ASSIGNMENT 1
COMP201 – Software Engineering

Abstract
This assignment is a comprehensive requirement engineering document for a proposed building security system.

Matt Paver
sgmpaver@liverpool.ac.uk

Table of Contents

Task 1

A) Use Case Model for Proposed Building Security System:

Decomposition of Actors

Actor:	Description:	Reference:
Senior Bank Staff	Senior employees with elevated access privileges, responsible for managerial and critical operations in the bank.	UC1: Access System UC2: Configure Burglar Alarm UC3: Configure Fire Alarm UC4: Trigger Tamper Alarm UC5: Trigger Burglar Alarm UC9: Press Fire Alarm Button UC14: Reset Fire Alarm UC15: Activate Burglar Alarm for Holidays UC16: Setup Burglar Alarm Schedule UC18: Access High-Security Area UC22: Visitor Registration UC23: Visitor Checkout UC25: Configure Sensor Thresholds UC26: Deactivate Burglar Alarm
Junior Bank Staff	Regular bank employees with standard access to the building and limited interactions with the security system.	UC1: Access System UC4: Trigger Tamper Alarm UC5: Trigger Burglar Alarm UC9: Press Fire Alarm Button UC10: Press Panic Alarm Button UC24: Incorrect Access Code Entry
Security Guard	Oversee the verification of identities, access permissions, security feed monitoring, and security alert management to uphold the building's security.	UC1: Access System UC2: Configure Burglar Alarm UC3: Configure Fire Alarm UC4: Trigger Tamper Alarm UC5: Trigger Burglar Alarm UC9: Press Fire Alarm Button

1

		UC20: Visitor Log Viewing
		UC21: Security Alert Management
		UC22: Visitor Registration
		UC23: Visitor Checkout
		UC25: Configure Sensor Thresholds
		UC26: Deactivate Burglar Alarm
Maintenance Staff	Responsible for ensuring that all sensors, alarms, and other system components are in working order. They perform regular checks, maintenance, and replacements when necessary.	UC1: Access System UC2: Configure Burglar Alarm UC3: Configure Fire Alarm UC25: Configure Sensor Thresholds UC27: System Maintenance Check
Police	Respond to security breach alerts in the building, ensuring the building's security and investigating potential threats.	UC4: Trigger Tamper Alarm UC5: Trigger Burglar Alarm UC6: Trigger Window Sensor UC7: Trigger Door Sensor UC8: Trigger Floor Sensor UC28: Alert Police
Fire Brigade	Respond to fire alerts in the building, ensuring the safety of the building's occupants.	UC9: Press Fire Alarm Button UC12: Detect Excessive Heat UC13: Detect Prolonged Smoke UC29: Alert Fire Brigade
Intruder	Unidentified entities attempting unauthorised access or malicious actions.	UC5: Trigger Burglar Alarm UC6: Trigger Window Sensor UC7: Trigger Door Sensor UC8: Trigger Floor Sensor
System	The automated system designed to detect security breaches and potential fire hazards.	UC6: Trigger Window Sensor UC7: Trigger Door Sensor UC8: Trigger Floor Sensor UC11: Activate Fire Door Release UC17: Handle Designated Entry Countdown UC19: Activate Alarms UC24: Incorrect Access Code Entry
Visitor	Individuals who don't work at the bank but are visiting for various reasons. They might require temporary access permissions and are subject to security checks.	UC9: Press Fire Alarm Button UC22: Visitor Registration UC23: Visitor Checkout

Use case descriptions:

UC1 – Access System

ID	UC1
Actors	Senior & Junior Bank Employees, Security Guard, Maintenance Staff
Name	Access System
Description	Any user of the system must access the system with both a swipe card and a corresponding access code. The code type (fire or burglary) determines the type of access granted. Each card has its access codes configured.
Pre-conditions	• The system is operational. • The employee possesses a valid swipe card and knows the access code.
Event flow	1. The user approaches the entry point. 2. The user swipes the card on the card reader. 3. The system prompts for an access code. 4. The user inputs the correct access code. 5. The system grants access and logs the entry.
Post-condition	User has access to the system for configuration.
Includes	UC2: Configure Burglar Alarm UC3: Configure Fire Alarm
Extensions	UC4: Trigger Tamper Alarm
Triggers	User attempts to access the system.

UC2 – Configure Burglar Alarm

ID	UC2
Actors	Senior Bank Staff, Security Guard, Maintenance Staff
Name	Configure Burglar Alarm
Description	User configures the burglar alarm settings after entering the burglary code.
Pre-conditions	User has authenticated access to the security system using the burglary code.
Event flow	1. User selects burglar alarm settings. 2. User configures desired settings. 3. System saves the configurations.
Post-condition	Burglar alarm settings are updated.
Includes	None
Extensions	None
Triggers	User enters the burglary code.

UC3 – Configure Fire Alarm

ID	UC3
Actors	Senior Bank Staff, Security Guard, Maintenance Staff
Name	Configure Fire Alarm
Description	User configures the fire alarm settings after entering the fire code.
Pre-conditions	User has authenticated access to the security system with the fire code.
Event flow	1. User selects fire alarm settings. 2. User configures desired settings. 3. System saves the configurations.
Post-condition	Fire alarm settings are updated.
Includes	None

Extensions	None
Triggers	User enters the fire code.

UC4 – Trigger Tamper Alarm

ID	UC4
Actors	Junior Bank Staff, Senior Bank Staff, Security Guard, Police
Name	Trigger Tamper Alarm
Description	User triggers a tamper alarm after entering incorrect access code 3 times.
Pre-conditions	User has entered incorrect access code three times
Event flow	1. User enters incorrect access code for the third time. 2. System detects three incorrect attempts. 3. System sounds a tamper alarm via the console speaker. 4. User's access card is disabled. 5. System automatically notifies the police about a potential security breach.
Post-condition	Tamper alarm is active; user's card is disabled and the police have been notified.
Includes	UC29: Alert Police
Extensions	None
Triggers	User enters an incorrect system access code three times consecutively.

UC5 – Trigger Burglar Alarm

ID	UC5
Actors	Junior Bank Staff, Senior Bank Staff, Security Guard, Police
Name	Trigger Burglar Alarm
Description	User or intruder action triggers the burglar alarm. System notifies the police. An audible alert is given through the console speaker.
Pre-conditions	System detects a security breach.
Event flow	1. System detects a security breach (door/window sensor activation). 2. Burglar alarm is activated. 3. System automatically notifies the police. 4. Warning sound and flashing lights are activated.
Post-condition	The Security Guard are aware of the security breach and can inform the police where necessary.
Includes	UC29: Alert Police
Extensions	UC6: Trigger Window Sensor UC7: Trigger Door Sensor UC8: Trigger Floor Sensor UC10: Press Panic Alarm Button
Triggers	Door, floor, or window sensor is activated when the system is active, or a designated sensor (always on) is activated. Panic button is pressed, regardless of system state.

UC6 – Trigger Window Sensor

ID	UC6
Actors	Intruder, System
Name	Trigger Window Sensor
Description	The window sensor is activated when a window is opened. Specific sensors can be designated as always on and will trigger the alarm even if the system is inactive.
Pre-conditions	System is armed.
Event flow	1. Intruder opens a window. 2. System detects window sensor activation. 3. System notifies the police.
Post-condition	Alarm system is triggered.
Includes	None
Extensions	None
Triggers	Opening of a window when system is armed.

UC7 – Trigger Door Sensor

ID	UC7
Actors	Intruder, System
Name	Trigger Door Sensor
Description	Door sensor is activated when a door is opened. Specific sensors can be designated as always on and will trigger the alarm even if the system is inactive.
Pre-conditions	System is armed.
Event flow	1. Intruder opens a door. 2. System detects door sensor activation. 3. System notifies the police.
Post-condition	Alarm system is triggered.
Includes	None
Extensions	None
Triggers	Opening of a door when system is armed.

UC8 – Trigger Floor Sensor

ID	UC8
Actors	Intruder, System
Name	Trigger Floor Sensor
Description	Floor sensor is activated when a protected area is stepped on. Specific floor areas can be designated as always on and will trigger the alarm even if the system is inactive.
Pre-conditions	System is armed.
Event flow	1. Intruder steps on a protected floor area. 2. System detects floor sensor activation. 3. System notifies the police.
Post-condition	Alarm system is triggered.
Includes	None
Extensions	None

Triggers	Stepping on a protected floor area when system is armed.

ID	UC9
Actors	Fire Brigade, Junior Bank Staff, Senior Bank Staff, Security Guard, Visitor
Name	Press Fire Alarm Button
Description	A user can manually trigger the fire alarm using the fire alarm button.
Pre-conditions	User perceives a fire threat.
Event flow	1. A fire alarm button is manually pressed by a user. 2. The fire brigade is summoned automatically via an automatic calling system. 3. All fire alarm bells are sounded, and lights are flashed throughout the building.
Post-condition	Fire alarm is activated.
Includes	UC19: Activate Alarms
Extensions	None
Triggers	A fire alarm button is pressed.

ID	UC10
Actors	Junior Bank Staff, Senior Bank Staff, Security Guard
Name	Press Panic Alarm Button
Description	Staff can manually trigger the panic alarm using the panic alarm button in cases of threats like robbery, regardless of whether the system is active or inactive.
Pre-conditions	Staff perceives a security threat.
Event flow	1. Staff presses the panic alarm button. 2. System activates the panic alarm. 3. System notifies the police.
Post-condition	Panic alarm is activated.
Includes	UC5: Trigger Burglar Alarm UC29: Alert Police
Extensions	None
Triggers	Pressing of the panic alarm button.

ID	UC11
Actors	System
Name	Activate Fire Door Release
Description	In case of fire detection, the fire door release solenoids are activated to allow for safe evacuation.
Pre-conditions	Fire is detected.
Event flow	1. Fire detection system is triggered. 2. System activates the fire door release solenoids.
Post-condition	Fire doors are released for safe evacuation.

Includes	None
Extensions	UC12: Detect Excessive Heat
	UC13: Detect Prolonged Smoke
Triggers	Fire detection.

ID	UC12
Actors	System, Fire Brigade
Name	Detect Excessive Heat
Description	The system detects if the temperature exceeds the critical threshold set by the fire brigade.
Pre-conditions	Excessive heat is detected by the heat sensors.
Event flow	1. Excessive heat is detected by the heat sensors.
	2. If temperature exceeds TC (Temperature Critical), the system identifies it as a potential fire threat.
	3. The fire brigade is summoned automatically via an automatic calling system.
	4. All fire alarm bells are sounded, and lights are flashed throughout the building.
Post-condition	Fire alarm is active, and notifications have been sent.
Includes	UC29: Alert Fire Brigade
Extensions	UC19: Activate Alarms
Triggers	Heat sensors detect a temperature greater than TC (Temperature Critical).

ID	UC13
Actors	System, Fire Brigade
Name	Detect Prolonged Smoke
Description	The system detects smoke presence for a duration longer than the critical time set by the fire brigade.
Pre-conditions	Smoke detectors detect smoke for a time greater than 'Time Critical'.
Event flow	1. Smoke detectors detect smoke for a time greater than 'Time Critical'.
	2. System triggers the fire alarm.
	3. The fire brigade is summoned automatically via an automatic calling system.
	4. All fire alarm bells are sounded.
	5. Lights are flashed throughout the building.
Post-condition	Fire alarm is active, and notifications have been sent.
Includes	UC29: Alert Fire Brigade
Extensions	UC19: Activate Alarms
Triggers	Smoke detectors detect smoke for a time greater than 'Time Critical'.

ID	UC14

Actors	Security Guard, Senior Bank Staff
Name	Reset Fire Alarm
Description	User resets the fire alarm after it has been triggered.
Pre-conditions	Fire alarm has been triggered.
Event flow	1. User approaches the system console. 2. User swipes a valid card. 3. User enters the fire disable code. 4. System validates the entered code. 5. Fire alarm is deactivated.
Post-condition	Fire alarm is inactive.
Includes	None
Extensions	None
Triggers	User's intent to deactivate the triggered fire alarm.

UC15 – Activate Burglar Alarm for Holidays

ID	UC15
Actors	Security Guard, Senior Bank Staff
Name	Activate Burglar Alarm for Holidays
Description	User activates the burglar alarm for a fixed number of days for holidays.
Pre-conditions	User has access to the system for configuration.
Event flow	1. User selects the option to activate burglar alarm for holidays. 2. User specifies the number of days for which the alarm should remain active. 3. System activates the burglar alarm for the specified duration.
Post-condition	Burglar alarm is active for the specified holiday duration.
Includes	None
Extensions	None
Triggers	User's intent to activate the burglar alarm for holidays.

UC16 – Setup Burglar Alarm Schedule

ID	UC16
Actors	Security Guard, Senior Bank Staff
Name	Setup Burglar Alarm Schedule
Description	User sets up specific activation and deactivation times for the burglar alarm.
Pre-conditions	User has access to the system for configuration.
Event flow	1. User selects option to set up burglar alarm schedule. 2. User specifies activation and deactivation times for each day of the week. 3. System saves the schedule.
Post-condition	Burglar alarm schedule is updated.
Includes	None
Extensions	None
Triggers	User's intent to set up a burglar alarm schedule.

UC17 – Handle Designated Entry Countdown

ID	UC17
Actors	System
Name	Handle Designated Entry Countdown
Description	System handles countdown for designated entry points, issuing an audio warning. The countdown duration is set based on the system's configuration.
Pre-conditions	A designated entry point door is opened while the system is active.
Event flow	1. The system detects the opening of a designated entry door. 2. The system starts the countdown and issues an audio warning. 3. The countdown duration is based on a pre-configured setting. 4. If the system is not deactivated before the countdown ends, a burglar alarm is triggered.
Post-condition	Burglar alarm is triggered if system is not deactivated in time.
Includes	None
Extensions	None
Triggers	Opening of a designated entry point door while system is active.

UC18 – Access High-Security Area

ID	UC18
Actors	Security Guard, Senior Staff
Name	Access High-Security Area
Description	User accesses high-security areas using special card readers on doors, distinct from standard access points.
Pre-conditions	User has a valid access card for the high-security area.
Event flow	1. User swipes card on the card reader near the door. 2. System validates access. 3. Door unlocks allowing the user to enter.
Post-condition	User has accessed the high-security area.
Includes	None
Extensions	None
Triggers	User's intent to access a high-security area.

UC19 – Activate Alarms

ID	UC19
Actors	System
Name	Activate Alarms
Description	When an alarm (either fire or burglar) is triggered, the flashing lights are activated as an alert mechanism.
Pre-conditions	An alarm condition is detected.
Event flow	1. System detects a triggering condition (like smoke detection or security breach). 2. Flashing lights are activated.
Post-condition	Flashing lights are on to alert the occupants.

Includes	UC4: Trigger Tamper Alarm
	UC5: Trigger Burglar Alarm
	UC9: Press Fire Alarm Button
	UC28: Alert Police
	UC29: Alert Fire Brigade
	UC12: Detect Excessive Heat
	UC13: Detect Prolonged Smoke
Extensions	None
Triggers	Detection of smoke, heat, door/window sensor activation, specific conditions as defined in the requirements

ID	UC20
Actors	Security Guard
Name	Visitor Log Viewing
Description	Security guard reviews the visitor log for a selected day.
Pre-conditions	The security guard has the necessary permissions to view the visitor log.
Event flow	1. The security guard selects the date to view the visitor log.
	2. The system shows the visitor log for the selected date.
Post-condition	The visitor log for the selected date is shown to the security guard.
Includes	None
Extensions	None
Triggers	Security guard's request to view visitor log for a specific date.

UC21 – Security Alert Management

ID	UC21
Actors	Security Guard
Name	Security Alert Management
Description	Security Guard manages the security alerts generated by the system.
Pre-conditions	A security breach has been detected, and a security alert has been generated.
Event flow	1. The Security Guard or Administrator logs into the system.
	2. They navigate to the Security Alerts section.
	3. They review the security alert details and act if needed.
	4. They update the security alert status in the system and log out.
Post-condition	The security alert status has been updated in the system.
Includes	None
Extensions	None
Triggers	Detection of a security breach or abnormal activity by the system that requires attention or review by the security guard.

ID	UC22
Actors	Security Guard, Visitor
Name	Visitor Registration
Description	When a visitor arrives, the security guard registers their details and provides them with a temporary access card.
Pre-conditions	The visitor does not have prior access permissions.
Event flow	1. Visitor arrives at the security desk. 2. Security Guard takes their details (name, purpose of visit, etc.). 3. Security Guard provides a temporary access card. 4. System logs visitor details.
Post-condition	Visitor is registered and can access permitted areas.
Includes	None
Extensions	UC1: Access System
Triggers	Visitor's arrival without prior access.

ID	UC23
Actors	Security Guard, Visitor
Name	Visitor Checkout
Description	Before leaving, visitors return their temporary access cards and are checked out from the system.
Pre-conditions	Visitor has a temporary access card.
Event flow	1. Visitor arrives at the security desk to check out. 2. Security Guard takes the temporary access card. 3. System logs visitor checkout.
Post-condition	Visitor is checked out and leaves the premises.
Includes	None
Extensions	None
Triggers	Visitor's intention to leave.

ID	UC24
Actors	Junior & Senior Bank Employees, Security Guard, Maintenance Staff
Name	Incorrect Access Code Entry
Description	The user enters an incorrect access code when trying to access the system.
Pre-conditions	• The system is operational. • The user possesses a valid swipe card.
Event flow	1. The user swipes the card on the card reader. 2. The system prompts for an access code. 3. The user inputs an incorrect access code. 4. System logs the incorrect entry.
Post-condition	Access is denied.
Includes	UC4: Trigger Tamper Alarm
Extensions	None

Triggers	Visitor's intention to leave.

UC25 – Configure Sensor Thresholds

ID	UC25
Actors	Senior Bank Staff, Security Guard, Maintenance Staff
Name	Configure Sensor Thresholds
Description	The user configures thresholds for various sensors, such as the critical temperature (TC) and 'Time Critical' for smoke detection, after entering the system.
Pre-conditions	User has authenticated access to the security system.
Event flow	1. User selects sensor settings. 2. User configures desired thresholds (e.g., temperature, smoke duration). 3. User sets the 'Temperature Critical' (TC) for heat sensors based on fire brigade recommendations. 4. User sets the 'Time Critical' duration for smoke detectors based on fire brigade recommendations. 5. System saves the configurations.
Post-condition	Sensor thresholds are updated.
Includes	None
Extensions	None
Triggers	User's intent to adjust sensor sensitivities.

UC26 – Deactivate Burglar Alarm

ID	UC26
Actors	Security Guard, Senior Bank Staff
Name	Deactivate Burglar Alarm
Description	Authorised personnel deactivate the triggered burglar alarm.
Pre-conditions	The burglar alarm has been triggered.
Event flow	1. User approaches the system console. 2. User swipes a valid card and enters the correct code. 3. System validates the entered code and card. 4. Burglar alarm is deactivated.
Post-condition	Burglar alarm is inactive.
Includes	None
Extensions	None
Triggers	User's intent to deactivate the triggered burglar alarm.

UC27 – System Maintenance Check

ID	UC27
Actors	Maintenance Staff
Name	System Maintenance Check
Description	Regular maintenance checks of the security system are performed to ensure everything is functioning correctly.
Pre-conditions	The system is operational.
Event flow	1. Maintenance staff logs into the system.

	2. System diagnostics are initiated.
	3. Any faults or issues are identified and rectified.
	4. Maintenance log is updated.
Post-condition	System is in optimal working condition.
Includes	None
Extensions	None
Triggers	Scheduled maintenance or system error detection.

UC28 – Alert Police
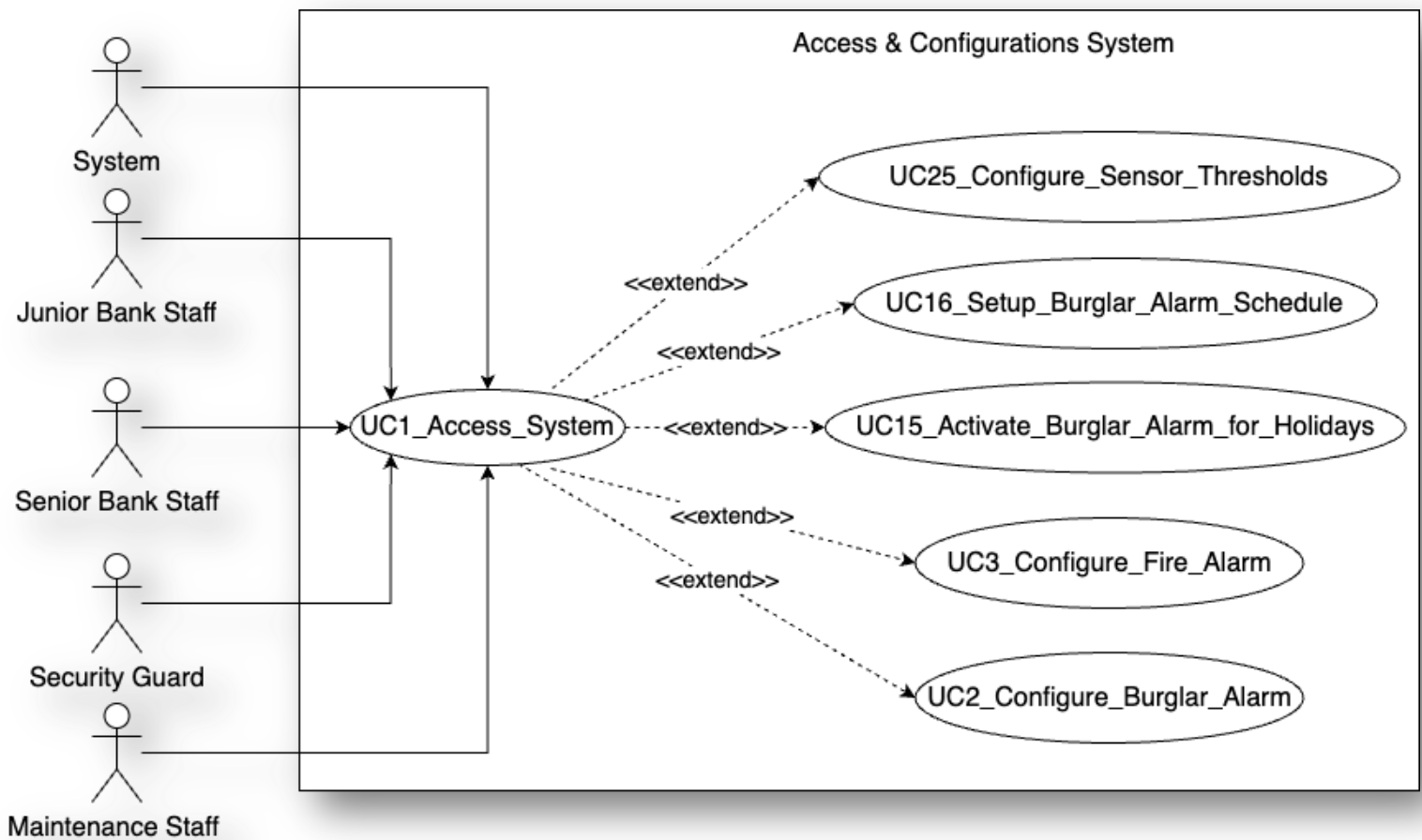
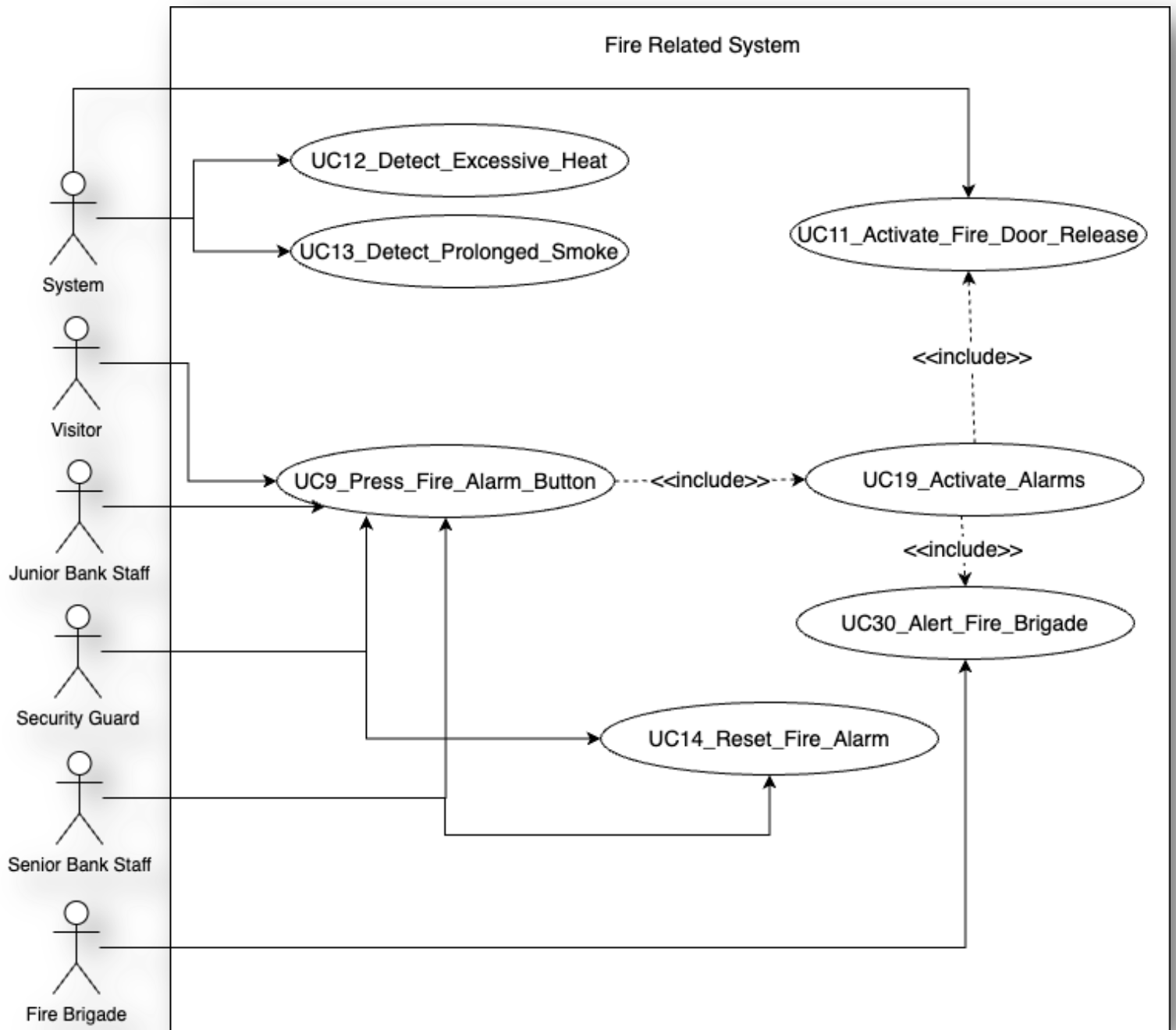| ID	UC28
Actors	System
Name	Alert Police
Description	The security system sends an automatic alert to the police in case of specific security breaches.
Pre-conditions	A security breach has been detected.
Event flow	1. The system identifies a condition that warrants police notification (e.g., multiple invalid access attempts, burglar alarm triggered, panic button pressed).
	2. The system sends an automatic alert to the police with relevant details (location, type of breach, timestamp).
Post-condition	Police have been notified of the security breach and can take appropriate action.
Includes	None
Extensions	None
Triggers	Specific conditions as defined in the system requirements, such as burglar alarm activation, panic button press, etc.

UC29 – Alert Fire Brigade

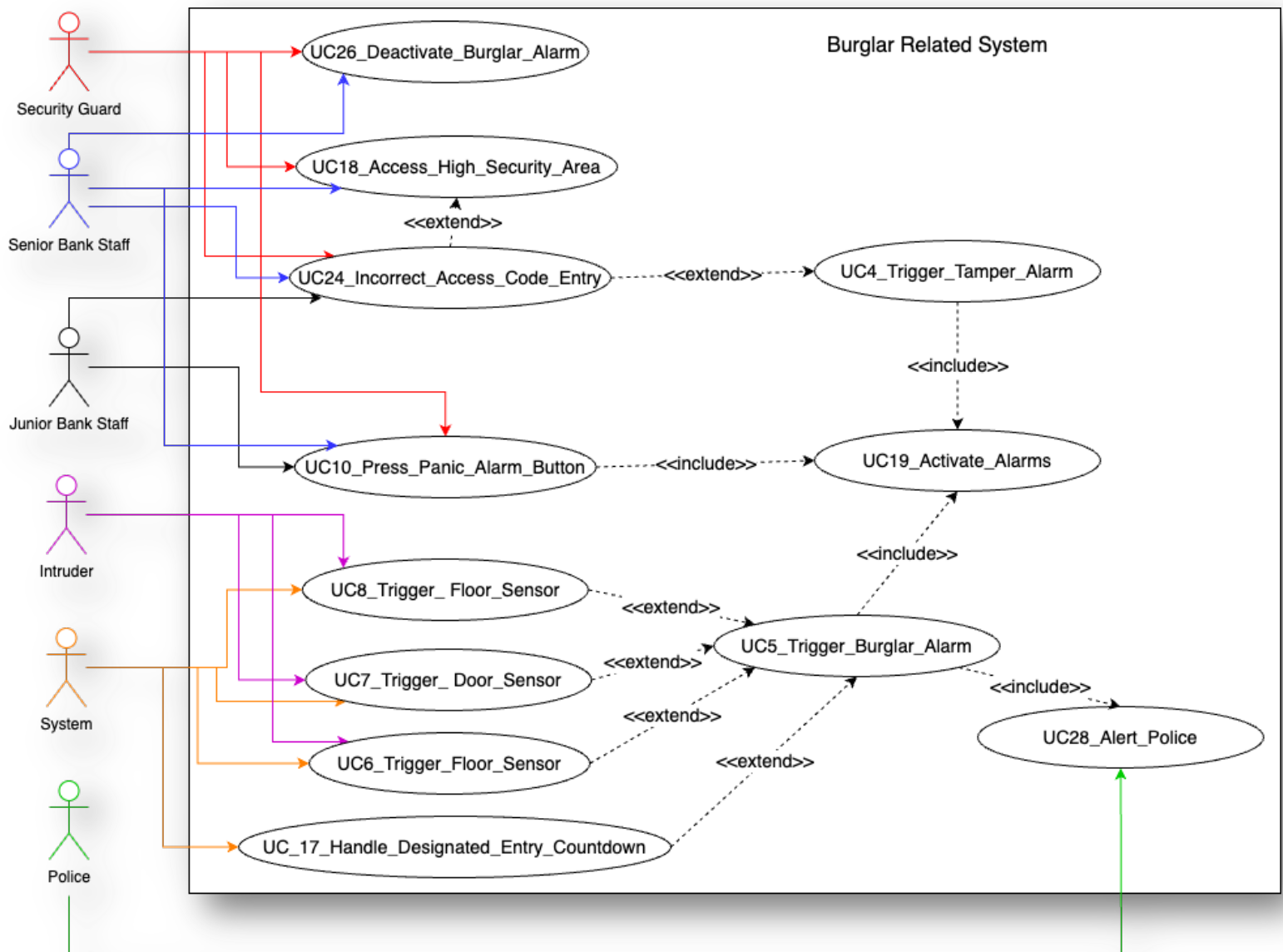| ID	UC29
Actors	System
Name	Alert Fire Brigade
Description	The security system sends an automatic alert to the fire brigade in case of fire-related emergencies.
Pre-conditions	A fire emergency has been detected.
Event flow	1. The system identifies a condition that warrants fire brigade notification (e.g., excessive heat, prolonged smoke detection).
	2. The system sends an automatic alert to the fire brigade with relevant details (location, type of fire emergency, timestamp).
Post-condition	The fire brigade has been notified of the fire emergency and can take appropriate action.
Includes	None
Extensions	None
Triggers	Specific conditions such as excessive heat detection, prolonged smoke detection, etc.

B) Use Case Diagram

Access & Configurations

Fire Related System
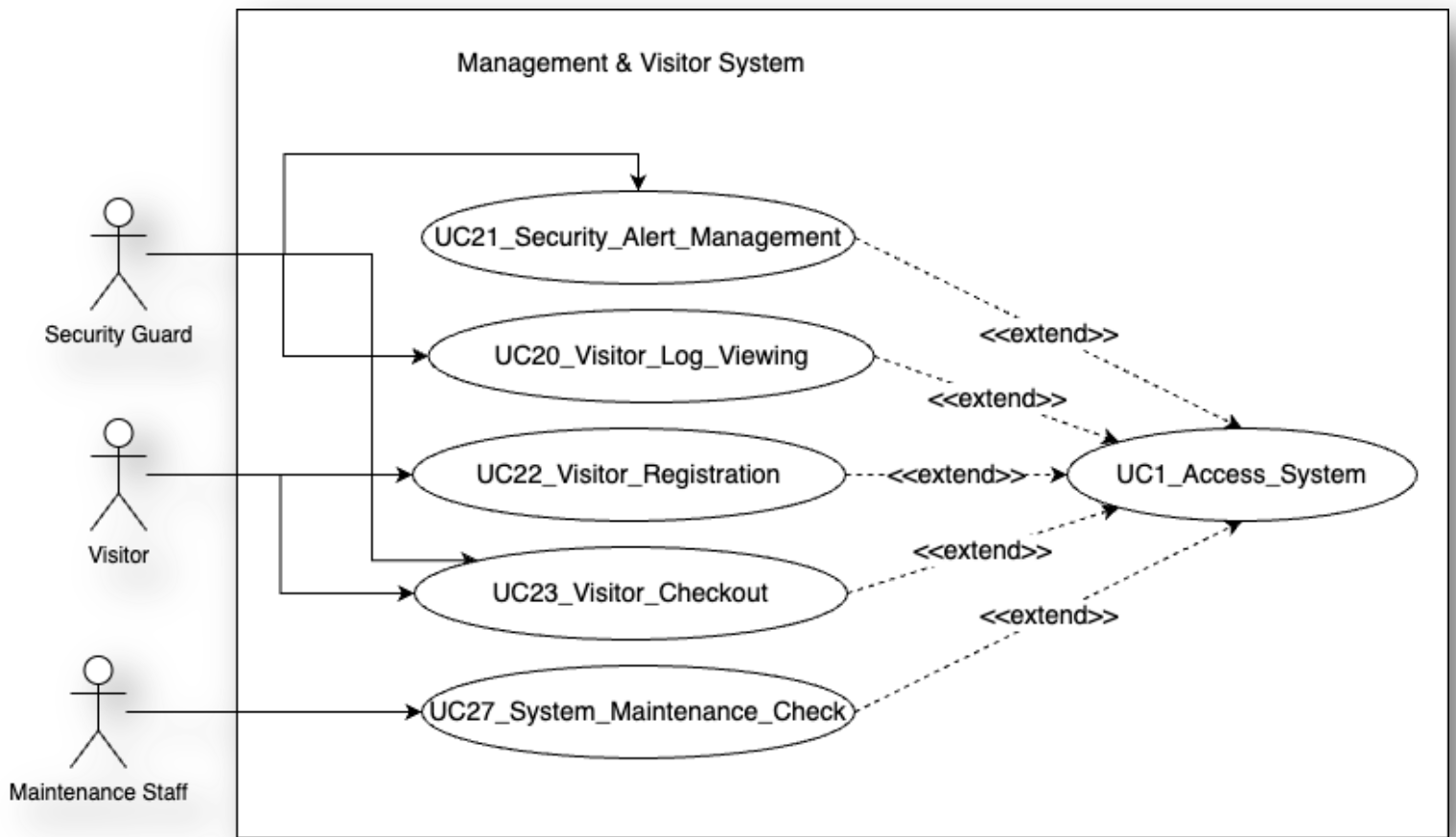
UC12_Detect_Excessive_Heat

UC13_Detect_Prolonged_Smoke

UC11_Activate_Fire_Door_Release

<<include>>

UC9_Press_Fire_Alarm_Button   <<include>>   UC19_Activate_Alarms

<<include>>

UC30_Alert_Fire_Brigade

UC14_Reset_Fire_Alarm

System

Visitor

Junior Bank Staff

Security Guard

Senior Bank Staff

Fire Brigade

Burglar Related System

Task 2

Here are ten non-functional requirements for the proposed building security system, each with an appropriate criterion for verification:

1) Response Time
Description: The system must respond to any sensor trigger (like door/window opening, or smoke detection) within 2 seconds.
Criterion for Verification: Test the system by triggering various sensors and measure the time it takes for the system to respond. This can be done using performance testing tools provided by the maintenance team.

2) Reliability
Description: The system should have an uptime of 99.9% annually.
Criterion for Verification: Monitor the system's uptime over a year and ensure it meets or exceeds 99.9%. This can be tracked using system monitoring tools.

3) Accessibility
Description: The system console should be easily accessible and usable by all bank employees regardless of physical disabilities.
Criterion for Verification: Conduct usability tests with a diverse group of bank employees, including those with physical disabilities, to ensure they can easily access and use the system console.

4) Scalability
Description: The system should support the addition of up to 100 more sensors without any degradation in performance.
Criterion for Verification: Simulate the addition of up to 100 sensors to the system and monitor its performance. This can be done in a test environment using load-testing tools.

5) Data Integrity
Description: In case of power failures, system settings and configurations should remain intact and not be lost.
Criterion for Verification: Intentionally cause power interruptions and then check if the system settings and configurations remain unchanged upon power restoration.

6) Backup
Description: The system must automatically backup its data and configurations at least once every 24 hours.
Criterion for Verification: Check the system's backup logs daily to ensure automatic backups are being taken. Additionally, periodically restore from a backup to ensure data integrity and completeness.

7) Security
Description: All data transactions, especially calls to fire brigade and police, should be encrypted using industry-standard encryption protocols.
Criterion for Verification: Conduct penetration testing and vulnerability assessments to ensure data transactions are encrypted and secure from potential threats.

8) Audibility

Description: The fire alarm bell and burglar alarm speaker should be audible in every part of the building.

Criterion for Verification: Trigger the alarms in various parts of the building and use sound level meters to ensure they are audible throughout.

9) Maintainability

Description: Any malfunctioning component of the system should be replaceable without shutting down the entire system.

Criterion for Verification: In a controlled environment, simulate a component malfunction and try replacing it. Check if the system continues to function without shutting down entirely.

10) Authentication

Description: After three consecutive failed login attempts, the system should lock the user out for at least 15 minutes to prevent brute-force attacks.

Criterion for Verification: Intentionally enter incorrect login credentials three times consecutively and observe if the system locks out the user for at least 15 minutes.

These requirements and their verification criteria will help ensure that the system is developed to meet the necessary standards and operates effectively in its intended environment.