

## **CRIMES AGAINST WOMEN**

### **PROJECT TRINETRA**

**(A Connected, Device-Independent Women's Safety and Rapid Response Network)**

**Submission by :**

MOUNISHA.T (URK25FS1022)

MAHIVARSHINI.P (URK25FS1020)

DHIVYADARSHINI .V(URK25FS1031)

KIRTHIVINYA (IRK25FS1029)

**2 year BSC FORENSIC SCIENCE, Karunya Institute Of Arts & Science**

**Academic Year: 2026-27**

**Semester: 3**

**Submitted to : Dr.P.G.Sunanda Bhagavathy**

**27th November 2026**



### **BONAFIDE CERTIFICATE**

This is to certify that the micro project e-report titled “**Violent crimes against women - TRINETRA (A Connected, Device-Independent Women’s Safety and Rapid Response Network)**” is the bonafide work of “MOUNISHA.T ,MAHIVARSHINI.P ,DHIVYADARSHINI.V,KIRTHIVINYA.I” who carried out the project work under my supervision.

Dr.P.G.Sunanda Bhagavathy

Professor

Division of Criminology and

Forensic Science, KITS,

Coimbatore

Submitted for the micro project presentation held on

## ABSTRACT

Women's safety in public places remains an important social and technological concern. Situations such as stalking, sexual harassment, physical assault, threats, and unsafe travel can occur when a person is alone or unable to access a mobile phone. Although emergency helplines, CCTV cameras, and mobile safety applications are available, these systems may operate separately, and a person experiencing danger may not always be able to use them.

**Project TRINETRA** proposes a connected, device-independent women's safety and rapid response network. The system combines physical SOS Safety Nodes installed at selected public locations with a digital platform monitored by trained operators. A person can request assistance by pressing a physical emergency button without needing a personal smartphone.

After receiving an alert, the operator can communicate with the person through the node, assess the situation, and coordinate appropriate assistance. Where authorised CCTV coverage is available, the system may support a request for camera review and record the last verified observation with its timestamp. The platform can also coordinate with authorised emergency services and support a safe-journey monitoring process when the individual voluntarily provides the necessary information.

The proposed system is designed to work alongside existing emergency services rather than replace them. It also considers privacy, consent, data security, affordability, and the limitations of CCTV coverage. The initial implementation can be demonstrated through a prototype using a simulated dashboard, a 3D Safety Node model, sample incident records, and a simulated response workflow.

Project TRINETRA aims to demonstrate how connected infrastructure and human-supervised technology can improve access to emergency assistance and support safer public spaces.

**Keywords:** Women's safety, SOS system, Safety Node, emergency response, CCTV coordination, crime prevention, digital platform, safe journey, forensic technology.

## TABLE OF CONTENTS

| S.No. | Title                                         |                                        | Page No. |
|-------|-----------------------------------------------|----------------------------------------|----------|
|       | BONAFIDE CERTIFICATE                          |                                        | ii       |
|       | ABSTRACT                                      |                                        | iii      |
|       | TABLE OF CONTENTS                             |                                        | iv       |
| 1     | INTRODUCTION                                  |                                        | 1        |
|       | 1.1                                           | Background of the selected problem     | 1        |
|       | 1.2                                           | Industry Relevance                     | 1        |
|       | 1.3                                           | Aim and Objective of the Micro Project | 2        |
|       | 1.4                                           | Link to SDG / KITS Technology Mission  | 2        |
| 2     | LITERATURE REVIEW                             |                                        | 3        |
| 3     | METHODOLOGY                                   |                                        | 6        |
| 4     | FABRICATION/SIMULATION/PROGRAM OR CODE/DESIGN |                                        | 9        |
| 5     | RESULTS AND INTERPRETATION                    |                                        | 12       |
| 6     | CONCLUSION AND FUTIRE SCOPE                   |                                        | 15       |
| 7     | DECLARATION                                   |                                        | 16       |

## CHAPTER 1: INTRODUCTION

### 1.1 Background of the Project

Women's safety is an important concern in modern society. Women may experience harassment, stalking, threats, physical assault, and other unsafe situations in public places such as streets, bus stops, railway stations, parking areas, and isolated walking routes. In such situations, immediate access to assistance can make a significant difference.

Mobile phones and emergency applications can help people request assistance. However, these options may not always be available. A person may have a discharged phone battery, poor network connectivity, no smartphone, or may be unable to unlock and use a device during an emergency.

Public CCTV cameras can support the observation and investigation of incidents, but their usefulness depends on camera coverage, image quality, access permissions, and the availability of trained personnel. Similarly, emergency helplines depend on a person being able to contact the service and communicate the relevant information.

Project TRINETRA proposes a connected safety system that brings these elements together through physical emergency devices, a digital monitoring platform, and coordinated response procedures.

The main idea is to install **physical SOS Safety Nodes at selected public locations**. These nodes would allow a person to request help by pressing an emergency button. The alert would reach a central digital platform, where a trained operator could assess the situation and coordinate appropriate assistance.

If the person needs immediate support, the operator could communicate through the node and coordinate with authorised emergency services. Where permitted and technically possible, authorised CCTV operators could review relevant camera footage and provide a verified observation of the person's last known location.

The system could also include a Safe Journey Manager that allows a person to voluntarily provide a destination and receive check-ins or assistance until reaching the intended location.

TRINETRA is proposed as a supportive public safety network rather than a replacement for existing emergency helplines, police services, or other official emergency systems.

## **Need for the Project**

The proposed system addresses several practical concerns:

1. A person may not have access to a mobile phone during an emergency.
2. A person may be unable to make a phone call or explain the situation clearly.
3. Existing emergency devices, CCTV systems, and response services may operate separately.
4. Some public locations may have limited access to emergency assistance.
5. Emergency responders may need verified information about the incident location.
6. A person travelling alone may benefit from a structured check-in and safe-arrival process.

By combining physical access points with a digital coordination platform, TRINETRA aims to make requesting assistance more accessible and improve communication between the person in danger and the response team.

## **1.2 Industry Relevance**

Project TRINETRA has relevance to public safety, smart-city infrastructure, emergency management, and digital forensic support.

### **A. Public Safety Infrastructure**

Physical SOS nodes can provide an additional way to request help in public spaces. They may be particularly useful at selected pedestrian routes, transport facilities, public parks, parking areas, and other locations identified through safety assessments.

### **B. Smart-City Technology**

The proposed system uses connected devices and a digital dashboard to manage emergency alerts, record incidents, and coordinate authorised services. This approach is relevant to smart-city initiatives that aim to improve the management of public infrastructure through technology.

### **C. Emergency Response Management**

A central platform can help operators record incoming alerts, assess urgency, assign response tasks, and track the progress of an incident. This may improve coordination and reduce confusion during emergencies.

### **D. CCTV and Forensic Support**

Where authorised access is available, CCTV review may help establish a person's last verified observation or support the reconstruction of an incident timeline.

Such information can be relevant to later investigation. However, CCTV footage must be interpreted carefully, and the system must not claim continuous tracking when cameras do not cover the person's route.

### **E. Digital Case Management**

The platform can maintain incident records, including the alert time, node identification, operator actions, response assignment, and closure details. These records may support administrative review and incident analysis.

Any information used for criminal investigation must be handled according to applicable legal requirements and evidence-handling procedures.

### **F. Cost-Effective Implementation**

The system can initially be developed as a small pilot project using a limited number of Safety Nodes and a simulated digital platform. If implemented in a real city, it could seek to use existing authorised CCTV infrastructure and emergency services rather than building an entirely separate network.

Actual integration would require approval, technical compatibility, operational agreements, and adequate funding.

### **1.3 Aim and Objectives**

#### **Aim**

To design a connected, device-independent women's safety and rapid response network that enables individuals to request emergency assistance through physical SOS nodes and supports coordinated response through a digital monitoring platform.

#### **Objectives**

1. To design a physical Safety Node with an easily accessible SOS button.
2. To develop a proposed digital platform for receiving and managing emergency alerts.
3. To enable communication between the person requesting help and a trained operator.
4. To propose a system for coordinating authorised CCTV review when relevant coverage is available.
5. To design a response coordination module for assigning and monitoring assistance.
6. To develop a Safe Journey Manager for voluntary journey registration, check-ins, and safe-arrival confirmation.
7. To provide a device-independent method of requesting assistance without requiring a personal smartphone.
8. To propose incident records and reporting functions for administrative review.
9. To consider privacy, consent, cybersecurity, and responsible data management.
10. To evaluate the proposed design through a prototype demonstration and a structured testing plan.

### **1.4 Link to Sustainable Development Goals and Technology Mission**

Project TRINETRA is connected to broader efforts to improve public safety through technology and coordinated public services.

#### **A. Sustainable Development Goal 5: Gender Equality**

The project supports the broader objective of gender equality by proposing an additional way for women to seek assistance in unsafe situations. It focuses on improving access to support rather than placing the responsibility for preventing crime solely on women.

#### **B. Sustainable Development Goal 11: Sustainable Cities and Communities**

The proposed Safety Nodes and digital coordination platform are relevant to the development of

safer and more inclusive public spaces.

The project encourages public authorities to identify vulnerable locations and consider safety infrastructure as part of urban planning.

### **C. Sustainable Development Goal 16: Peace, Justice and Strong Institutions**

The proposed system supports the broader aims of effective public institutions and access to assistance by creating structured incident records and a defined response workflow.

Its successful implementation would depend on transparent procedures, appropriate oversight, and cooperation with authorised authorities.

### **D. Technology Mission and Smart-City Approach**

TRINETRA follows a technology-enabled public service approach by combining connected devices, digital incident management, communication systems, and authorised surveillance coordination.

The proposed system could complement smart-city infrastructure, integrated command and control centres, and existing emergency response services.

However, TRINETRA is a proposed project concept. It should not be represented as an officially approved government mission or as an already integrated public safety service.

## **CHAPTER 2: LITERATURE REVIEW**

### **2.1 Existing Emergency Response Systems**

Emergency response systems allow individuals to contact authorised services when they face immediate danger or require urgent assistance.

In India, the Emergency Response Support System uses the emergency number **112** to provide access to emergency assistance. Existing services provide an important foundation for public safety.

However, a person may sometimes find it difficult to make a call, provide an exact location, or communicate during a stressful incident.

A physical SOS node could provide an additional access point through which an alert is raised. The proposed TRINETRA platform would then help manage the incident and coordinate assistance.

The intention is to complement existing emergency systems rather than replace them.

### **2.2 CCTV Surveillance and Public Safety**

CCTV cameras are used in public places for security monitoring, incident review, and investigation support.

Depending on camera placement and image quality, CCTV footage may help establish what happened at a particular location and time. It may also help investigators identify the direction in which a person travelled or locate relevant events in a recorded timeline.

However, CCTV systems have limitations:

- Not all locations have camera coverage.
- Camera angles may not capture every activity.
- Image quality may be poor in darkness or adverse weather.
- Footage may not be available immediately.
- Access may require authorisation.
- A person may leave the area covered by the cameras.

For these reasons, TRINETRA proposes a **CCTV Coordination Module** rather than claiming uninterrupted tracking.

When an authorised CCTV operator confirms an observation, the platform should record the camera reference, observation time, and verification status. If no verified observation is available, the dashboard should clearly display that information.

### 2.3 Device-Independent Emergency Assistance

Many personal safety systems depend on a smartphone, a mobile application, or a wearable device.

Although these tools can be useful, they may not work for every individual or every emergency.

A physical Safety Node provides an alternative method of requesting assistance. A person can press a button without needing to own a smartphone or install an application.

The proposed node may include:

- A clearly marked SOS button.
- A microphone and speaker.
- A unique node identification number.
- Registered location information.
- A communication module.
- A visible status indicator.
- Backup power.
- An optional camera, subject to legal and privacy requirements.

This design aims to make emergency assistance more accessible to people who cannot use a personal device.

## **2.4 Human-Supervised Emergency Response**

Technology can help collect information and manage incidents, but emergency situations often require human judgement.

A trained operator can communicate with the person requesting help, ask relevant questions, identify the immediate concern, and coordinate the next steps.

For example, the operator may need to determine whether the person is injured, being followed, unable to leave a location, or seeking assistance to reach a safer public place.

The proposed TRINETRA system therefore includes a central control platform staffed by trained personnel.

The operator would follow established procedures and coordinate with authorised emergency services when necessary. The system would not automatically determine guilt or treat an unverified report as proof that a crime has occurred.

## **2.5 Privacy and Data Protection**

A public safety platform may handle sensitive information, including incident reports, audio communication, CCTV references, journey details, and contact information.

If this information is not handled responsibly, it could expose individuals to additional risks.

Privacy protection should therefore be part of the system design.

The proposed safeguards include:

1. Access to incident records based on authorised roles.
2. Collection of only the information necessary for the incident.
3. Secure transmission and storage of sensitive information.
4. Records of access to incident information.
5. Defined retention and deletion procedures.
6. Consent for voluntary journey monitoring and non-emergency sharing.
7. Appropriate restrictions on the disclosure of personal information.
8. Human review before sensitive information is shared.
9. Procedures for correcting inaccurate incident records.
10. Compliance with applicable laws and authorised operational policies.

Emergency handling must also follow applicable legal requirements. The system should not delay necessary emergency assistance while seeking optional information that is not essential to the response.

## **2.6 Research Gap and Proposed Solution**

The proposed project identifies a practical design gap between emergency access, incident management, CCTV coordination, and response follow-up.

Physical emergency buttons, emergency helplines, CCTV systems, and safety applications may each serve useful purposes. However, a person experiencing danger may still face difficulties accessing assistance, communicating their situation, or receiving coordinated support.

TRINETRA proposes to address this design gap through a connected workflow.

The main features of the proposed solution are:

- Physical SOS access without a personal smartphone.
- A central dashboard for managing emergency alerts.
- Two-way communication between the operator and the person requesting assistance.
- Authorised CCTV coordination where coverage is available.
- Response assignment and status tracking.
- Voluntary safe-journey monitoring.
- Incident closure and administrative reporting.
- Privacy-conscious handling of sensitive information.

The project does not claim that these features are entirely new individually. Its proposed contribution is to bring them together within one coordinated design and demonstrate how the workflow could operate.

## **CHAPTER 3: METHODOLOGY**

### **3.1 Requirement Analysis**

Requirement analysis was conducted conceptually to identify the basic needs of the proposed system.

The requirements were divided into functional and non-functional requirements.

#### **A. Functional Requirements**

The proposed system should be able to:

1. Register Safety Nodes and their approved installation locations.
2. Receive an SOS alert from a registered node.
3. Display the alert on the central dashboard.
4. Record the time and node identification number.
5. Allow an operator to acknowledge the alert.
6. Support two-way communication with the person requesting help.
7. Record incident details and operator actions.
8. Request authorised CCTV review when relevant.
9. Display verified observations with timestamps.
10. Assign and monitor response tasks.
11. Support voluntary journey check-ins.
12. Record safe-arrival confirmation where applicable.
13. Close incidents with a documented outcome.

14. Generate administrative reports for authorised users.

## **B. Non-Functional Requirements**

The system should aim to provide:

- **Accessibility:** The SOS button should be easy to locate and operate.
- **Reliability:** The node and platform should have suitable fault monitoring and backup arrangements.
- **Security:** Sensitive information should be protected from unauthorised access.
- **Usability:** The interface should be understandable during urgent situations.
- **Scalability:** Additional nodes should be capable of being registered as the network expands.
- **Maintainability:** Devices and software should be regularly inspected and updated.
- **Privacy:** Personal data should be collected and shared only when justified and authorised.
- **Transparency:** The platform should distinguish verified information from unconfirmed reports and simulations.

## **C. Hardware Requirements**

The proposed physical node may require:

- SOS push button.
- Microphone and speaker.
- Communication module.
- Controller or embedded computing unit.
- Status indicator.
- Power supply and backup battery.
- Protective enclosure.
- Unique node identification label.
- Optional camera, where justified and authorised.

The exact components would depend on the final design, budget, environmental conditions, and communication method.

## **D. Software Requirements**

A digital prototype may use:

- HTML, CSS, and JavaScript or React for the user interface.
- Python with FastAPI or Node.js for backend functions.
- SQLite for a small demonstration or PostgreSQL for a larger implementation.
- A schematic map or mapping interface for displaying node locations.
- A local development environment for testing.

These technologies are proposed options. The final implementation should use the tools actually selected and tested by the project developer.

### **3.2 Proposed System Architecture**

The proposed TRINETRA architecture contains five main components.

#### **1. Physical Safety Nodes**

Safety Nodes are installed at selected public locations. Each node has a unique identification number and a registered location.

When a person presses the SOS button, the node sends an alert to the digital platform through the available communication system.

The node may also allow two-way audio communication so that the person can speak with an operator.

#### **2. Digital Monitoring Platform**

The digital platform receives alerts and displays them on an incident management dashboard.

It records the alert time, node identification, incident status, operator actions, and response progress.

The dashboard helps the operator manage incidents systematically rather than relying entirely on informal communication.

#### **3. CCTV Coordination Module**

This module supports requests for authorised CCTV review.

Where relevant camera coverage is available, an authorised operator can review footage and report a verified observation.

The system should distinguish between:

- Confirmed observations.
- Unconfirmed information.
- Pending CCTV review.
- No available camera coverage.
- Simulated information used in a demonstration.

The module must not claim continuous location tracking when such tracking is not technically available.

#### **4. Rapid Response Coordination Module**

This module records the response assigned to an incident and tracks the progress of the response.

Depending on the circumstances, assistance may involve authorised police personnel, emergency

medical services, or other approved support services.

Actual dispatch integration would require formal authorisation and technical coordination. A student prototype should demonstrate this process through simulated assignments unless a genuine authorised connection exists.

## **5. Safe Journey Manager**

The Safe Journey Manager supports individuals who voluntarily request journey monitoring.

A user may provide a destination, select a check-in arrangement, and confirm safe arrival.

If a check-in is missed, the system can follow a defined procedure, such as sending an agreed notification or initiating a follow-up call where consent and operational arrangements permit.

The system should not automatically assume that a missed check-in means a crime has occurred.

### **Proposed Architecture Diagram**

**Insert the system architecture diagram here.**

The diagram should show the following connections:

Safety Node → Digital Monitoring Platform → Control Centre Operator → CCTV Coordination, where authorised → Response Coordination → Safe-Arrival Confirmation and Incident Closure.

## **3.3 Working Procedure**

The proposed working procedure consists of the following steps.

### **Step 1: Installation and Registration**

Each Safety Node is assigned a unique identification number. Its installation location, maintenance details, and operational status are entered into the system.

### **Step 2: Emergency Alert**

When a person experiences danger, they press the SOS button.

The node sends an alert to the platform through the configured communication system.

### **Step 3: Alert Acknowledgement**

The dashboard displays the incoming alert, including the registered node location and alert time.

A trained operator acknowledges the incident and begins the response process.

### **Step 4: Communication with the Person**

The operator attempts to establish two-way communication through the node.

The operator asks relevant questions, assesses the urgency, and identifies the assistance required.

If the person cannot speak, the operator follows an approved procedure for assessing and escalating the alert.

#### **Step 5: Incident Assessment**

The operator records the information available and categorises the incident according to the organisation's approved procedure.

The system should allow uncertain information to remain marked as unverified.

#### **Step 6: CCTV Coordination**

If CCTV review may help and the required authorisation is available, the operator requests a review from the relevant CCTV control room.

Any verified observation is recorded with the observation time and source information.

#### **Step 7: Response Coordination**

The operator coordinates appropriate assistance through authorised channels.

The digital platform records the assignment, response status, and any relevant updates.

#### **Step 8: Safe Destination or Journey Support**

Where appropriate, the operator may help the person identify a safer public location or coordinate assistance to reach one.

If the person has voluntarily registered a journey, the Safe Journey Manager records check-ins and the safe-arrival status.

#### **Step 9: Incident Closure**

After the incident has been handled, the operator records the outcome, actions taken, and any necessary follow-up.

The incident is then marked as closed or referred for further action.

### **3.4 System Workflow and Algorithm**

The following algorithm describes the proposed process.

#### **Algorithm: TRINETRA Emergency Response**

1. Start the system.
2. Monitor registered Safety Nodes.
3. Check whether an SOS button has been activated.
4. If no alert is received, continue monitoring.
5. If an alert is received, record the node ID and alert time.
6. Display the alert on the dashboard.
7. Assign the alert to an available authorised operator.
8. Attempt two-way communication with the person.
9. Assess the reported situation and determine the required level of response.
10. If relevant and authorised, request CCTV review.
11. Record only verified CCTV observations with timestamps.
12. Coordinate appropriate assistance through authorised channels.
13. Update the incident status as information becomes available.
14. If journey monitoring applies, record check-ins and safe-arrival confirmation.
15. Record the final outcome and any required follow-up.
16. Close or refer the incident according to the approved procedure.
17. End the incident workflow.

**Note:** The algorithm describes the intended operation of the proposed system. It should not be presented as a fully functioning emergency dispatch system unless each function has been implemented and tested.

### **3.5 Proposed Safety Node Placement**

The placement of Safety Nodes is an important part of the proposed network.

Nodes should be located according to a safety assessment rather than being installed at equal distances without considering local conditions.

Factors to consider include:

- Pedestrian movement.
- Previous incident reports, where reliable and lawfully available.
- Street lighting.
- Public transport access.
- Isolated walking routes.
- Public parks and parking areas.
- Existing emergency infrastructure.
- Network connectivity.
- Accessibility for people with disabilities.
- Availability of electricity and maintenance access.

### **Preliminary Spacing Proposal**

For the initial project design, the following spacing ranges may be considered.

| Location type                                              | Preliminary spacing proposal | Reason                                                      |
|------------------------------------------------------------|------------------------------|-------------------------------------------------------------|
| Selected standard pedestrian routes                        | Approximately 250 m          | Provides planned access points along the route              |
| Isolated or poorly connected routes                        | Approximately 150–250 m      | May reduce the distance to the nearest node                 |
| Locations identified as higher priority through assessment | Approximately 100–200 m      | Allows denser placement where justified                     |
| Busy, well-lit streets with existing infrastructure        | Approximately 250–400 m      | May be suitable where other safety facilities are available |

These distances are **preliminary design targets for the project, not official standards or proven optimal distances**. A real installation would require site surveys, local risk assessment, engineering review, accessibility assessment, and budget analysis.

CCTV coverage must be assessed separately because the spacing of Safety Nodes does not guarantee camera coverage.

## CHAPTER 4: FABRICATION, SIMULATION, PROGRAMMING AND DESIGN

### 4.1 Physical Safety Node Design

The physical Safety Node is the main public-facing component of Project TRINETRA.

Its purpose is to provide a simple and accessible way to request emergency assistance.



Figure 4.1: Proposed three-dimensional design of the Project TRINETRA Safety Node.

## Proposed Components

### 1. SOS Button

The node should have a large, clearly labelled emergency button that is easy to identify and operate.

The button should be designed to reduce accidental activation while remaining usable during stressful situations.

### 2. Microphone

A microphone allows the person to communicate with the control centre.

### 3. Speaker

A speaker allows the operator to respond and provide instructions or reassurance.

### 4. Communication Module

The communication module transmits the emergency alert to the central platform.

The selected communication method would depend on network availability, cost, reliability, and the intended installation environment.

## **5. Status Indicator**

A status indicator may show whether the node is operational, processing an alert, or experiencing a fault.

The indicator should be understandable and should not expose sensitive incident information.

## **6. Backup Power**

A backup power supply can help the node remain operational during a temporary power interruption. Its actual backup duration would depend on the hardware and power requirements.

## **7. Node Identification**

Each node should have a unique identification number and a clearly recorded installation location.

## **8. Protective Enclosure**

The enclosure should be designed to withstand normal outdoor conditions and reduce the risk of damage or tampering.

## **9. Optional Camera**

A camera may be considered where it is justified and legally authorised. It should not be assumed to be necessary at every node.

Camera use must follow applicable privacy, security, and public surveillance requirements.

## **Working Principle**

When a person presses the SOS button, the node generates an emergency alert containing the node identification and relevant registered location information.

The platform receives the alert and notifies the operator.

The operator then attempts to communicate with the person and coordinates appropriate assistance.

The actual device would need to be engineered and tested for reliability, weather resistance, electrical safety, communication performance, and accessibility.

## **4.2 Digital Platform Design**

The digital platform is the central software component of TRINETRA.

It provides a common interface for managing emergency alerts, recording incidents, coordinating authorised CCTV review, and tracking response progress.

### **Module 1: Main Dashboard**

The dashboard displays the current operational status of registered nodes and the incidents being handled.

It may show:

- Total registered nodes.
- Operational and faulty nodes.
- Active incidents.
- Alerts awaiting acknowledgement.
- Incidents under review.
- Response assignments.
- Recently closed incidents.

All displayed figures should come from actual prototype data or be clearly labelled as sample data.

### **Module 2: Incident Management**

This module stores incident details and tracks each incident through its lifecycle.

The incident record may include:

- Incident ID.
- Alert date and time.
- Node ID.
- Registered node location.
- Incident category.
- Assigned operator.
- Current status.
- Actions taken.
- Response assignment.
- Closure details.

The module should distinguish reported information from information that has been independently verified.

### **Module 3: Live Communication**

This module represents the communication process between the person requesting help and the operator.

In a basic prototype, the interface may show communication status such as:

- Connection requested.
- Operator attempting contact.
- Communication established.
- Communication unavailable.
- Follow-up required.

If actual audio communication has not been implemented, these statuses must be demonstrated as simulated interface functions.

#### **Module 4: CCTV Coordination**

This module records requests for authorised CCTV review.

Its interface may include:

- Incident reference.
- Requested camera or area.
- Request status.
- Reviewing authority.
- Verified observation.
- Observation timestamp.
- Review notes.

The system should not display invented live locations or pretend to connect to real CCTV networks.

#### **Module 5: Rapid Response Coordination**

This module records the response action assigned to an incident.

It may show:

- Response required.
- Assistance requested.
- Assignment pending.
- Response assigned.
- Response in progress.
- Assistance completed.
- Further action required.

These are proposed workflow states. Actual integration with police or emergency dispatch systems would require approval and technical arrangements.

#### **Module 6: Safe Journey Manager**

This module supports voluntary journey monitoring.

It may allow a person to register a destination, choose check-in intervals, and confirm safe

arrival.

If a check-in is missed, the platform follows the agreed follow-up procedure.

The module must avoid treating a missed check-in as proof of an emergency.

### **Module 7: Safe Destination Directory**

This module can maintain a verified directory of suitable support locations, subject to agreements with the relevant organisations.

Potential entries may include:

- Police stations.
- Approved help centres.
- Participating public facilities.
- Authorised emergency service locations.
- Other verified support centres.

The platform should display accurate opening hours and service availability where these details are maintained.

### **Module 8: Safety Node Management**

This module manages information about registered nodes.

It may include:

- Node ID.
- Installation location.
- Installation date.
- Operational status.
- Last maintenance date.
- Fault reports.
- Maintenance history.

### **Module 9: Notifications**

This module manages notifications related to incidents, assignments, maintenance, and journey check-ins.

Notifications should be sent only to appropriate recipients and should avoid exposing sensitive details unnecessarily.

### **Module 10: Missing-Person Assistance**

This module may support authorised missing-person procedures by recording relevant information and coordinating approved CCTV review.

Access to personal details and the sharing of information must follow applicable laws and official procedures.

The system must not treat ordinary movement patterns or an individual's presence at a location as evidence of wrongdoing.

### **Module 11: Cybercrime Referral Support**

The platform may provide information about official cybercrime reporting channels and help users reach appropriate services.

It cannot independently detect most online offences simply through a physical SOS node. Its role in cybercrime cases would mainly involve referral, support, and incident documentation where appropriate.

### **Module 12: Reports and Analytics**

The reporting module may generate summaries of:

- Number of alerts received.
- Average acknowledgement time.
- Types of incidents reported.
- Node faults and maintenance needs.
- Response status.
- Incident closure status.
- Safe-journey completion.
- Areas requiring further assessment.

Reports should use only data that the project is authorised to process.

### **Module 13: Control Centre Management**

This module supports authorised operator accounts, role assignment, access control, and review of system activity.

It may also maintain records of operator actions to support accountability.

### **Module 14: Privacy and Access Control**

This module manages access to sensitive information.

It should support role-based permissions, access logs, secure authentication, and defined data retention procedures.

The prototype should demonstrate that different users receive only the access necessary for their assigned responsibilities.

## **4.3 Database and User Roles**

The proposed platform requires a structured method of storing information.

For a prototype, a small database may be sufficient. A larger deployment would require more detailed security, availability, and backup arrangements.

### Proposed Database Tables

| Table name           | Purpose                                          | Example fields                                         |
|----------------------|--------------------------------------------------|--------------------------------------------------------|
| Users                | Stores authorised user accounts                  | User ID, role, account status                          |
| Safety Nodes         | Stores registered node information               | Node ID, location, operational status                  |
| Incidents            | Stores emergency incident records                | Incident ID, node ID, time, category, status           |
| Communications       | Records communication status and permitted notes | Communication ID, incident ID, time, status            |
| CCTV Requests        | Records authorised CCTV review requests          | Request ID, incident ID, request status                |
| Observations         | Stores verified observations                     | Observation ID, source, timestamp, verification status |
| Response Assignments | Tracks assigned response tasks                   | Assignment ID, incident ID, status                     |
| Safe Journeys        | Stores voluntary journey details                 | Journey ID, destination, check-in status               |
| Maintenance          | Records node inspections and faults              | Maintenance ID, node ID, date, action                  |
| Audit Logs           | Records relevant system activity                 | Log ID, user ID, action, timestamp                     |

These are proposed database structures. The final schema should reflect the functions actually implemented.

### **Proposed User Roles**

#### **1. Administrator**

Manages system settings, authorised accounts, and node registration.

#### **2. Control Centre Operator**

Receives alerts, communicates with the person requesting assistance, and records incident actions.

#### **3. CCTV Liaison Officer**

Coordinates authorised CCTV review and records verified observations.

#### **4. Response Coordinator**

Tracks response assignments and updates the incident status.

#### **5. Maintenance Officer**

Checks node functionality and records faults or repairs.

#### **6. Auditor or Supervisor**

Reviews permitted records and system activity for quality assurance and accountability.

Role separation helps reduce unnecessary access to sensitive information.

### **4.4 Prototype Demonstration and Testing**

The initial prototype is intended to demonstrate the proposed workflow rather than claim a complete operational emergency network.

The prototype can include a 3D Safety Node model, a digital dashboard, sample incident records, and a simulated response process.

### **Proposed Demonstration Steps**

#### **Step 1: Register a Safety Node**

Create a sample node record with a unique ID and a clearly identified demonstration location.

#### **Step 2: Trigger a Test Alert**

Activate a simulated SOS event.

The dashboard should display the node ID, alert time, and incident status.

### **Step 3: Acknowledge the Alert**

The operator acknowledges the alert and the system records the action.

### **Step 4: Demonstrate Communication Status**

The interface displays whether communication is pending, established, or unavailable.

If no actual audio hardware is connected, the demonstration must be labelled as simulated.

### **Step 5: Demonstrate CCTV Coordination**

Create a sample CCTV review request.

The demonstration may show a sample verified observation with a timestamp, but the data must be clearly identified as demonstration data.

### **Step 6: Assign a Response**

Assign a simulated response task and update its status.

Do not imply that a real police unit or emergency service has been dispatched unless this has actually occurred through an authorised integration.

### **Step 7: Demonstrate Safe Journey Monitoring**

Create a voluntary test journey, record a sample check-in, and mark safe arrival.

### **Step 8: Close the Incident**

Record the demonstration outcome and close the test incident.

### **Step 9: Review the Record**

Confirm that the alert, operator actions, updates, and closure information appear correctly in the incident record.

### **Prototype Testing Checklist**

- Safety Node appears in the node register.
- Test alert is received by the dashboard.
- Alert time and node ID are recorded correctly.
- Operator acknowledgement updates the incident status.
- Communication status is displayed correctly.
- CCTV request status is recorded.
- Verified observations are distinguishable from unverified data.
- Response assignment can be created and updated.

- Safe-journey check-in can be recorded.
- Safe-arrival status can be recorded.
- Incident closure is saved.
- Unauthorised users cannot access restricted functions.
- Simulated data is clearly labelled.

**Important:** Include only tests that have actually been performed in the final report. If a feature is planned but not implemented, describe it as a proposed feature.

## **CHAPTER 5: RESULTS AND INTERPRETATION**

### **5.1 Proposed Testing Procedure**

The proposed prototype can be evaluated through a series of controlled tests.

The purpose of testing is to determine whether the designed interface and workflow perform the functions expected of them.

#### **Test 1: Safety Node Registration**

**Procedure:** Enter the node ID, location, and operational status into the system.

**Expected observation:** The node appears in the node register with the correct details.

#### **Test 2: SOS Alert**

**Procedure:** Trigger a simulated SOS alert from a registered node.

**Expected observation:** The dashboard displays the incident and records the alert time.

#### **Test 3: Alert Acknowledgement**

**Procedure:** Assign the alert to an operator and acknowledge it.

**Expected observation:** The incident status changes according to the defined workflow.

#### **Test 4: Communication Status**

**Procedure:** Demonstrate the communication status function.

**Expected observation:** The system records whether communication is pending, established, or unavailable.

#### **Test 5: CCTV Coordination**

**Procedure:** Create a CCTV review request using sample demonstration data.

**Expected observation:** The request status and any sample observation are displayed with the appropriate timestamp and verification label.

#### **Test 6: Response Assignment**

**Procedure:** Create a simulated response assignment and update its status.

**Expected observation:** The dashboard displays the assignment and its current status.

#### **Test 7: Safe Journey**

**Procedure:** Register a sample journey, record a check-in, and confirm safe arrival.

**Expected observation:** The journey status updates correctly.

#### **Test 8: Incident Closure**

**Procedure:** Enter the final outcome of the test incident and close it.

**Expected observation:** The incident record retains the required information and displays the correct closure status.

#### **Test 9: Access Control**

**Procedure:** Test the application using different authorised roles.

**Expected observation:** Each role can access only the functions permitted by its assigned permissions.

#### **Test 10: Fault and Error Handling**

**Procedure:** Simulate an unavailable communication connection or an incorrectly entered record.

**Expected observation:** The system displays an appropriate status or error message instead of silently treating the operation as successful.

### **5.2 Expected Results**

The proposed TRINETRA design is expected to demonstrate the following functions when implemented and tested successfully.

1. A registered Safety Node can initiate a test alert.
2. The dashboard can display the alert and its associated node information.
3. The system can record the acknowledgement and subsequent incident updates.
4. The interface can support a structured communication workflow.
5. CCTV requests and observations can be recorded separately from unverified information.
6. Response assignments can be tracked through defined status changes.
7. A voluntary journey can be monitored through recorded check-ins.

8. The system can record safe-arrival confirmation and incident closure.
9. User permissions can help restrict access to sensitive functions.
10. Incident records can support administrative review and evaluation.

These are **expected results**, not confirmed experimental findings. They should be changed to actual results after the prototype has been tested.

**Results Table**

| S. No. | Test performed        | Expected result                       | Actual observation           | Status  |
|--------|-----------------------|---------------------------------------|------------------------------|---------|
| 1      | Node registration     | Node details are saved                | To be recorded after testing | Pending |
| 2      | SOS alert             | Alert appears on dashboard            | To be recorded after testing | Pending |
| 3      | Alert acknowledgement | Status updates correctly              | To be recorded after testing | Pending |
| 4      | Communication status  | Correct status is displayed           | To be recorded after testing | Pending |
| 5      | CCTV request          | Request is recorded                   | To be recorded after testing | Pending |
| 6      | Response assignment   | Assignment status updates             | To be recorded after testing | Pending |
| 7      | Safe-journey check-in | Journey status updates                | To be recorded after testing | Pending |
| 8      | Incident closure      | Final record is saved                 | To be recorded after testing | Pending |
| 9      | Access control        | Restricted functions remain protected | To be recorded after testing | Pending |
| 10     | Fault handling        | Error or unavailable status           | To be recorded after testing | Pending |

|  |  |              |  |  |
|--|--|--------------|--|--|
|  |  | is displayed |  |  |
|--|--|--------------|--|--|

### **5.3 Limitations of the Proposed System**

Although TRINETRA proposes a coordinated approach to emergency assistance, several limitations must be considered.

#### **1. Dependence on Communication Infrastructure**

The Safety Node must have a working communication connection to send an alert. A network outage may delay or prevent transmission.

#### **2. Power Failure**

The node may stop functioning if its power supply fails and the backup system is unavailable or exhausted.

#### **3. Limited CCTV Coverage**

CCTV coordination cannot guarantee continuous observation. A person may move outside the available camera coverage, and footage may not clearly show the relevant activity.

#### **4. Need for Human Operators**

The platform requires trained personnel who can assess incidents, communicate appropriately, and coordinate assistance.

A dashboard alone cannot guarantee that an emergency will be resolved.

#### **5. False or Accidental Alerts**

An SOS button may be pressed accidentally or used inappropriately. The system requires a procedure for assessing alerts without delaying urgent assistance.

#### **6. Privacy Concerns**

The collection and use of incident information may create privacy risks. Access restrictions, secure storage, retention limits, and legal compliance are necessary.

#### **7. Installation and Maintenance Costs**

Installing, connecting, maintaining, and monitoring public Safety Nodes requires financial and operational resources.

#### **8. Dependence on Authorised Integration**

The system cannot independently access restricted CCTV networks or control official emergency dispatch systems without appropriate permissions and technical arrangements.

## 9. No Guarantee of Crime Prevention

The presence of a Safety Node may improve access to help, but it cannot guarantee that a crime will not occur or that every alert will receive an immediate response.

## 10. Prototype Limitations

A simulated dashboard does not demonstrate real-world communication, live CCTV access, physical hardware reliability, or official emergency dispatch.

These functions require separate implementation and testing.

## 5.4 Evaluation Metrics

The proposed system can be evaluated using measurable indicators.

| Metric                       | What it measures                                                 | Method of evaluation                     |
|------------------------------|------------------------------------------------------------------|------------------------------------------|
| Alert delivery rate          | Percentage of test alerts received by the platform               | Compare alerts sent with alerts received |
| Alert acknowledgement time   | Time between receiving an alert and operator acknowledgement     | Calculate from recorded timestamps       |
| Communication success rate   | Percentage of test communication attempts completed successfully | Review communication test records        |
| Incident record completeness | Whether required fields are present                              | Audit test incident records              |
| CCTV request processing      | Whether requests and their outcomes are recorded correctly       | Review test request records              |

|                            |                                                                       |                                          |
|----------------------------|-----------------------------------------------------------------------|------------------------------------------|
| Response status accuracy   | Whether assignment statuses match the recorded workflow               | Compare status changes with test actions |
| Safe-journey completion    | Whether check-ins and arrival confirmations are recorded              | Review test journey records              |
| System availability        | Percentage of the testing period during which the prototype is usable | Record uptime and downtime               |
| Access-control performance | Whether unauthorised access attempts are blocked                      | Conduct controlled permission tests      |
| Fault reporting            | Whether simulated failures produce an appropriate status              | Review fault test records                |

## Interpretation

The evaluation should compare actual observations with the expected results.

For example, if the alert delivery rate is calculated, the report should state the number of alerts tested, the number received, and the resulting percentage.

The percentage can be calculated using:

$$\text{Alert Delivery Rate (\%)} = (\text{Number of alerts received} \div \text{Total alerts sent}) \times 100$$

Similarly:

$$\text{System Availability (\%)} = (\text{Total test time} - \text{Downtime}) \div \text{Total test time} \times 100$$

The results should be interpreted in relation to the test conditions. A successful software simulation does not prove that a full public safety network will perform equally well in real-world conditions.

## CHAPTER 6: CONCLUSION AND FUTURE SCOPE

### 6.1 Conclusion

Project TRINETRA proposes a connected, device-independent women's safety and rapid response network designed to improve access to emergency assistance in public spaces.

The project combines physical SOS Safety Nodes with a digital monitoring platform, human-supervised communication, authorised CCTV coordination, response management, and voluntary safe-journey monitoring.

One of its main features is that a person can request assistance through a physical node without needing a personal smartphone. After an alert is received, a trained operator can assess the situation, communicate with the person, and coordinate appropriate support through authorised channels.

The proposed CCTV Coordination Module can help record verified observations when relevant camera coverage and permission are available. The Safe Journey Manager can support check-ins and safe-arrival confirmation for individuals who voluntarily use the service.

The project also recognises that technology alone cannot eliminate crime or guarantee an immediate response. Communication failures, limited CCTV coverage, maintenance requirements, privacy concerns, and dependence on trained personnel must all be addressed before real-world deployment.

A prototype can demonstrate the main workflow through a 3D Safety Node model, a digital dashboard, sample incident records, and simulated response updates. Further development would be required to connect physical hardware, real communication systems, authorised CCTV infrastructure, and official emergency services.

Overall, Project TRINETRA presents a proposed technology-supported approach to improving emergency access and coordination. Its value lies in connecting existing safety resources through a structured, accessible, and privacy-conscious workflow.

## **6.2 Future Scope**

The project can be developed further in the following ways.

### **1. Functional Hardware Prototype**

A physical Safety Node can be constructed with an SOS button, communication module, microphone, speaker, status indicator, and backup power.

The prototype would need appropriate electrical and environmental testing.

### **2. Mobile Application**

A companion mobile application could provide optional access to journey registration, check-ins, emergency information, and incident updates.

The mobile application would supplement the physical Safety Nodes rather than replace them.

### **3. Authorised CCTV Integration**

With the required approvals and technical arrangements, the platform could support structured requests to existing CCTV control rooms.

Any integration should preserve access restrictions and record the source and time of verified observations.

### **4. Integration with Official Emergency Services**

Future development could explore authorised coordination with existing emergency response services, including India's ERSS 112.

Such integration would require formal approval, technical compatibility, operational procedures, and clearly assigned responsibilities.

### **5. Improved Location Support**

The system could explore additional methods of location confirmation where technically feasible and legally permitted.

Any location information must be labelled according to its source and reliability. The system should not present an unverified estimate as an exact live location.

### **6. Accessibility Improvements**

Future nodes could include accessible button placement, multilingual audio instructions, clear visual indicators, and features designed for people with different physical or communication needs.

### **7. Multilingual Communication**

The platform could support multiple Indian languages so that users can communicate more comfortably during emergencies.

### **8. Predictive Infrastructure Planning**

Aggregated and appropriately anonymised incident data could help authorised planners identify locations that require better lighting, maintenance, or additional emergency access points.

Such analysis should avoid discriminatory profiling and should not label individuals or communities as criminal based on incomplete data.

### **9. Improved Cybersecurity**

Future versions could include stronger authentication, encrypted communication, security monitoring, backup systems, and independent security assessments.

## 10. Pilot Implementation

A small pilot involving approximately five to ten nodes could be considered after technical, legal, financial, and operational review.

The pilot should be evaluated before any large-scale installation. Testing should measure alert delivery, communication reliability, maintenance requirements, accessibility, user experience, privacy protection, and coordination performance.

## CHAPTER 7: REFERENCES

The following sources provide background information relevant to emergency response, women's safety, cybercrime reporting, and sustainable development.

1. **Ministry of Home Affairs, Government of India.** Emergency Response Support System (ERSS) and emergency number 112. Official government information.
2. **Ministry of Women and Child Development, Government of India.** Women Helpline Scheme and related support services.
3. **Ministry of Women and Child Development, Government of India.** One Stop Centre Scheme for women affected by violence.
4. **Indian Cyber Crime Coordination Centre, Ministry of Home Affairs.** National Cyber Crime Reporting Portal and related reporting information.
5. **United Nations.** Sustainable Development Goal 5: Achieve Gender Equality and Empower All Women and Girls.
6. **United Nations.** Sustainable Development Goal 11: Make Cities and Human Settlements Inclusive, Safe, Resilient and Sustainable.
7. **United Nations.** Sustainable Development Goal 16: Promote Peaceful and Inclusive Societies, Provide Access to Justice for All and Build Effective, Accountable and Inclusive Institutions.
8. **Government of India.** Digital India programme and related digital public infrastructure initiatives.
9. **Government of India.** Applicable laws and rules relating to data protection, privacy, public surveillance, and emergency response.
10. **Project TRINETRA.** Proposed system design, Safety Node concept, digital platform modules, workflow, and prototype testing plan developed for this micro-project..

### **DECLARATION**

I understand that Karunya Institute of Technology and Sciences retains the rights to any product developed (*software or hardware*) through the Micro Project submitted by me to the Institution.

Furthermore, if I intend to document or publish any findings from the Micro Project work for commercial purposes, I shall obtain a No Objection Certificate (NOC) from the Office of the Registrar before engaging in such activities.

I also understand that any patentable outcomes arising from the Micro Project shall be reported to the Institution, and that patent filing, ownership, and revenue-sharing will be governed by the Intellectual Property Rights (IPR) policies of Karunya Institute of Technology and Sciences.

I acknowledge that any commercial utilization or republication of the Micro Project work, in full or in part, shall require prior permission from Karunya Institute of Technology and Sciences. I further agree that any royalty accruing from such utilization will be shared between the inventor(s) and the Institution in the ratio of 60:40, respectively, in accordance with the Institute's Intellectual Property Rights policy.

|                                  |                                                                 |
|----------------------------------|-----------------------------------------------------------------|
| <b>Signature of the Student:</b> |                                                                 |
| <b>Name of the Student:</b>      | MOUNISHA.T , MAHIVARSHINI.P,<br>DHIVYADARSHINI.V, KIRTHIVINYA.I |
| <b>Register Number:</b>          | <b>URK25FS1022, URK25FS1020,<br/>URK25FS1031, URK25FS1029</b>   |
| <b>Date:</b>                     | <b>27/10/2026</b>                                               |