

Software Architecture Document

Environment Monitoring and Analysis

Software

Author : CSCE742Project_Team3

Date : 07/01/2016

Version : 1.0

Team 3:

Ferguson, Harry S.

Gangala, Deepthi

Kalusani, Krishna Sindhuja

Kanapala, Allen J.

McCreary, Justin W.

Wodarczyk, Andrew K.

Table of Contents

1. Software Product Overview
2. Business Drivers
3. Quality Attributes
4. Architectural Views
 - a. Logical View
 - b. Process View
 - c. Development View
 - d. Physical/Deployment View
5. Use Cases
6. Utility Tree

Appendix

- I. Glossary

Software Product Overview:

Environment Monitoring and Analysis Software system is to be provided as a thin-client solution to homeowners who are interested in remote monitoring of status of various elements within the perimeters of their connected home(s). When an incident occurs, the system will have a fully automated decision-making process and ensure appropriate action is taken which does not harm the environment it is deployed in.

The system is expected to support integration with the following monitoring equipment, namely:

1. Cameras (supported types: Analog and IP)
2. Sensors (supported types: Optical, Proximity, Thermal and Chemical)
3. Networking devices (supported types: routers, modems and switches)
4. External Vendor managed reporting and notification infrastructure (SMTP server and SMS gateway, call to mobile gateway)
5. Data analytics for analyzing the observed incidents and broadcasting reports that are of two kinds:
 - a. Generic reports accessible to all users of this software system.
 - b. Specific reports relevant to the individual customers who have this equipment deployed at their sites.

The software product will mainly comprise of the following layers for handling data:

1. Data Collection Layer – Input Devices(Cameras/Sensors)
2. Data Translation Layer – Encoding/Compression software
3. Data Transfer Layer – SSH FTP of data stream to the FTP Servers hosted within the Firm's network
4. Data Processing Layer – Application Servers
5. Data Storage Layer - Databases
6. Data Notification Layer – SMTP Server/SMS/Call Gateway
7. Data Analysis Layer – COTS package deployed on servers
8. Data Presentation Layer – GUI for the end users (clients) to access encrypted data and reports. Special user interface for the installers to work onsite which is not available to any of the users within the end user category.

The following is an initial representation of the software product's implementation landscape obtained from the customer's project proposal documentation, an overview of the main components and their high level interactions is depicted below:

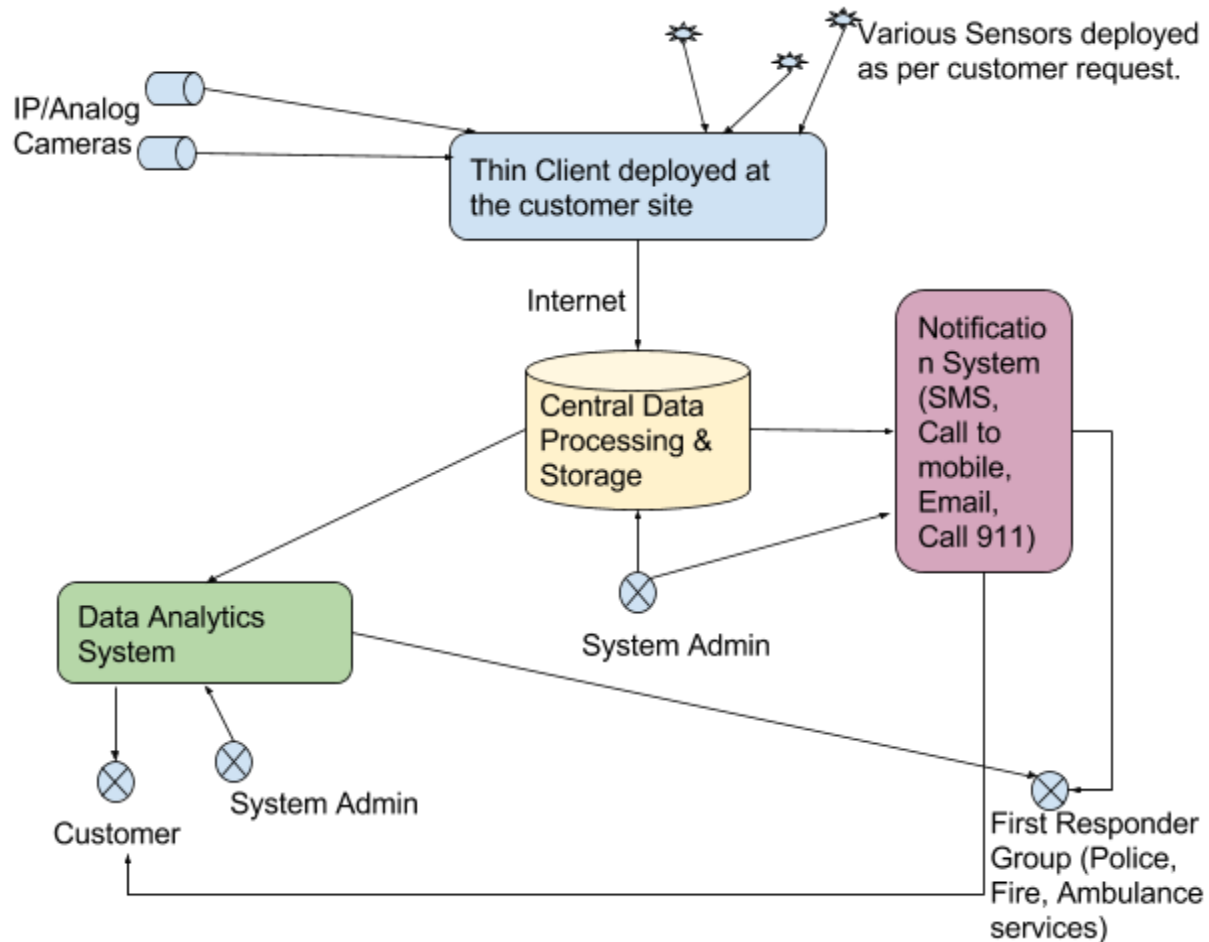


Figure 1: Initial overview of Software System provided by Customer

Camera: Send images / videos to the system, and can be panned and zoomed. Can record and save data received up to a set period of time.

Sensors: Various devices deployed at the customer's residence. Where and how many depends upon the size the residence as well as the wishes of the customer(s).

Thin Client: The main interface where the user can interact with the system. This is deployed to the site that handles the recording and monitoring of all devices for the system at the residence where the device is placed. Acts like an Interface Control Panel and allows them to activate/deactivate the security system.

Central Data Processing and Storage: The central processing unit communicates with the main security system to record data, keep track of the sensors, and send alerts depending on the type of emergency

Data Analytics System: analyzes observed incidents and broadcasts reports based upon what is found. These reports come in two forms: (1) Generic Reports accessible to all users of the

software system; (2) Specific reports relevant to the individual customers who have this equipment deployed at their sites.

Customer: The person(s) purchasing the security system, who will have access to their own system, and any information related to it.

System Admin: Person(s) in charge of handling the data coming in, and sending out Notifications based upon the type of emergency that is being received.

First Responder(s): Emergency services responding to the notification. What type of responder that will be sent (police, firemen, ambulance) will depend upon the type of emergency.

Remote User Access: Allows the user to access the thin Client (Central Processor) from a remote location through the appropriate device. This can include a laptop, PC, MAC, tablet, and a number of other mobile devices.

Socket I/O: Provides a direct encrypted communication to the thin client for security purposes.

Business Drivers:

The following are the list of business drivers that are identified from the customer's project proposal document:

1. The Firm aims to position themselves as the leading providers of software products and services with the lowest security monitoring costs for homeowners.
2. Another important goal is to be known as a creators of the most up to date software products by continuously integrating existing technologies so that the clients have the most technologically advanced solutions implemented at their residences which were previously not possible in a retail market environment.
3. The software is required to implement the highest form of security to ensure the customer's personal information and secured property related information remains highly confidential without any loss of data integrity. Goal is to use the latest industry standard of AES-encryption for securing the client's data.
4. The Firm aims to be known as the best technology integrators with society as the system is expected to communicate with the first responders within the first minute of any incident to handle all emergencies. The product's intent is to benefit the first responders from the analytics part of the software described in the next paragraph.
5. Improve the business processes within the organization to design relevant products and/or functionality to better serve the newly identified needs of the customer revealed through the analysis of historical customer data.
6. The Firm aims to gain a strong foothold in the retail market space initially with a single product with a limited set of features. The system is expected to be scalable to accommodate deployments for all sizes of homes and lots.

7. The system is also expected to be flexible to interoperate with any existing COTS/vendor based products for managing the notification and reporting software infrastructure. By being flexible, the Firm aims to lower the software manufacturing costs and will be able to pass on the savings to the end users and sustain a relatively high market share.
8. The overarching goal of the Firm is to provide software systems that create a safe living and operating environment for the occupants of homes of all sizes located anywhere within the United States which will help the Firm with large revenue inflows.

Quality Attributes:

The following are the list of top quality attributes the Firm is interested in achieving for this product as inferred within the project proposal documentation by the customer. Additional information revealed in subsequent discussions with the customer are also listed within this section.

1. High Availability of the software system.
2. High Performance for the notifications transaction.
3. Security.
4. Usability for the various categories of users:
 - a. End User
 - i. Customers of the Firm
 - b. Internal User
 - i. Installer
 - ii. System Administrator
5. Modifiability.
 - a. Scalability
 - b. Modularity

Architectural Views

The intent of this section is to provide the reader with a thorough understanding of the various aspects of the architecture implemented for the Environment Monitoring and Analysis system. This will help in understanding the Architect's view of how the system needs to function in order to ensure the specified quality attributes are fulfilled to the fullest extent possible.

Logical View:

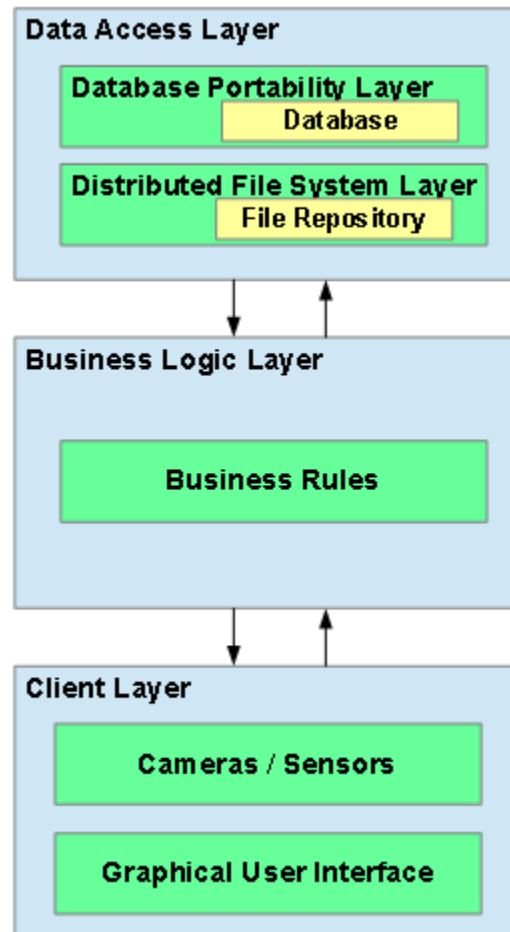


Figure 2: Strongly Layered Logical components of the software system

Element Catalog:

Each individual layer consists of multiple sub-components that are clearly described in the documentation related to the Physical View. They are strongly layered and hence communication has to be channeled through the indicated layers only.

Purpose of the Layers:

1. Database Portability Layer : Allows ability to switch database vendors. The database considered will be a relational database.
2. File Repository will be used to store video files.
3. Graphical User Interface supports:
 - a. external users (customers)
 - b. internal users (customer support & administrators) through a web portal.

Context Diagram:

A separate context diagram is not required at this stage as the components are logically grouped into a layered structure to enable ease of comprehension of the system's overall structure for all the necessary stakeholders.

These components are represented in sufficient detail within the Physical View.

Variability Guide:

The customer's project proposal did not indicate any product lines explicitly based on the current architecture, hence this section is not applicable as on date.

Rationale:

The current architecture view was designed to cater to the explicit mention of the QAR's within the project proposal document, namely:

1. Availability – This was also specified as a market differentiator for the client hence the databases were configured in a HA mode with secondary mirror which is acting as hot spare.
2. Performance – The customer expects the communication with the first responders to be within the first minute of any incident occurrence. This is taken care of by streaming the data frames over a high-bandwidth broadband connection from the customer site to the Firm's network where the notification services are configured to utilize the dedicated in-house gateways to communicate with the first responder teams and the customers within the specified time frame
3. Modifiability – The customer indicated in the project proposal that the customer's data will be analyzed to improvise on their product offerings which indicate the need to provide modifiability for existing services hence all components in the current architecture are designed to be modular in nature to facilitate the goal.

UML version for the Logical View.

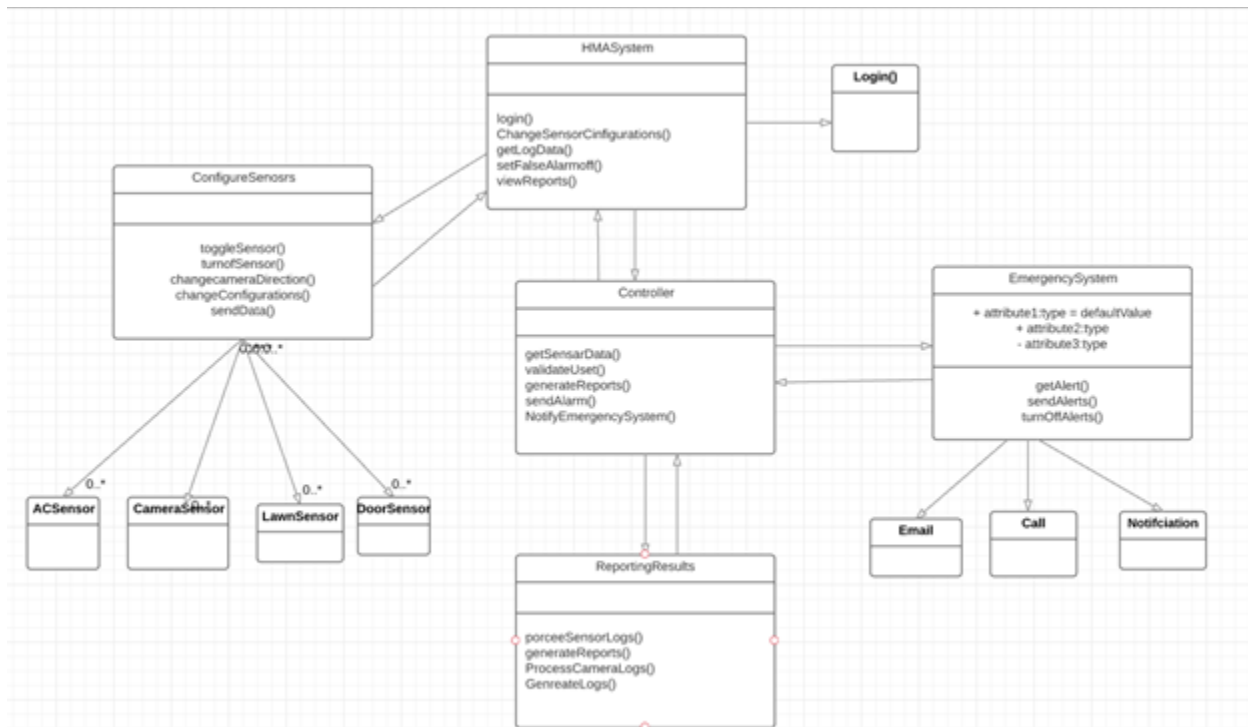


Figure 3: UML Diagram of the Logical View

EMSystem: This is a class is a center for providing the user login, interacting with central system and providing the sensor configuration details, and reporting details. This class provides the functionality for the user side functionality.

ConfigureSensor: This class is provides the functionality for configuring the sensors, controlling the sensors for user and central system. This has many subclass like ACSensor, CamareSensor,LawnSensor etc which extends the main class to support the similar functionality.

Controller: This is main Function of the software where all the defined functionality is implemented like accessing sensors, User details, Providing emergency service, interacting and storing the data, providing the reporting to users.

EmergencySystem: This class is responsible for generating the alerts to 911, emailing users, sending calls incase of emergency.

ReportingSystem: This class is responsible for processing the data generated by sensors and generate the reports.

Process View:

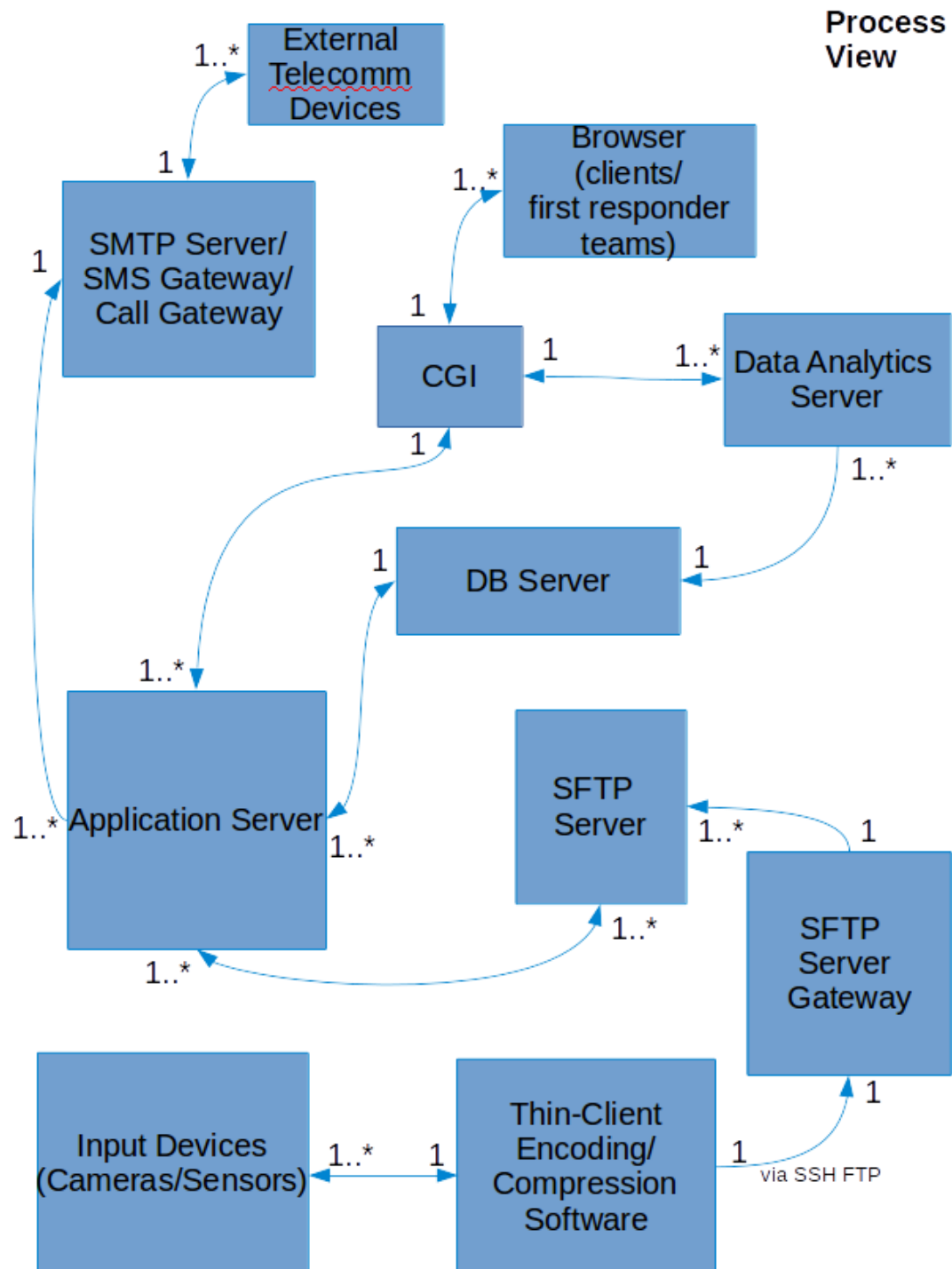



Figure 4 : Process View of the Interactions of the Software Components

Key:

All directed communication is represented by connectors with arrows.

Any interactions between the deployed components follow the below legend:

 Interactions between the various hardware and software components within the architecture.

 Physical Hardware/Software component within the architecture of the software system

Element Catalog:

Each individual hardware/software component may have one or more instances, which dictate the number of processes that can be instantiated and processed simultaneously.

External Telecomm Devices: End user devices. Eg: Mobile Phones, Tablets etc.

Browser (clients/first responder teams): Web Browsers on the client/first responder team's computers.

SMTP Server / SMS Gateway / Call Gateway: Gateways for routing the calls to the telecomm devices.

Data Analytics Server: Any COTS package chosen by the customer to analyze the data.

CGI: Common Gateway Interface to serve pages to the user requests based on the nature of their requests.

DB Server: Used to store all the processed information related to the data received from the client networks. Its also includes address references to the actual video files associated with a specific customer that are stored on the FTP servers.

Application Server:

SFTP Server: FTP server that stores all the client specific data within the Firm's internal network.

SFTP Server Gateway : This is used for load balancing the incoming data requests to the various FTP servers within the Firm's internal network.

Thin-Client : Consists of an installable on the local PC at the remote site which is connected to a broadband internet connection. This aids in collection of data, encoding / compressing it and transmitting it back to the FTP servers via SSH FTP protocol.

Input Devices (Cameras / Sensors): Depending on the customers need, there can be various types of cameras and sensors deployed at the remote site to collect the information related to the environment.

Context Diagram:

A separate context diagram is not required at this stage as the components are logically grouped into a layered structure to enable ease of comprehension of the system's overall structure for all the necessary stakeholders.

These components are represented in sufficient detail within the Physical View.

Variability Guide:

The customer's project proposal did not indicate any product lines explicitly based on the current architecture, hence this section is not applicable as on date.

Rationale:

The current architecture view was designed to cater to the explicit mention of the QAR's within the project proposal document, namely:

1. Availability – This was also specified as a market differentiator for the client hence the databases were configured in a HA mode with secondary mirror which is acting as hot spare.
2. Performance – The customer expects the communication with the first responders to be within the first minute of any incident occurrence. This is taken care of by streaming the data frames over a high-bandwidth broadband connection from the customer site to the Firm's network where the notification services are configured to utilize the dedicated in-house gateways to communicate with the first responder teams and the customers within the specified time frame
3. Modifiability – The customer indicated in the project proposal that the customer's data will be analyzed to improvise on their product offerings which indicate the need to provide modifiability for existing services hence all components in the current architecture are designed to be modular in nature to facilitate the goal.

UML version for the Process View.

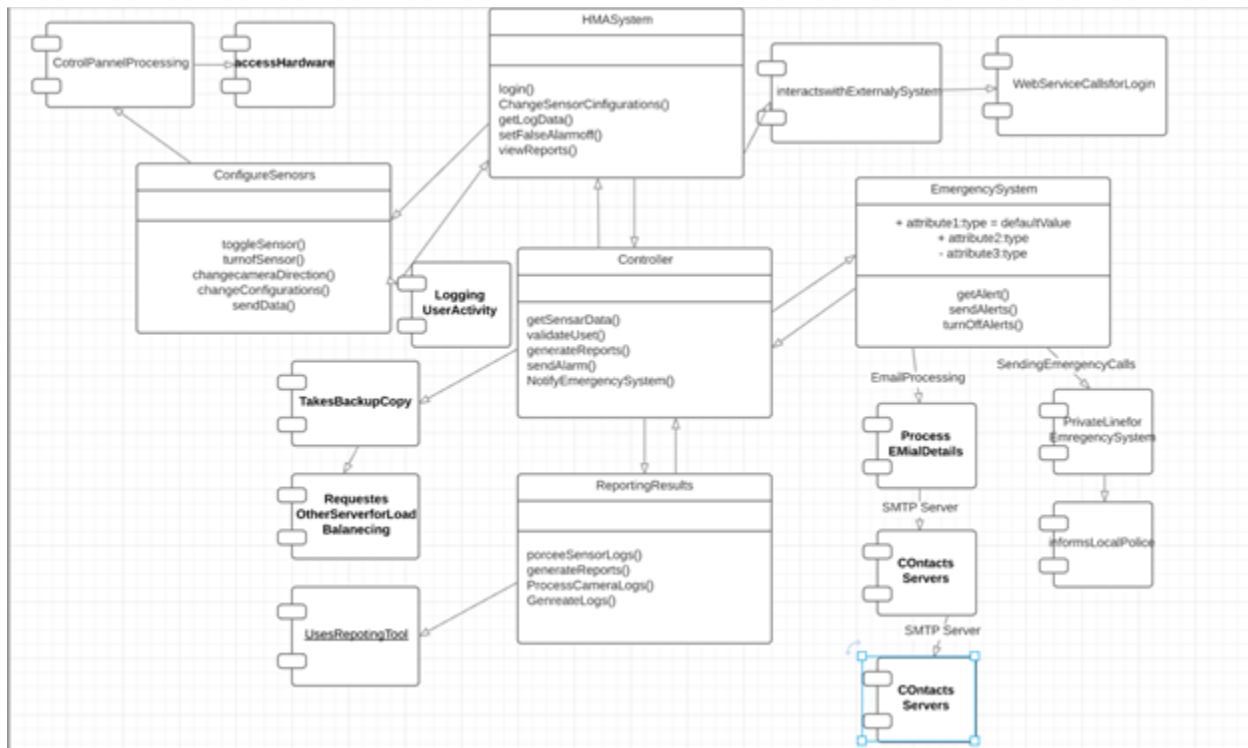


Figure 5: UML Diagram of the Process View

The process view UML diagram specifies the logging mechanism the system uses, the kind of servers used for the generating the alerts and how the load balancing is performed with the backup server.

Development/Implementation View:

Implementation View

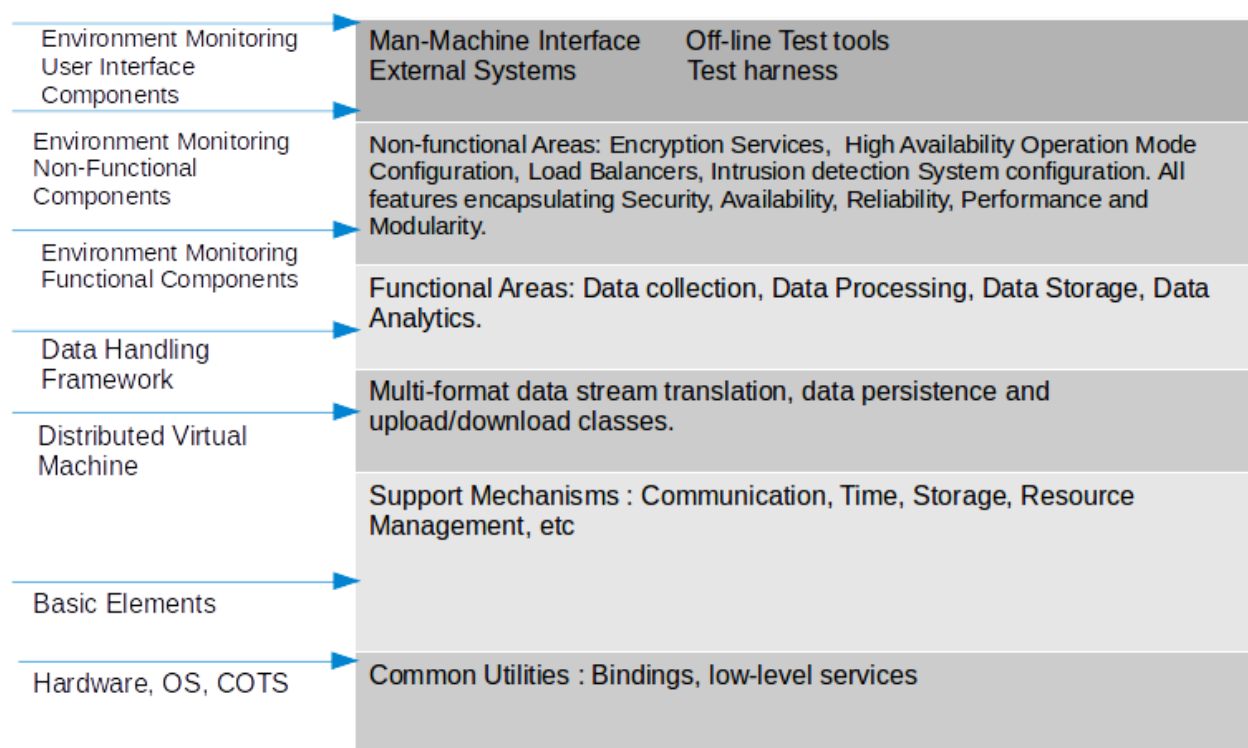




Figure 6: Layered view of work distribution for the teams

Key:

Any interactions between the deployed components follow the below legend:

 Indicator for the encapsulated services that are available to the layer described next to it on the right.



 Logical Grouping of the development work that can be used to plan for resource allocation and work planning by the Project Manager.

Element Catalog:

Each individual layer consists of multiple components that can be developed and implemented by a specific team. Each layer can be developed independently with the help of stubs by geographically diverse development teams.

Context Diagram:

A separate context diagram is not required at this stage as the components are logically grouped into a layered structure to enable ease of comprehension of the system's overall work breakdown structure for all the necessary stakeholders.

These components are represented in sufficient detail within the Physical View and their interactions are described in the Process View.

Variability Guide:

The customer's project proposal did not indicate any product lines explicitly based on the current architecture, hence this section is not applicable as on date.

Rationale:

The current architecture view was designed to cater to the explicit mention of the QAR's within the project proposal document, namely:

1. Availability – This was also specified as a market differentiator for the client hence the databases were configured in a HA mode with secondary mirror which is acting as hot spare.
2. Performance – The customer expects the communication with the first responders to be within the first minute of any incident occurrence. This is taken care of by streaming the data frames over a high-bandwidth broadband connection from the customer site to the Firm's network where the notification services are configured to utilize the dedicated in-house gateways to communicate with the first responder teams and the customers within the specified time frame
3. Modifiability – The customer indicated in the project proposal that the customer's data will be analyzed to improvise on their product offerings which indicate the need to provide modifiability for existing services hence all components in the current architecture are designed to be modular in nature to facilitate the goal.

Physical/Deployment View:

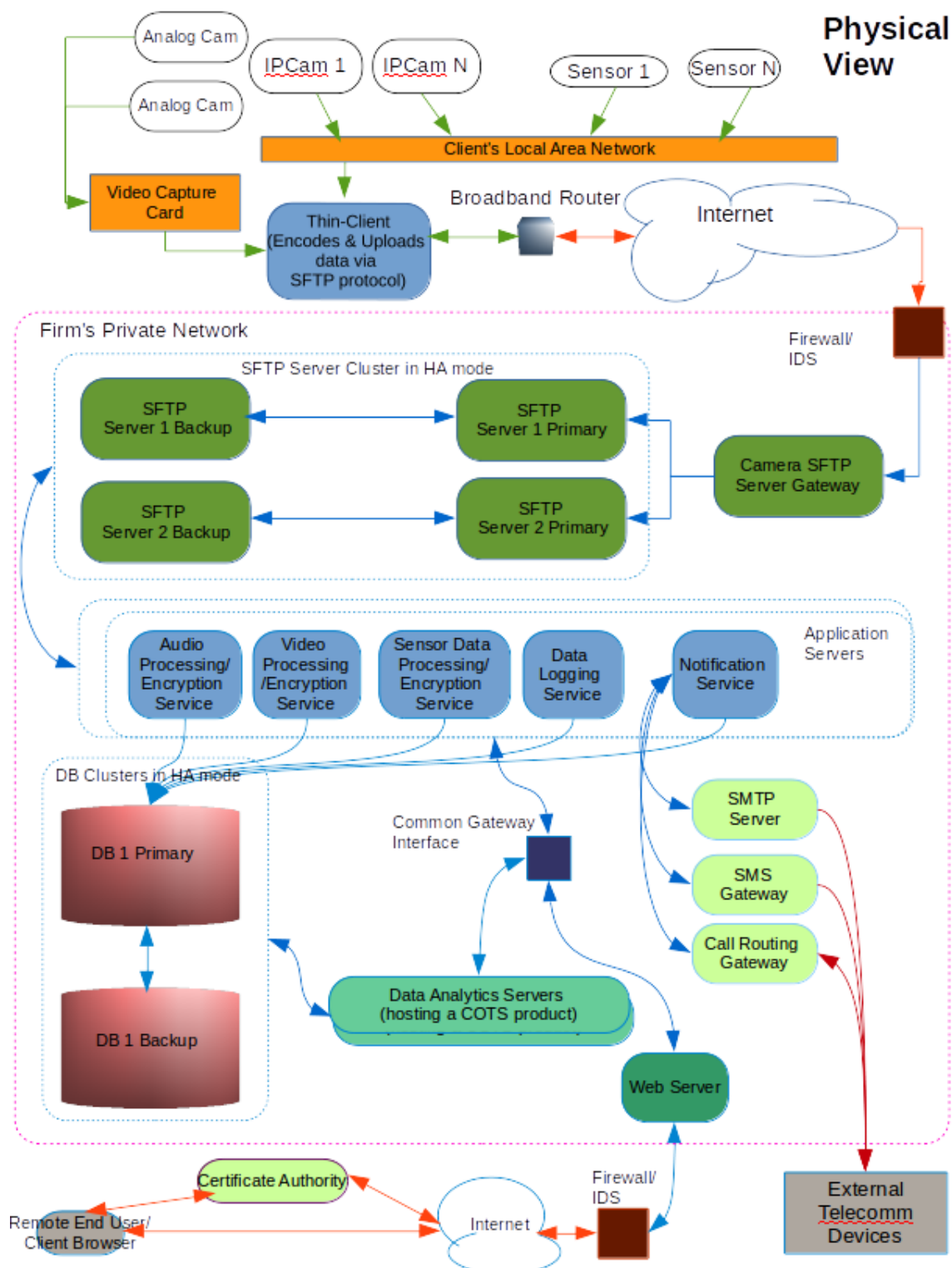
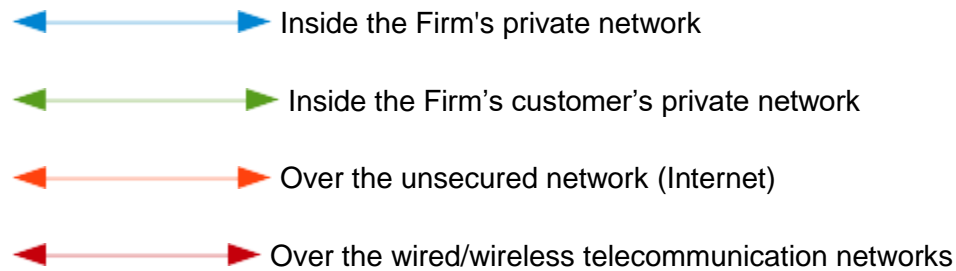


Figure 7 : Deployment View of software implementation

Key:

All directed communication is represented by connectors with arrows.

Any interactions between the deployed components follow the below legend:



Element Catalog:

IP Cam : IP Camera used for video/audio data collection

Analog Cam: Analog Camera used for video collection along with a separate microphone attached to it.

DB : Database used for storing the pointers to the processed/encrypted video/audio/sensor/log/notification data items.

Sensor : All supported types of sensors as per the customer project proposal documentation are represented with a generic description within this view for lack of space to represent all individual types.

Context Diagram:

A separate context diagram is not required at this stage as the system over view is represented in sufficient detail on the previous page.

Variability Guide:

The customer's project proposal did not indicate any product lines explicitly based on the current architecture, hence this section is not applicable as on date.

Rationale:

The current architecture was designed to cater to the explicit mention of the QAR's within the project proposal document, namely:

1. Availability – This was also specified as a market differentiator for the client hence the databases were configured in a HA mode with secondary mirror which is acting as hot spare.

2. Performance – The customer expects the communication with the first responders to be within the first minute of any incident occurrence. This is taken care of by streaming the data frames over a high-bandwidth broadband connection from the customer site to the Firm's network where the notification services are configured to utilize the dedicated in-house gateways to communicate with the first responder teams and the customers within the specified time frame
3. Modifiability – The customer indicated in the project proposal that the customer's data will be analyzed to improvise on their product offerings which indicate the need to provide modifiability for existing services hence all components in the current architecture are designed to be modular in nature to facilitate the goal.

UML version for the Deployment View:

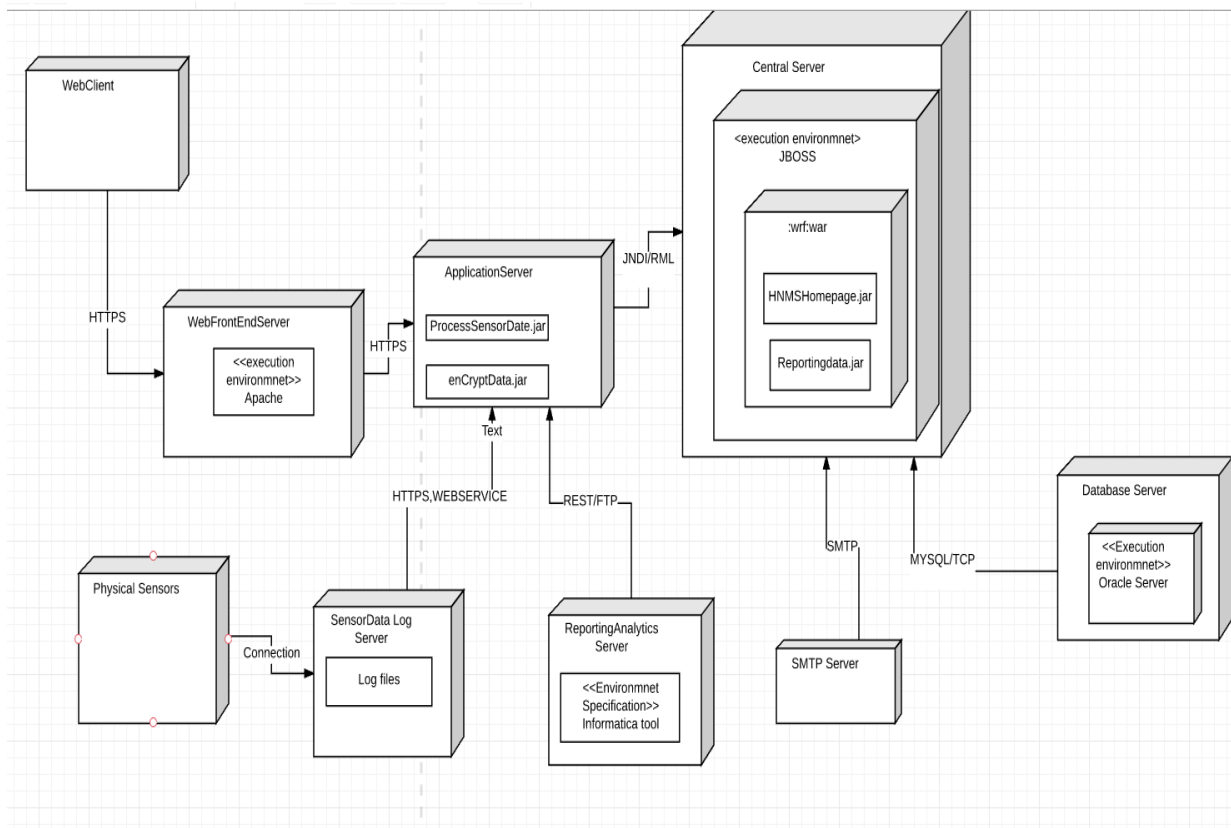
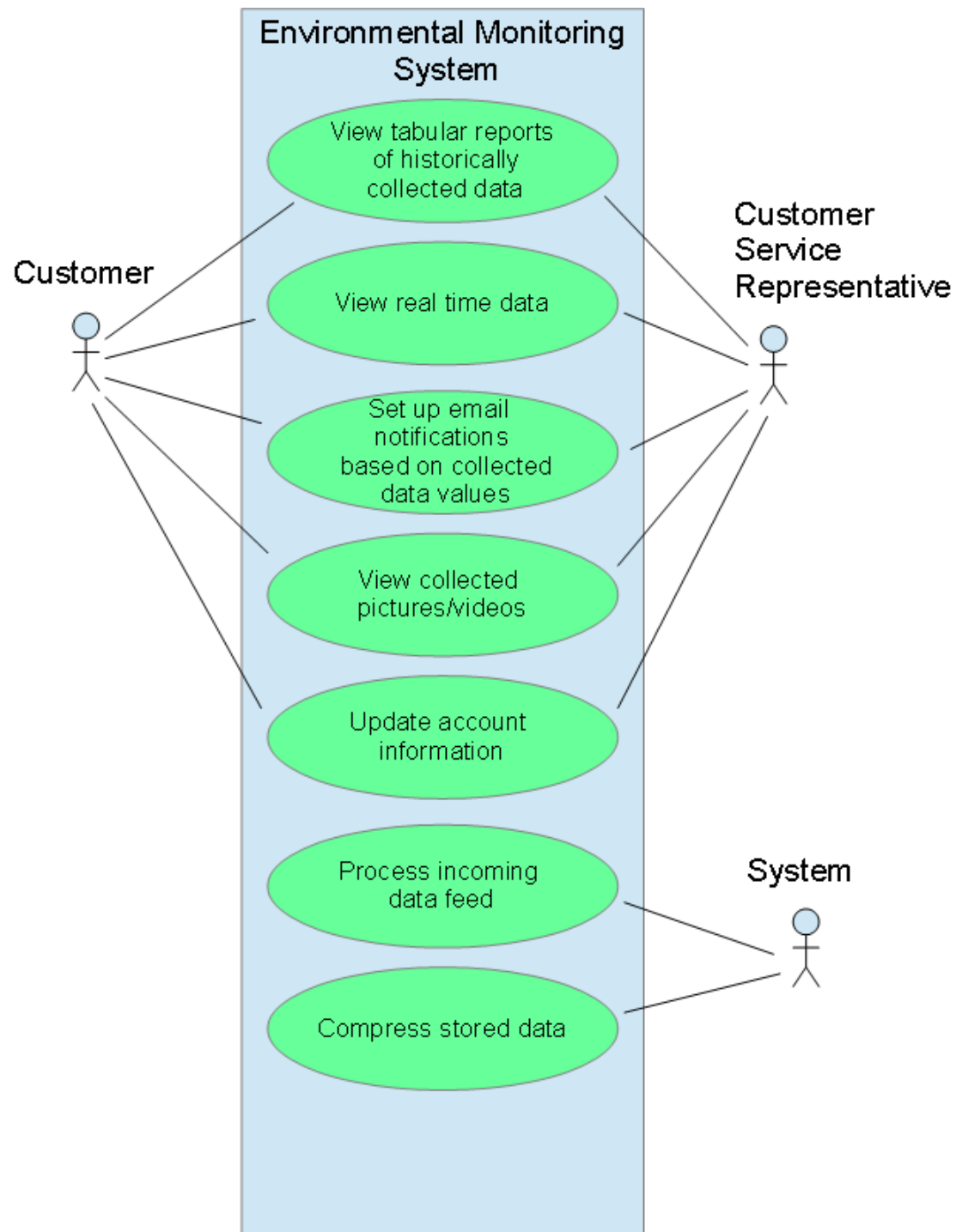


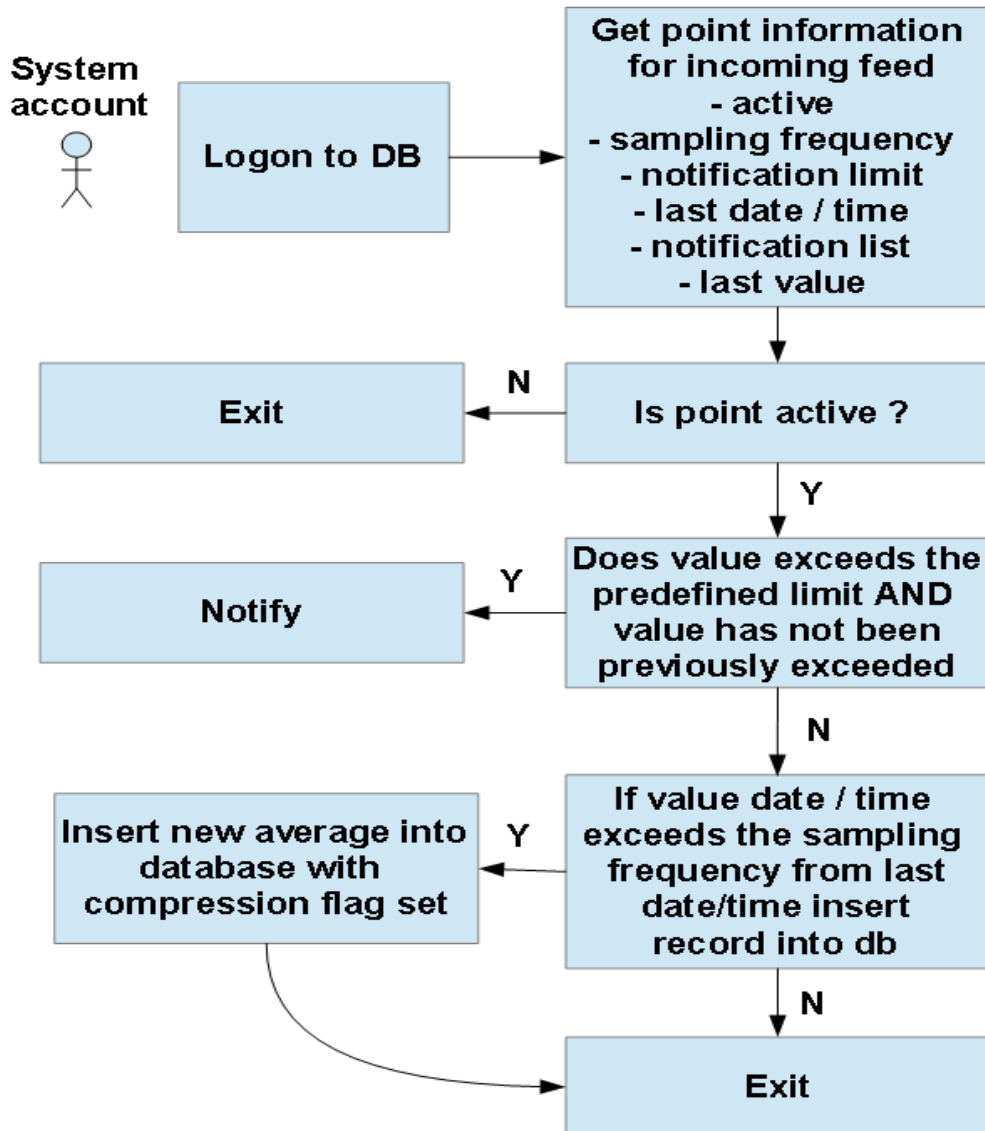
Figure 8: UML Diagram of Software Deployment

For Environment Monitoring application to modernize the hardware platform, EMNS system consists of 3 large Linux servers with 8 CPU and 32 GB RAM. One node is dedicated for Central Server from where the content is syndicated to the publish nodes. The other two boxes are used for publishing mode. In each publishing server, there will be two JVM instances with 4 GB RAM. The total 4 JVMs are clustered to take the load. Apache HTTP server is used for load balancing the 4 JVMs. For Database, we are going to host a new oracle Server.

Use Cases:

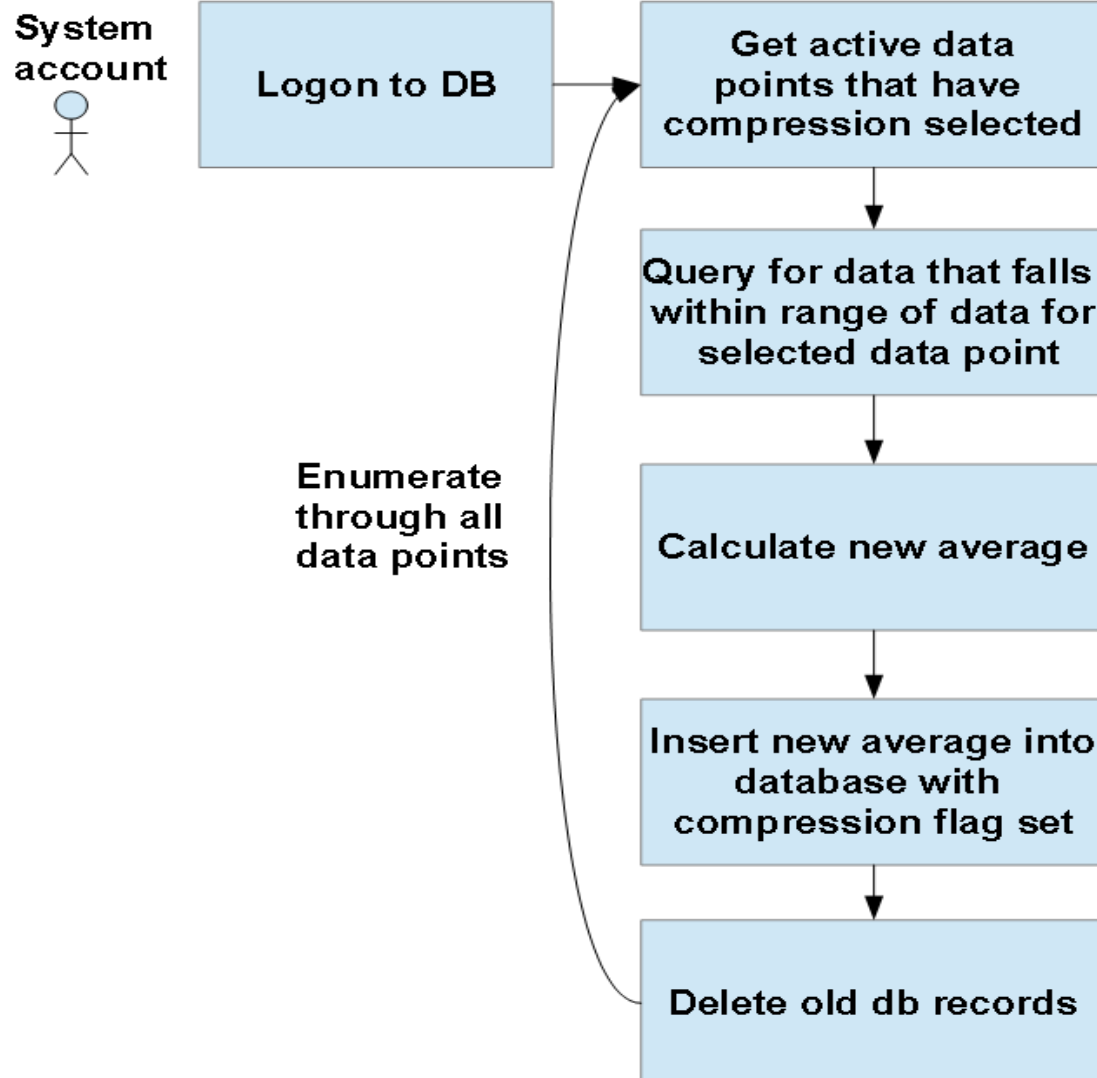
Case#1



Case#2**Data Feed Input**

Case#3

Data Compression Service



Case#4

Key Users Interactions: In the eventual full development of this home environment monitoring and analysis security system, there will most likely be numerous use cases that will cover all possible avenues for such a rich and diverse security system. For the meantime, let us look at the use cases that need to be available from the very beginning of the system's development. The first figure describes two of the main users of the system, the Home user and the Technician, and how they both interact with the system. The Arm System and Disarm System use cases both require the actor to specify an activation code. The latter is shown as an inclusion use case. The use cases performed by the Configuration manager require a more sophisticated Log-In use case to be performed.

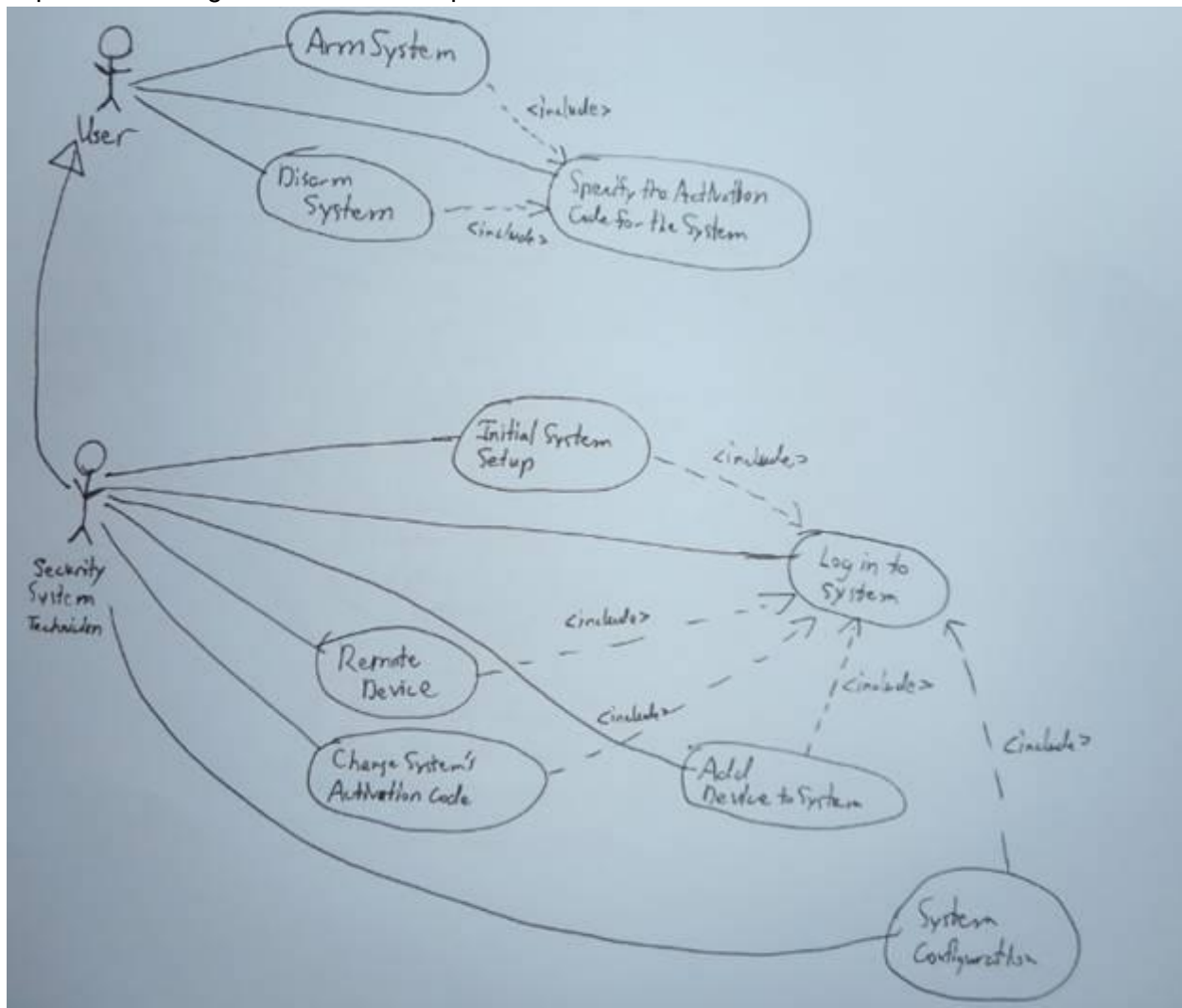


Figure : Use Case for Release of the System to the User

Case#5

Security monitoring of the system The figure displays the user known as the System Admin, and their interaction with the system. Much like with the Home user and the Technician, the System Admin must log in to the system in order to perform their functions. This includes monitoring the security system, central data & storage, data analytics, as well as providing notification when there is a breach/alert to the system.

*

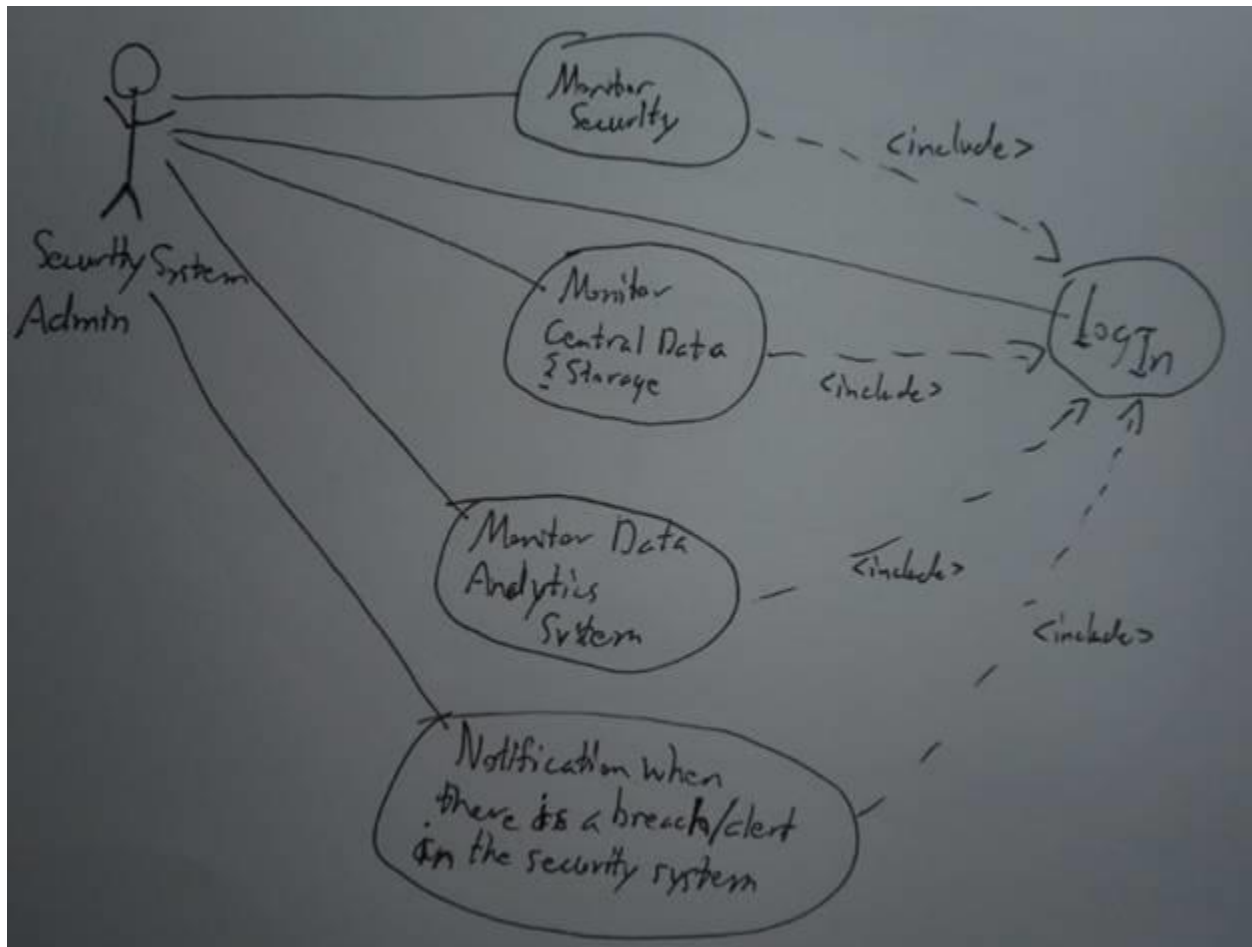


Figure : Use Case for Handling of System by the System Admin

Activity/State Diagrams

The following contain some examples of the behavior of the security system.

The following, Figure 6, is an activity diagram displaying the top level behavior of the Security System when one is class. When the security system's central processor is running, it must be able to do two things at once: Perform its main security monitoring functions and respond to configuration changes. Figure shows that these 'Monitoring' and 'Configuration' activities are conceptually concurrent – any part of either may overlap the other. For instance, the system could be armed and detecting a burglar at the same time the homeowner is logging in from an external location via the web in order to change the active configuration.

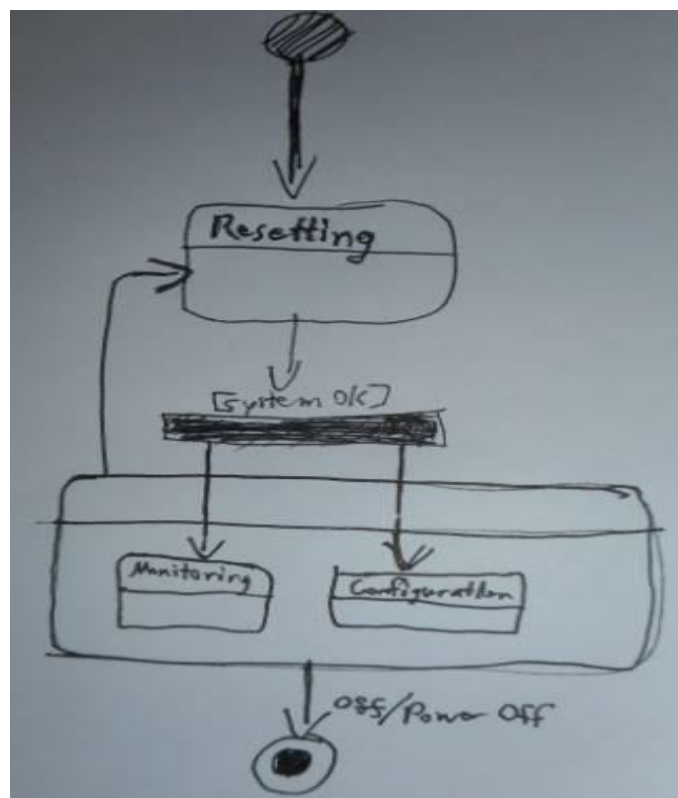


Figure : Top level activity diagram

Figure 7 presents the behavior of the home environment monitoring system class during the monitoring activity of the previous figure. There are three possible values for its activationState attribute: CheckingSystem, Disarmed and Armed. The system toggles backwards and forwards between Disarmed and Armed in response to user actions. The successfulActivation and successfulDeactivation events are triggered by the user interface. The return event marks when,

after resetting, the system will go back to what it was doing before (being armed or disarmed). This is important, as it prevents the reset process from circumventing the security.

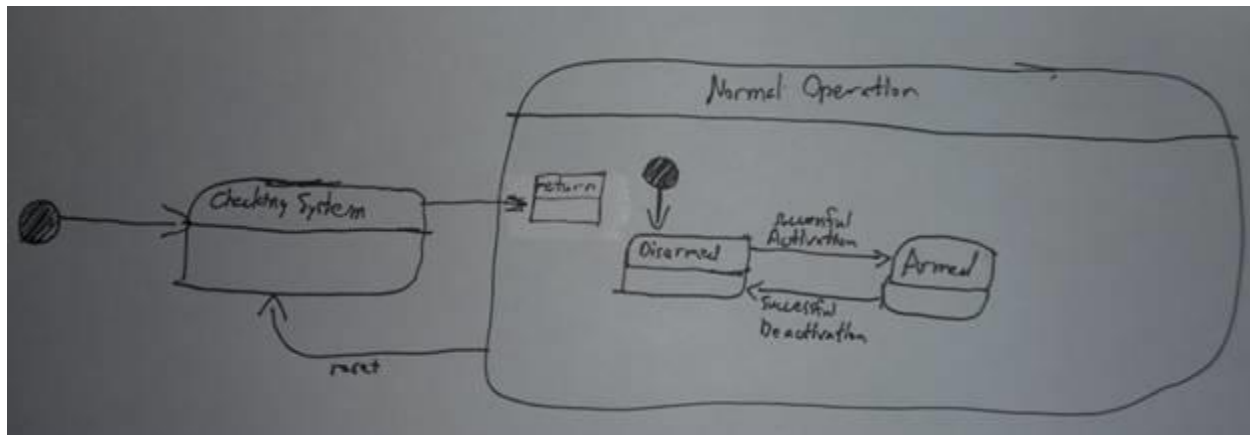


Figure : Behavior of Home Environment Monitoring System during its Monitoring Activity

Figure 8 shows details of the system's armed state. If a motion detector detects motion, no alarm is immediately sounded: The system requires more than a short period of motion to sound an alarm; the motion could be caused by the homeowner coming home and going through the process of deactivating the system at a control panel, for example. After 40 seconds the system goes into Heightened Motion Sensitivity state. In this state, the system will respond immediately to any further motion; it will stay in this state for 5 minutes before dropping back to No Sensors Triggered state. If any other sensor is triggered (or if a motion sensor is triggered in Heightened Motion Sensitivity) state, then the system goes into Acting On Alarm state. A timer is started on entry into this state, if no further sensors are triggered, this timer will time out after a user-configurable amount of time and the alarm will go off. This prevents a persistent false alarm from ringing indefinitely. On the other hand, if sensors continue to be triggered, the timer is reset, so the alarm will keep ringing.

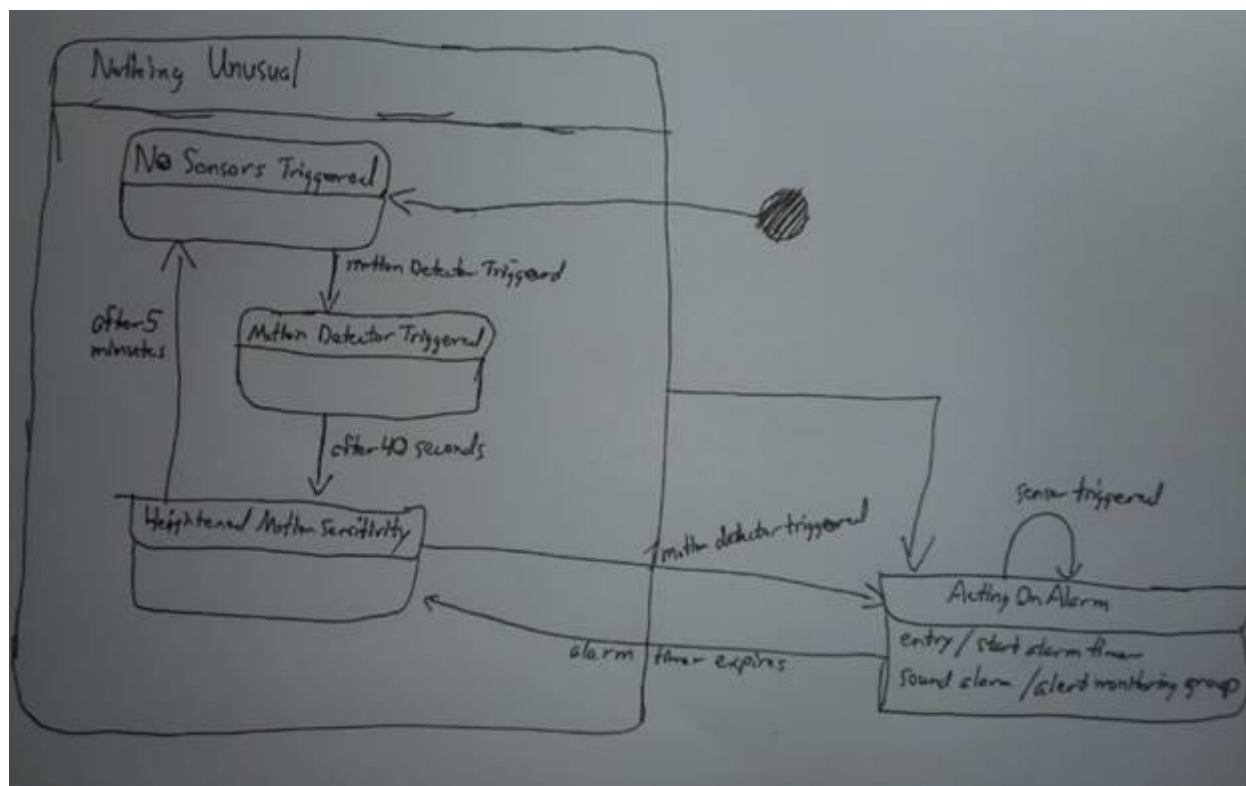


Figure : State Diagram of the Armed State

Figure 9 shows the user interface of a model of control panel that is used to arm or disarm the system.

The control panel has a display capable of displaying a message, along with a series of buttons: Ten digit buttons (0-9), and keys labeled 'Arm - Stay', 'Arm - Away', 'Test', and 'Cancel'. In the following we only model the events and state transitions, not what is displayed on the screen. The control panel starts up displaying a welcome message. Then it goes into Ready For Use state if the system is currently disarmed, or Security Delay 2 state if the system is currently armed. Ready For Use state means that the system is not armed; in order to perform some function, however, the user must enter a valid ActivationCode. As soon as the first number key is pressed, the control panel goes into Entering Activation Code state. The panel stays in this state as long as the user keeps pressing number keys (activation codes can be very long if the configuration manager wants). When the user has finished entering his or her code he or she presses a function key: There are three function keys in the control panel modeled here: Arm - Stay, Arm - Away, and Test. If the user presses Test, and the activation code was correct, then the system goes into Test Alarm state for five seconds before returning to Ready For Use state. If the user presses either Arm key after entering a valid code, the system goes into Delay To Leave state. This gives the user time to leave the house, lock the doors, etc. before the system becomes armed. The difference between the Arm keys is that the system will be sensitive to different sets of sensors – however from the perspective of the current diagram, both keys cause the same effect. If the user presses a function key without entering a valid activation code, the system goes into Security Delay 1 for a few seconds. The security delay prevents

somebody with ill intent from trying out codes over and over again rapidly until they randomly stumble on a valid one; they always have to put up with a delay, which should make the random guessing process infeasible.

If a user presses the Cancel key while entering the activation code, the system goes back to Ready For Use state. This ensures that if a legitimate user starts typing the wrong code, they can try again immediately.

Sixty seconds after entering Delay To Leave state, the system triggers the successfulActivation event and goes into Awaiting Disarm Activation Code state. Triggering this event forces the Security System to become armed.

Once the system is armed, the only way to disarm it is to enter a valid ActivationCode again. As soon as the user presses the first number key, the system goes into Accepting Disarm Code state. The system keeps accepting keys until a valid code has been entered, at which time the UI triggers the successfulDeactivation event and transitions to Ready For Use state.

If the user types an invalid code, he or she can press 'Cancel' to try again. However it will not be possible to try again for 20 seconds due to the presence of the Security Delay 2 state. This prevents rapid retries by someone trying to guess the code.

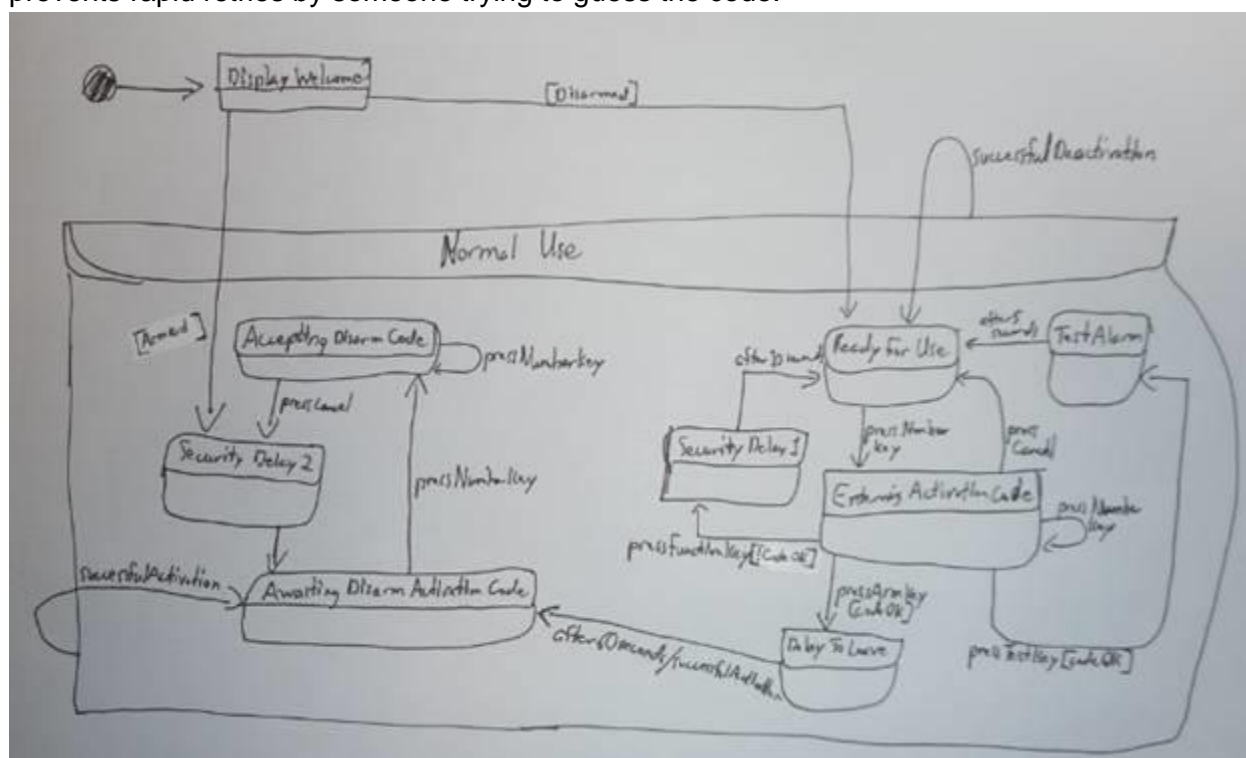


Figure : Behavior of the Control Panel Interface for the User

Utility Tree:

| Root Node | Quality Attribute Requirement | Refinement | ASR |
|--------------|-------------------------------|-------------------------|---|
| Utility Tree | Availability | Availability Percentage | The system should have 99.9999% availability. (H, H) |
| | | Detect Fault | An email notification is expected to be received from the Server Health Monitoring System with the relevant failure and server details when a heartbeat is not received every 2 seconds (H,L). |
| | | Recover from Fault | If the primary DB server fails, then the secondary DB server automatically assumes role of primary DB server with no loss of data within 180 seconds of the failure of the primary server. (H,M) |
| | Performance | Throughput | The software system should be able to process 10,000 transactions per second during normal operations. (H,H) |
| | | Latency | The system should notify the end-users (customers/first responder teams) any incident within the first 60 seconds of its occurrence. (H,H) |
| | | | At peak load, a user is able to generate a tabulated report for a selected data point for a 24 hour period within 60 seconds. (M,L) |
| | | | Any user initiated transaction during normal load, should be processed by the software system in less than 5 seconds. (H,M) |
| | | | Any user initiated transaction while the system is at peak load (considered as twice the normal load), and the transaction completes in less than 10 seconds. (L,M) |
| | Security | Availability | An attacker attempts to make EMS unusable for its intended use by a denial of service attack. This denial of service attack is detected by the server health monitoring system and an alarm is sent to system administrator within 30 seconds of its detection. (H,M) |

| | | | |
|--|-----------------|---|--|
| | | Integrity | The system resists unauthorized intrusion and reports the intrusion attempt to the authorities within 90 seconds. (H,M) |
| | | Confidentiality and Assurance | The client's data should be secured with the highest form of encryption standard (the AES standard). (H,H) |
| | | How much is the system compromised when the system is compromised | The system should issue an alarm to all relevant stakeholders every single time when an attacker(internal/external) attempts to disable the software system. (H,H) |
| | Usability | Proficiency Training | A new hire assigned to work on the security aspects of the system with more than a year experience in the business becomes proficient with the security system's core functions in less than a week. (M,L) |
| | | | A home user should become proficient in using the system via its web interfaces in under 45 minutes. (M,M) |
| | | User satisfaction | A minimum of 85 % of the end users should be satisfied with the layouts and content of the generic and specific reports offered by the software product at the end of the first year of its operation. (M,M) |
| | | Initial Training | A new user is able to logon to the web portal and view real time data within 15 minutes after viewing a 15 minute instructional video. (M,M) |
| | Testability | Probability of fault being revealed by any test run | The system should have the ability to reveal any fault 99% of the times when a test is run repeatedly. (L,H) |
| | Scalability | Growth | The system should have the ability to align according to the future need to add infrastructure to support the business with no downtime. (M,L) |
| | Maintainability | Routine Maintenance | Any preventive maintenance to the software/hardware system should not take more than 8 hours from start to finish. (H,M) |
| | Modifiability | Ability to add physical | An installer should be able to add/delete/modify configuration of a new piece |

| | | | |
|--|------------------|---|--|
| | | monitoring equipment | of monitoring equipment without disruption to the rest of the existing infrastructure. (M,M) |
| | | Customizability | The system should have the ability to be configured depending on the customer's requirements, with no constraints on the functionality offered irrespective of the number of physical monitoring elements configured within the software. (H, L) |
| | | Integration | The software should support continuous integration with new technologies and improvise the service offerings to its end users. (H,H) |
| | Modularity | Replace Database | Replace the underlying database with another vendor's database that is compatible with the Database Portability Layer within 14 days without any disruption to the business. (L,M) |
| | Interoperability | Percentage of information exchanges correctly processed | The system should correctly process input from each and every associated monitoring equipment 99.99 percent of the time. (M,M) |

Priority ranking based on importance to customer(business value) / difficulty to implement ranking using a H (high), M (medium), and L (low) ranking.

Appendix

Glossary

Login: (Home Monitoring Alarm) System: The core singleton class (only one instance exists)

login: Entered when logging into the system through a web browser

ConfigurationSensors: A setup of the system with various Devices (in zones), Sensors, and ActivationCodes. There will always be at least one configuration – a configuration named 'default' is created when the system starts. This will contain an activation code 9999 and all devices initially added to the system. Additional configurations can be created (Duplicate Configuration use case) to allow the homeowner to experiment with the system, set up temporary configurations (e.g. when guests will be present and need their own activation codes) etc.

CameraSensor: Represents a camera that can send images / videos to the system, and can be panned and zoomed.

LawnSensor: To verify the status of the lawn's moisture content at the remote site.

DoorSensor: To verify the status of the Door Closed position at the remote site.

ACSensor: To verify the status of the Air Conditioner at the remote site.

Controller: A number from 0 to 5 that can be defined to help the user understand where an emergency is occurring. This can be used to divide the house into up to five zones (e.g. outside, basement, living room, eating areas, upstairs). The default is zero, meaning undefined zone. The sound of an the alarm depends on the zone of the sensor that triggers the system (zone 0 = continuous sound, zone 1 = evenly spaced beeps, zone 2 = pairs of beeps, etc.) An AlarmSignaler in zone 0 will always sound. An AlarmSignaler given a numbered zone will only sound if a sensor in that zone triggers the alarm..

EmergencySystem: The systems relates to 3 types (attributes) of emergency systems.

- getAlert.
- sendAlerts.
- turnOffAlerts.

HMA System: The core singleton class (only one instance exists)

- login: Entered when logging into the system through a web browser
- ChangeSensorConfigurations:

- getLogData:
- setFalseAlarmOff:

• viewReport:

ControlPanelProcessing:

accessHardware:

ConfigurationSenors: A setup of the system with various Devices (in zones), Sensors, and ActivationCodes. There will always be at least one configuration – a configuration named 'default' is created when the system starts. This will contain an activation code 9999 and all devices initially added to the system. Additional configurations can be created (Duplicate Configuration use case) to allow the homeowner to experiment with the system, set up temporary configurations (e.g. when guests will be present and need their own activation codes) etc.

- toggleSensor:
- turnoffSensor: turn of the security sensor
- changeCameraDirection: changes the current position of the camera on the residence that it is viewing.
- sendData: sends data to the HMA System

Controller: A number from 0 to 5 that can be defined to help the user understand where an emergency is occurring. This can be used to divide the house into up to five zones (e.g. outside, basement, living room, eating areas, upstairs). The default is zero, meaning undefined zone. The sound of an the alarm depends on the zone of the sensor that triggers the system (zone 0 = continuous sound, zone 1 = evenly spaced beeps, zone 2 = pairs of beeps, etc.) An AlarmSignaler in zone 0 will always sound. An AlarmSignaler given a numbered zone will only sound if a sensor in that zone triggers the alarm.

UsesReportingTool:

EmergencySystem: The systems relates to 3 types (attributes) of emergency systems.

- getAlert.
- sendAlerts.
- turnOffAlerts.