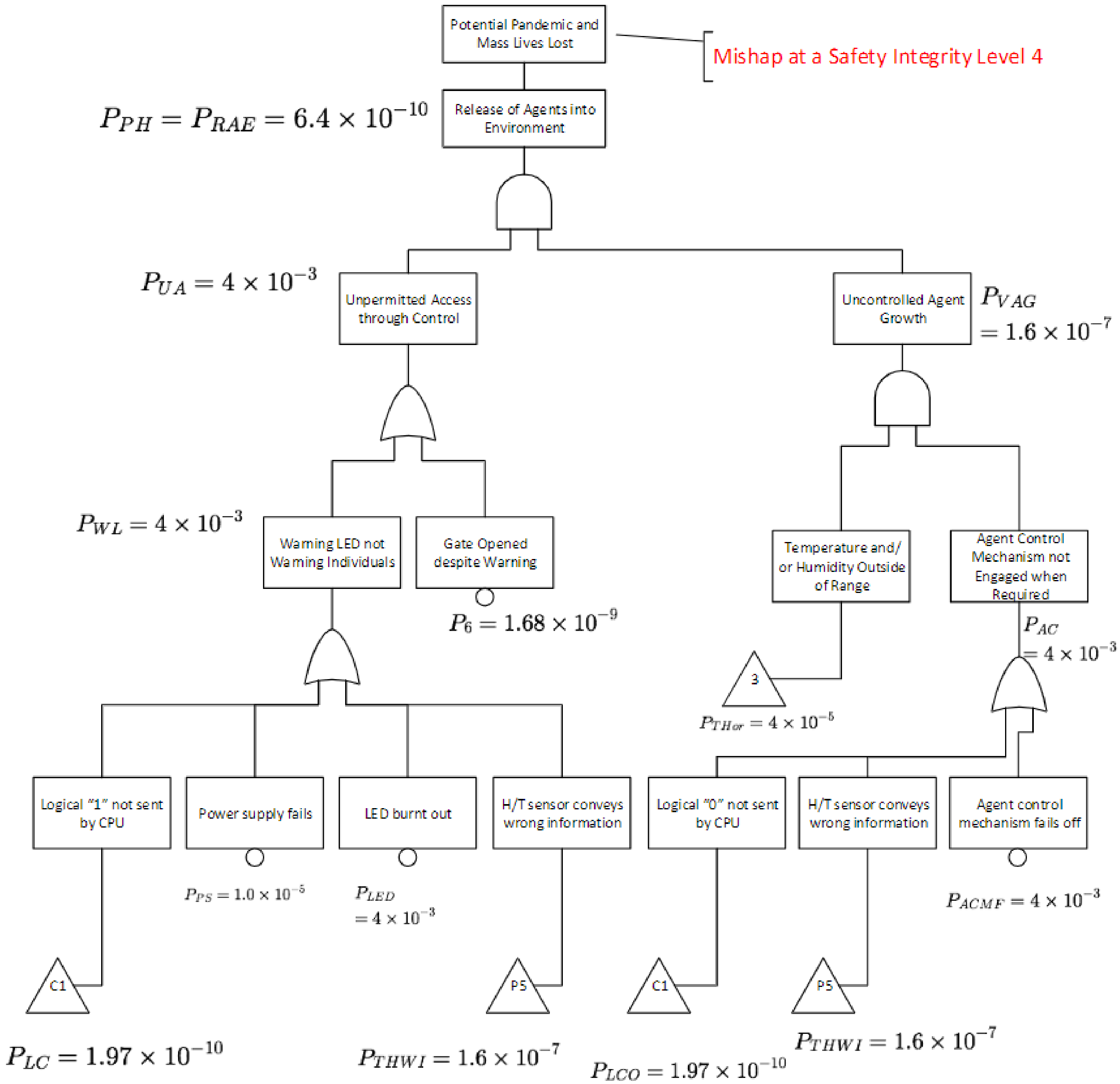
F.1: Simplex RA (Continued)



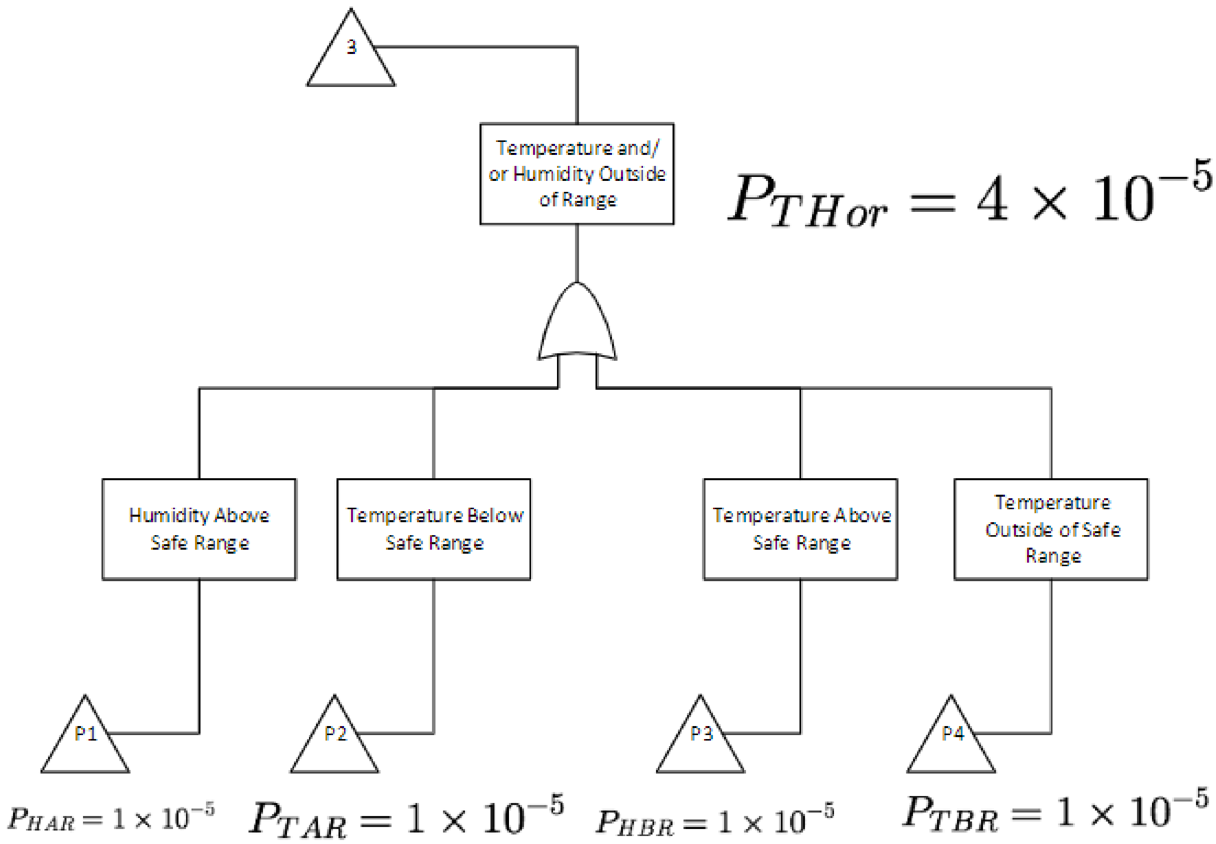
F.1: Simplex RA (Continued)



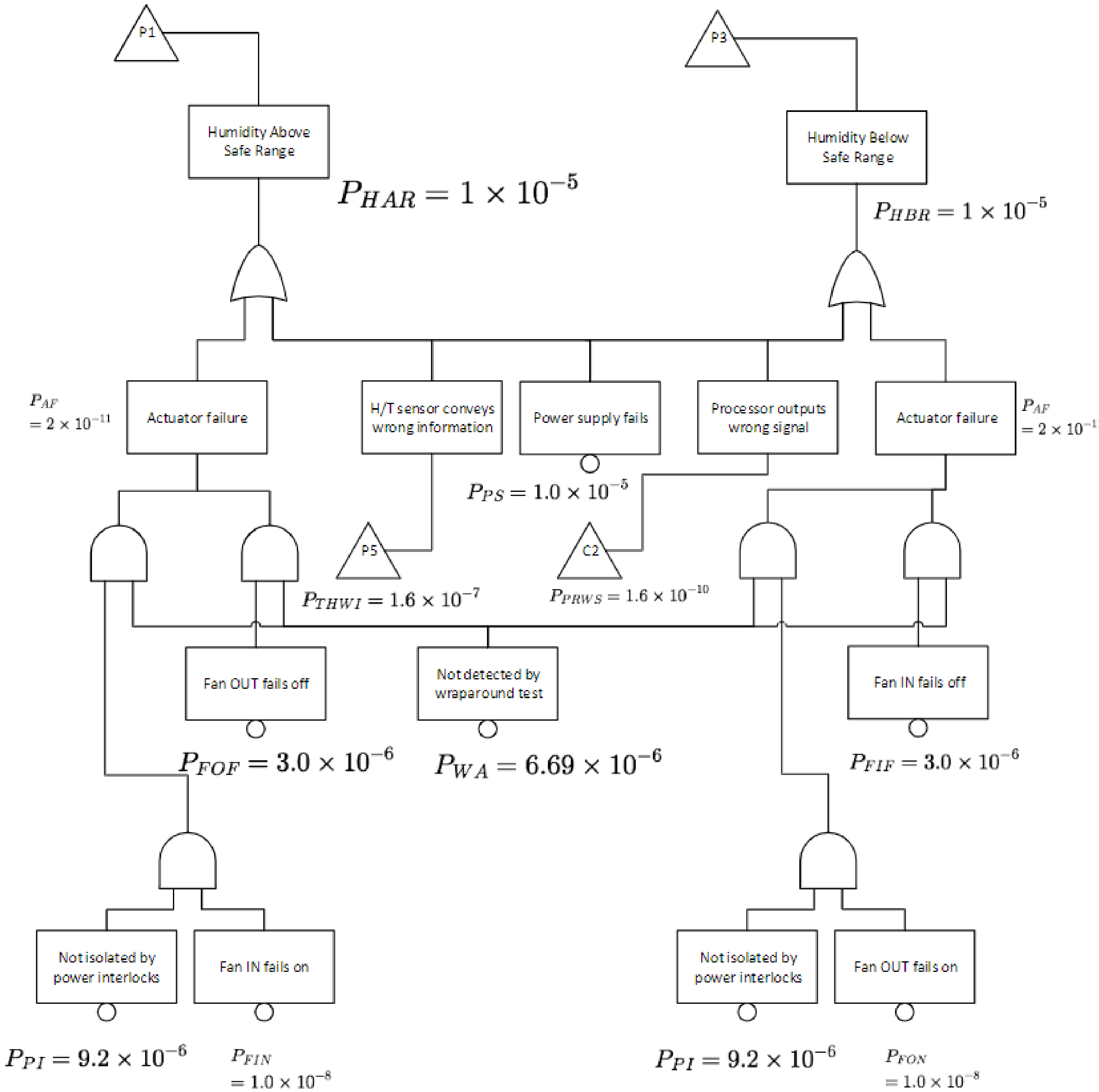
F.2: Fail-Operate RA



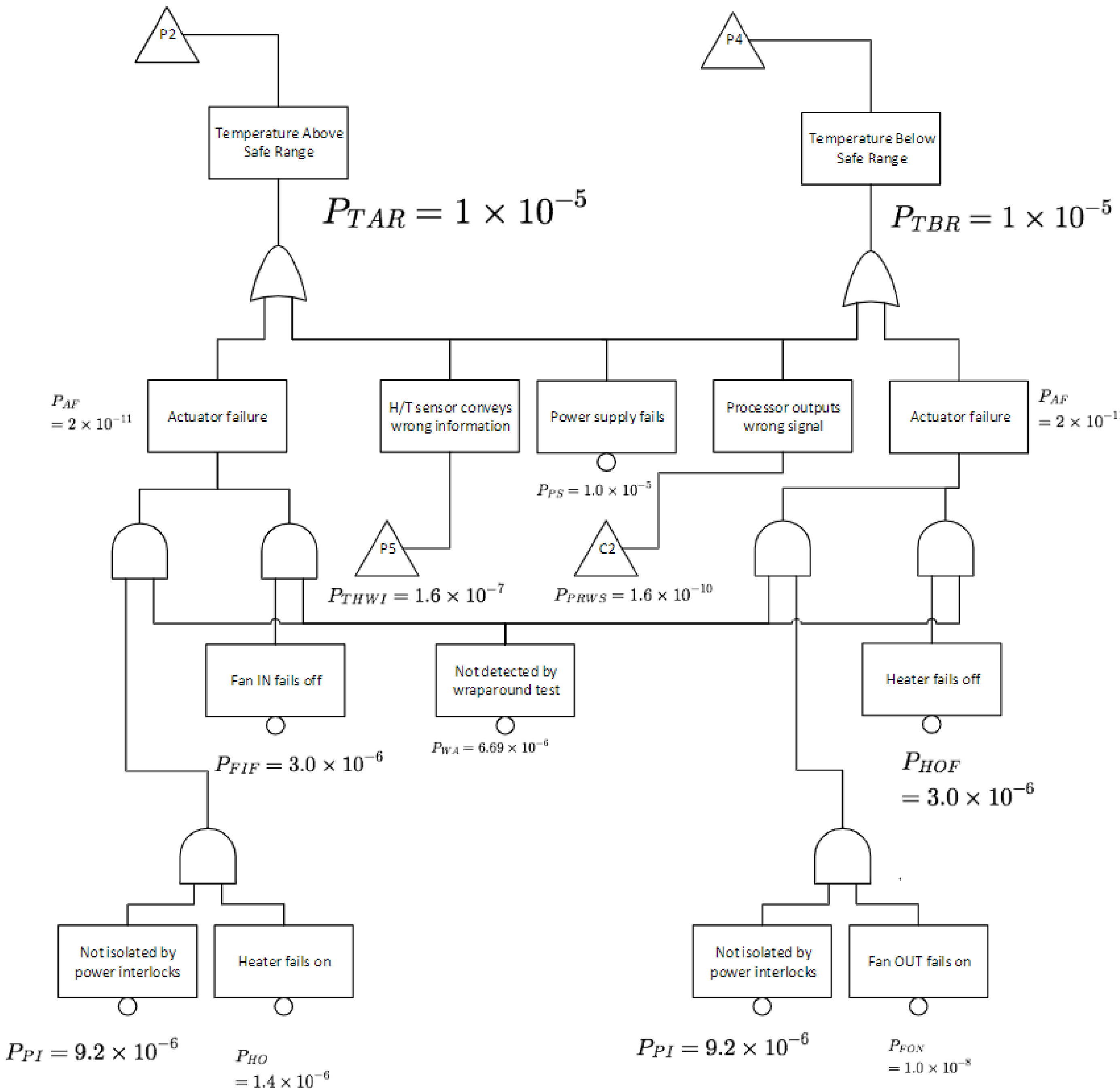
F.2: Fail-Operate RA (Continued)



F.2: Fail-Operate RA (Continued)



F.2: Fail-Operate RA (Continued)



F.2: Fail-Operate RA (Continued)