Energy Efficient House Control System

Francis Pollock: 40618059

SET10112 Formal Approaches to Software Engineering

Abstract. A detailed specification and analysis of ADA-built control system for an energy-efficient home. The system is made up of four main subsystems: Heating Control, Exterior Control, Appliances Control, and Carbon Monitoring System. Each subsystem is contained in its own package, adhering to good coding standards and Object-Oriented Programming. SPARK is implemented for formal proofing, enhancing the system's reliability. The safety analysis details the process of finding hazards and risk leading to the development of a safety case and manual, addressing potential hazards and risks associated with the system. Despite these efforts made through the specification, some aspects that could have been beneficial to the system were not included, such as a system for monitoring individual sections or rooms of the house. Future iterations could benefit from implementing such features to further optimize energy usage and user comfort. Overall, this paper provides a solid foundation for designing an energy-efficient home control system, with potential for further expansion and improvement.

1 Introduction

The focus of this paper is to detail an ADA built control system for an energy efficient home. The home system will be the main system with the following subsystems:

- Heating Control.
- Exterior Control (Windows and exterior doors).
- Appliances Control (Fridge and Oven).
- Carbon Monitoring System.

SPARK will be implemented for formal proofing and monitoring aspects of the system such as data flow, initialization and more.

Hazard, risk, and safety analysis was completed through a safety plan leading to the formation of a safety case and manual.

2 Controller Structure

To adhere to good coding standards, subsystems were split into their own packages allowing for code separation and good Object-Oriented Programming standards to be implemented into the system. The control structure is as follows:

- Heating System: A central heating system monitoring the temperature of the house, ensuring that it stays within the band of 17 to 19 degrees Celsius.

When the temperature reaches 17, the heating system is turned on. When the temperature reaches 19, the heating system is turned off.
- Exterior System: A simple control system that will unlock or lock doors dependent on the heating system being turned on or off. If the heating is on, the exterior system will lock, if the heating is otherwise off then the exterior system will remain unlocked.
- Appliances System: A control system that will ensure that when the Fridge is open/unlocked, then the Oven is closed/Locked and vice versa.
- Carbon Monitoring System: This system will make sure that the CO2 levels of the house never get above a certain margin, always ensuring safe levels. When the CO2 rises to a certain level, the air filter system will be toggled on, and when the air is clean the system will turn itself off.

The system does not contain global variables to help maintainability and readability. It does, however, contain numerous types and records that will be thoroughly detailed in section 3 for clarity (easier to understand and read), and for the passing of and creation of the values in the types and records.

3 Descriptions of Procedures and Functions

To detail each procedure clearly, the subsystems will be structured here, starting with heating control. All the following packages contain a function, however this function simply initializes and starts each package, so pre and post conditions were not included as they aren't necessary in assessing the package's strength of postconditions.

3.1 Heating Control

The heating control system is a key aspect of the system, not only to make sure that the temperature is at a level always needed but also to control the heating system and either turn it on or off and the moments that it's needed.

The house heating control system is defined as a record, containing the temperature and status of the heating system, with both temperature and status being established as types to contain the temperature's range (17-19) and the two possible states of the heating system (On, Off).

Likewise, there is a procedure for updating the record, if the heating system is off, then the temperature will by an amount set to 1 in this simulation, and if the heating system is on then the temperature will rise by 1 in this simulation. Then, with the new temperature there will be a check to see if the temperature is at either the heating system turn on or off temperatures, stating the status to the appropriate setting.

The procedure has the precondition that the temperature must be in the defined range of 17 to 19 degrees. The postcondition states that the status will be turned on, and the heating will rise, or the heating will be off, and the temperature will fall, there is also the unchanged scenarios in which the status of the heating is the same and the temperature has not changed also.

3.2 Exterior Control

The exterior control system will unlock or lock the exteriors based on the status of the heating system. This is done in two parts, from the main house package, a check is done to determine if the heating system is on, then the exterior package will be called to set the status of the exterior to locked, and if the heating system is off, then the exterior will be unlocked.

The exterior is defined as a record with a status based on a Type defined with the values of (Openable, Shut). There are two procedures for doing opposite things.

The first procedure is UpdateLocked, taking in the exterior and setting its status to shut. This has the precondition that the status is set currently to Openable, with the postcondition that the status is now shut. A simple but necessary procedure.

The second procedure is UpdateUnlocked, taking in the exterior again and setting the status to Openable. This has the precondition that the status is currently set to shut. Another simple but necessary procedure.

3.3 Appliances

The appliance package is designed to ensure that only one appliance at a time can be unlocked. This is done thought two types , locked containing the options of (Fridge, Oven) and unlocked containing the same.

The record will contain a statusUnlocked based on type Unlocked, and statusLocked based on type Locked. There is one procedure that will update both status' depending on which appliance is open.

There is a precondition that one of the appliances must be unlocked, and the postcondition that Unlocked is set to the opposite of Locked (So if oven is unlocked, then fridge is locked).

3.4 Carbon Monitoring System

The Carbon Monitoring System is essential in keeping the carbon levels of the house at a safe level. This is done by implementing two types, a type of carbon monitoring the level it is as, ranging from 0 to 8ppm and a type of AirConditioning that will have a mode of (Disabled, Activated).

There will be a record of this Monitoring system called CleanAir and it will contain carbs based on Carbon and status based on AirConditioning.

There will be a procedure that updates the values of the package as needed. The precondition is that the carbon values are in the valid range of carbon type, and that the status of the AirCon matches Disabled or Activated. The postcondition states that the carbon value will be in the carbon range, the status will be activated or disabled, and the carbon level will be adjusted based on the status of the air conditioning (decreased or increased carbon level).

3.5 House System

To complete the system, having information flow and records from each package passing on its information to the main package of house system was created. The house package will contain a record featuring types of the other packages and their records.

The house record includes heating (Temperature and Heating Status), exterior (Status of exterior), air (Carbon levels and air conditioning status), and appliances (Locked and unlocked appliance).

The package contains a procedure for updating each of the types contained in the record, ensuring that up-to-date information and dataflow is always enforced. The preconditions for this update procedure are that the temperature must be in the defined range, the heating status is set correctly, the exterior status is defined correctly, the appliances are set locked and unlocked correctly, the carbon levels are safe, and the air conditioning is set to a valid state,

The postcondition states that heating status will be updated, and whatever is returned will determine the exterior to be closed or open setting it as such, it will also use a safety invariant to determine that carbon is in the safety range of Carbon levels/ The inclusion of an invariant to ensure that the carbon levels are always safe was utilized as well as per the requirements.

3.6 Main

A simple main package is utilized to create a house system object and update the object until the program is terminated, with a predetermined delay (Set to 2 seconds for debugging) to simulate the system in action.

Moving on, proof of consistency will be analyzed to ensure that each of the previously described packages and their procedures are proved correct, at what level they reach, and an example proof done by hand.

4 Proof of Consistency

As demonstrated in the video, each of the major functional requirements and their procedures have proofs in the performed (and all passed at gold level). To demonstrate the major functional requirements proofs by hand, the carbon monoxide monitoring system will be demonstrated first:

For starters, the carbon monoxide monitoring system will need to ensure that the level of carbon monoxide does not get higher than 8ppm and the air conditioning is turned on to prevent it getting higher:

$$Precondition \Rightarrow (carbonLevel \in Carbon'Range) \wedge (ConditionerState \in AirCon)$$

With the precondition passed, and the procedure not being applied the following post condition will be true:

$$\begin{gathered}\textit{Post} \Rightarrow (\textit{This.carb in Carbon'Range}) \wedge \\ ((\textit{This.status} = \textit{Activated} \wedge \textit{This.carb} \leq \textit{Carbon'Last} - \textit{CarbonDecrease}) \vee \\ (\textit{This.status} = \textit{Disabled} \wedge \textit{This.carb} \leq \textit{Carbon'Last} + \textit{CarbonIncrease}))\end{gathered}$$

This proof will ensure that the carbon level is in the correct range, and that the carbon level will set the ConditionerState to an appropriate value of AirCon (Activated, Disabled) with the carbon level being increased or decreased according to the status of the aircon. This ensures that the carbon monoxide levels will always be kept at a healthy level and the air conditioning will be enabled exactly when it is needed to maintain that safety.

Each major function and their update have their pre and postconditions defined and shown in the video, but for the purposes of this document and the space limitation only the most important condition of the carbon levels is discussed and detailed.

5 Safety Plan

Although the proofs of the system passed at gold level, that does not mean the system is completely failure proof and risk adverse. To achieve such a level, or as close to that level as feasible, a safety plan needs to be conducted.

This includes a Hazard and Risk analysis with proposed mitigations for the system (in this case only two of the main subsystems will have this applied), with Hazard analysis being conducted via a Hazard log and Risk Evaluation to identify any risks.

To begin the safety plan, a hazard log will now be created with a further risk analysis on each hazard identified.

5.1 Hazard Log:

Hazard ID	Hazard	Hazard Description	Component
H1	Sensor Degradation	Exposure to high carbon monoxide levels due to system failure	Carbon Monitoring System
H2	Maintenance Issues	Lack of maintenance could lead to reduced accuracy of monitoring	Carbon Monitoring System
H3	Temperature Control Failure	Overheating/Lack of Heating due to temperature control malfunction	Heating Control System
H4	Sensor Malfunctions	Sensor malfunctions leading to inaccurate temperature readings	Heating Control System

With this hazard log (limited to only two components) defined, there will now be a risk evaluation using a criticality analysis and risk table.

5.2 Criticality Analysis

The criticality analysis includes defining certain aspects and contexts that the risk analysis will consider when determining the overall risk level associated with the hazard in question.

Likelihood: Assess the likelihood of the hazard occurring, considering context of system reliability, maintenance, and environmental conditions.

Consequence: Evaluate the potential consequences of hazard, aimed at health, safety, system functionality and environment.

With the above defined and context now applied, the next step is to construct a risk table that will assess the hazard come to an overall risk level that will be associated with hazard.

5.3 Risk Table

Hazard ID	Likelihood	Consequence	Severity	Risk Level
H1	Medium	High	High	High
H2	Low	High	Medium	Medium
H3	Low	High	Medium	Medium
H4	Medium	Medium	Medium	Medium

1. H1
   - Likelihood: Medium - There is a moderate likelihood that the temperature control system could fail from system malfunctions or disruptions.
   - Consequence: High – Failure of the temperature control system could lead to consequences of discomfort, health risk, property damage.
   - Severity: High – The combination of medium likelihood and high consequence weights the severity as high.
   - Risk Level: High – With all previous aspects weighted the overall risk is high.
2. H2
   - Likelihood: Low – This hazard is low as the regular maintenance and standard sensor design will keep it in standard safety practice.
   - Consequence: High – Although the likelihood is low, the consequence of it happening is high as incorrect readings from sensors could be catastrophic.
   - Severity: Medium – With low likelihood and high consequences, the severity of the medium.
   - Risk Level: Medium – With all previous aspects weighted the overall risk is medium.
3. H3
   - Likelihood: Low - The likelihood of carbon monoxide sensor degradation is considered low, with the assumption made that regular maintenance and calibration practices are employed as they should be.

- Consequence: High - Despite a low likelihood, sensor degradation could lead to inaccurate detection of carbon monoxide levels, posing health risks to occupants.
- Severity: Medium - The severity of sensor degradation is labeled as being moderate, balancing the low likelihood with the high consequence.
- Risk Level: Medium - With a low likelihood and moderate severity, the overall risk level is medium.

4. H4
    - Likelihood: Medium - There is a moderate likelihood of maintenance focused issues arising during the system’s lifetime, considering factors such as human error or lapses in maintenance schedules.
    - Consequence: High - Maintenance issues could lead to moderate consequences such as reduced system reliability or increased risk of component failure, potentially leading to carbon levels rising above where they should.
    - Severity: High – With medium likelihood and high consequence, the severity is deemed high.
    - Risk Level: High - With a moderate likelihood but high consequence, and severity, the overall risk level is assessed as high.

5.4 Mitigations Proposed

Hazard ID	Hazard	Mitigation(s) Proposed
H1	Sensor Degradation	Regular maintenance and calibration of carbon sensors, additional sensors installed, self-diagnostic system for errors.
H2	Maintenance Issues	Create comprehensive maintenance protocols with regular servicing.
H3	Temperature Control Failure	Regular maintenance and calibration of sensors, install multiple sensors over the house as backups, sensory self-diagnostic and issue reporting.
H4	Sensor Malfunctions	Schedule regular calibration and testing of the temperature sensors for accuracy and reliability testing, install additional sensors across the home.

5.5 Failure Analysis

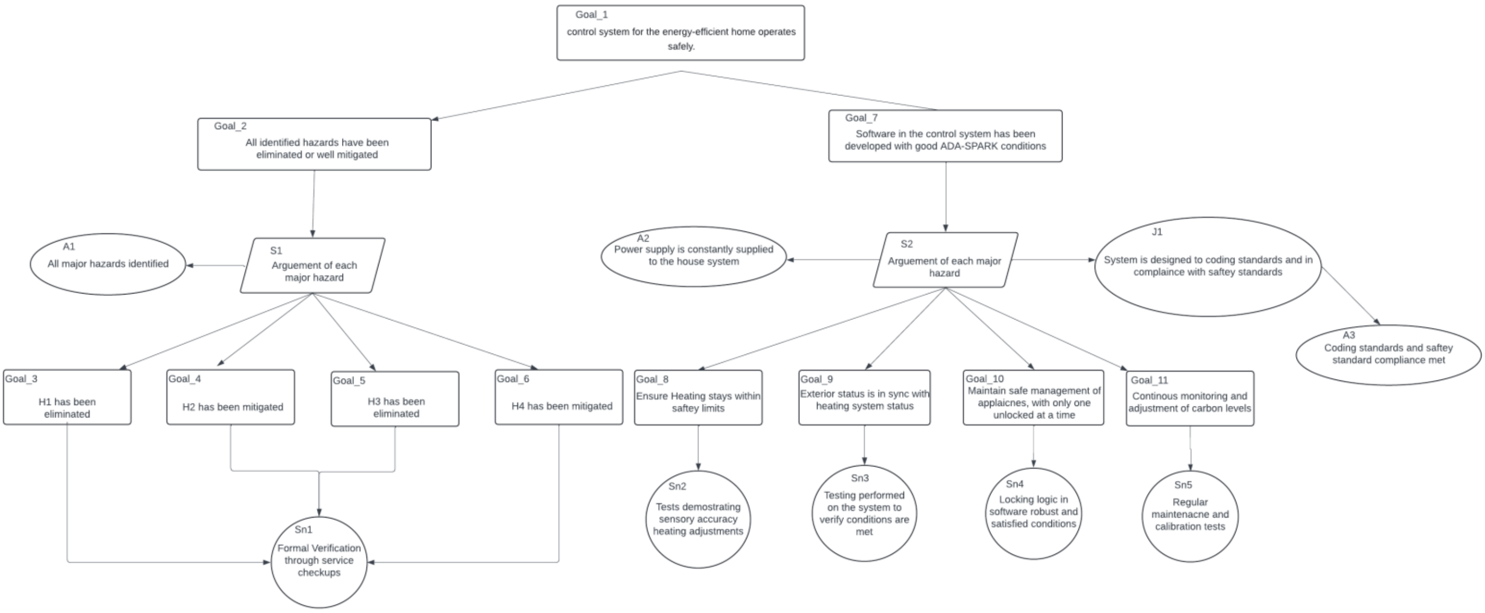
The following failure analysis will be performed using Software Failure Modes and Effects Analysis (SW)FMECA, using the three most severe risks:

Hazard	Failure Mode	Effect	Criticality
H1	Carbon monoxide sensors degrade over time, leading to inaccurate readings or failure to detect elevated carbon monoxide levels.	Failure to detect carbon monoxide buildup, leading to occupant health risk.	High – Health risks to occupants require immediate attention.
H3	Temperature Control System malfunctions, leading to heating system remaining on	Overheating, Increased energy consumption and cost, discomfort, heat related health issues, potential damage to property from excess heat.	High – Failure will lead to severe consequences impacting safety, property, and comfort.
H4	One or more temperature sensors fail to provide accurate readings.	Inaccurate readings could lead to discomfort in temperature, increased energy consumption and risk of equipment damage.	High – System performance and occupant comfort affected.

6 Safety Case and Safety Manual

To demonstrate safety case, the use of goal structuring notation (GSN) will be utilized.

6.1 GSN:


Goal_1
control system for the energy-efficient home operates safely.
Goal_2
All identified hazards have been eliminated or well mitigated
Goal_7
Software in the control system has been developed with good ADA-SPARK conditions
A1
All major hazards identified
S1
Arguement of each major hazard
A2
Power supply is constantly supplied to the house system
S2
Arguement of each major hazard
J1
System is designed to coding standards and in complaince with saftey standards
A3
Coding standards and saftey standard compliance met
Goal_3
H1 has been eliminated
Goal_4
H2 has been mitigated
Goal_5
H3 has been eliminated
Goal_6
H4 has been mitigated
Goal_8
Ensure Heating stays within saftey limits
Goal_9
Exterior status is in sync with heating system status
Goal_10
Maintain safe management of applaicnes, with only one unlocked at a time
Goal_11
Continous monitoring and adjustment of carbon levels
Sn1
Formal Verification through service checkups
Sn2
Tests demostrating sensory accuracy heating adjustments
Sn3
Testing performed on the system to verify conditions are met
Sn4
Locking logic in software robust and satisfied conditions
Sn5
Regular maintenacne and calibration tests

6.2 Safety Manual

A safety manual is an essential document for guiding the users and maintainers of any system, providing comprehensive details on proper operation, maintenance procedures, emergency responses, and safety precautions. Below is an outlined Safety Manual based on the energy-efficient ADA-controlled home system.

7 Safety Manual for Energy-Efficient Home System

7.1 Introduction

Purpose and Scope:
Ensure the safe use and maintenance of the Energy Efficient Control System for a Home. Covers all subsystems and their interactions.

7.2 System Overview

System Description:
The system is an energy efficient system that will keep the house temperature in a certain range, ensure that the while the heating is on, exteriors and windows are closed, make it so that only one appliance can be opened at a time, and monitor carbon levels, cleaning the air when they get too high.

Components:

- Heating System: Temperature monitoring and automatic heating.
- Exterior System: Automatic closing and locking of windows and exterior doors.
- Appliance System: Automatic locking and unlocking of the oven and fridge.
- Carbon System: Automatic monitoring of the carbon levels, with automatic air conditioning to clean the air.

7.3 Emergency Procedures

General Emergency Responses – See Failure Analysis for further detail:

Specific Subsystem Responses:
Heating Control Failures: Turn off the central heating, turn the main system off.
Exterior Lock Failure: Manually unlock a door/window, turn the main system off.
Appliance Failure: Turn off the main system, manually or lock as needed.

High CO2 Levels: turn the main system off and view air conditioning manual for instructions.

7.4 Maintenance and Troubleshooting

Routine Maintenance Schedule:
Main system should be checked up once a year for maintenance and updating.

Troubleshooting Guide:
In case of a system crash or shutdown, please restart the system. If it does not work, please contact support.

7.5 Safety Precautions

General Safety Warnings:
Please keep the system clean and up to date. Do not allow maintenance schedules to stop, contact support immediately in case of critical issue.

8 Conclusion

In conclusion, a detailed specification and analysis has been presented in this paper, providing a solid design of the ADA-built control system for an energy-efficient home. Through breaking down the system into the four main subsystems and describing their procedures and functions, we have outlined a structured approach to employ the system's reliability. Additionally, the integration of SPARK for formal proofing adds an extra layer of robustness to the system.

Despite the thoroughness of the specification, there are some shortcomings and aspects that could have been implemented but were not. The most notable is the lack of a subsystem that monitors individual sections or rooms of the house.

While the current design focuses on controlling the house, having the capability to monitor and control specific areas could potentially enhance both energy efficiency and user comfort. For example, adjusting heating and cooling based on occupancy levels in different rooms could lead to more optimized energy usage.

Although we have performed a comprehensive safety analysis and proposed mitigations, there is always a possibility of unforeseen risks or failures. Future iterations of this system could benefit from ongoing risk assessment and refinement of safety protocols to ensure continuous improvement and adaptation to changing conditions.

Overall, the paper provides a solid specification and detailing for an energy-efficient home control system, with room for expansion and improvement. By incorporating additional features such as individual room monitoring, the system can further enhance the functionality and effectiveness of energy efficiency.