



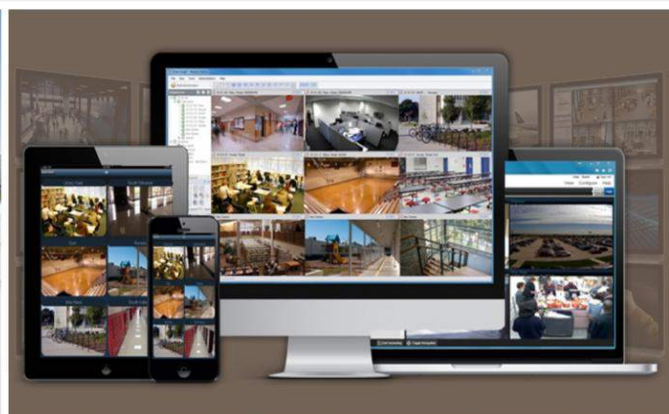
TECHNICAL REPORT

M2M ENABLEMENT IN

SAFETY & SURVEILLANCE SYSTEMS

TEC-TR-S&D-M2M-005-01

M2M SAFETY & SURVEILLANCE WORKING GROUP



TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

Revision History

Date	Release	Document No.	Description
12-05-2015	R1.0	TEC-TR-S&D-M2M-005-01	Technical report on M2M enablement in Safety & Surveillance Systems.

Important Notice

Individual copies of the present document can be downloaded from **<http://www.tec.gov.in>**

Users of the present document should be aware that the document may be subject to revision or change of status.

Any suggestions/comments may please be sent to **m2mreports.tec@gov.in**

Disclaimer

The information contained is mostly compiled from different sources and no claim is being made for being original. Every care has been taken to provide the correct and up to date information along with references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

रवि शंकर प्रसाद
RAVI SHANKAR PRASAD



मंत्री
संचार एवं सूचना प्रौद्योगिकी
भारत सरकार
MINISTER
COMMUNICATIONS & IT
GOVERNMENT OF INDIA

Message

I am glad to note that Telecommunication Engineering Centre is bringing out Technical Reports on M2M enablement in Transport, Health, Power and Safety & Surveillance sectors and a Report on M2M Gateway & Architecture.

M2M communications is going to change the way the humans live and control their surrounding as well as various social and economic sectors operate. It is expected to improve the efficiency of various sectors such as Automotive, Health, Power and Safety & Surveillance etc. by transmitting the information electronically and automation of information processing. It will help in providing quality services to our citizens.

I am confident that the Technical Reports will help in developing specifications/ standards to be used in India and opportunity of manufacturing wide variety of devices and other products in India. I congratulate TEC and all concerned for this commendable work which is very timely, and wish them success in all their endeavors.

(RAVI SHANKAR PRASAD)

राकेश गर्ग
सचिव
RAKESH GARG
Secretary



भारत सरकार
Government of India
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
Ministry of Communications &
Information Technology
दूर संचार विभाग
Department of Telecommunications

08th May 2015

Message

I am extremely happy to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a Technical Report on Gateway an Architecture of M2M communications.

2. While Government started the work of developing roadmap for M2M communications in India, TEC at the same time initiated the work of identifying technical requirements of Automotive, Health, Power, Safety and Surveillance sectors. As there has been active participation from stakeholder of each sector, the reports have taken into account the ground level status and requirement for M2M enablement.

3. India has to make strides in making its various sectors smart for which quick adoption of M2M is the necessary. These reports will help stakeholders in development and finalization of sectors specific plans for adoption of M2M.

4. I appreciate the efforts put in by Telecommunication Engineering Centre in bringing out these reports. I wish them success in all their endeavours.

(Rakesh Garg)
Secretary(Telecom)



सदस्य (प्रौद्योगिकी) एवं
पदेन सचिव, भारत सरकार
Member (Technology), Telecom
Commission &
Ex-Officio Secretary to Govt. of India
Tel : 23372307 Fax : 23372353

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
संचार भवन, २०, अशोक रोड,
नई दिल्ली-११०००९
Government of India
Ministry of Communications &
Information Technology
Department of Telecommunications
Sanchar Bhawan, 20, Ashoka Road,
New Delhi-110001



Message

I am happy to note that Telecommunication Engineering Centre (TEC) is bringing out technical reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a report of Gateway an Architecture of M2M communications. We are aware that adoption of M2M communication will inter-alia, lead to enhancement in the efficiency of various sectors of society and economy.

Need for improvement in efficiency in various socio-economic sectors has been felt for a long time and some efforts in this direction have also been made whereby M2M based systems have been deployed. However, the solutions which have been implemented are generally based on propriety platforms. However, to achieve smart processes and functioning in all the sectors, interoperability of devices/ platforms/ applications is necessary which entails adoption of open standards.

The technical reports of TEC are a good step in this direction and will certainly help various stakeholders to take preparatory steps in their respective sectors for future adoption of M2M communications.

(S.S. Sirohi)
Member (T)
8.5.2015.

सलाहकार (प्रौद्योगिकी)

Advisor (Technology)

Tel. : + 91-11-23718460

+ 91-11-23036317

Fax : + 91-11-23329525



भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
संचार भवन, नई दिल्ली-110 001
Government of India
Ministry of Communications &
Information Technology
Department of Telecommunications
Sanchar Bhawan, New Delhi-110 001

A.K. Bhargava
Advisor, DoT




Message

I am pleased to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a report on Gateway & Architecture of M2M communications.

TEC has taken timely action to take up the work of study and preparation of the Technical Reports in the Automotive, Health, Power, Safety and Surveillance sectors. The Reports have been prepared to be released along with the National M2M roadmap by virtue of relentless efforts of TEC and its Working Groups consisting of stake holders.

M2M communication is an opportunity for India not only to keep pace with the world but also to march ahead in development of specifications of new products consisting of Devices, Gateways and Platforms meeting the Indian requirements, though of course, in sync with the standards.

I appreciate the efforts of Telecommunication Engineering Centre specially its S&D Division and all the Working Groups for bringing out these technical reports in a very timely manner. I wish them success in all their endeavours.


(A.K. Bhargava)

AJAY KUMAR MITTAL

वरिष्ठ उप महानिदेशक

Sr. Deputy Director General

Tele : 23320252 Fax : 23329088

e-mail : srddg tec@gov.in

www.tec.gov.in



सत्यमेव जयते

भारत सरकार

दूरसंचार विभाग

दूरसंचार इंजीनियरी केन्द्र

खुरशीद लाल भवन, जनपथ, नई दिल्ली-110001

Government of India

Department of Telecommunications

Telecom Engineering Centre

Khurshid Lal Bhawan, Janpath, New Delhi-110001

ISO 9001:2008



FOREWORD

Telecommunication Engineering Centre (TEC) is an organ of Department of Telecommunications (DoT). It provides technical support to DoT. TEC develops technical specifications of products for use in telecom networks. It carries out technology studies and proactively takes up development of specifications based on such studies. Development of specifications is a transparent process with active participation of stakeholders. Certification of telecom products is also one of its activities.

M2M Communication is an area which has rapidly attracted attention of world over, primarily due to its enormous potential in bringing about fundamental changes in the delivery and use of services in almost all sectors of economy and society and the quality of human life.

M2M systems have been in use for some time past, e.g. in automotive sector. However, the use of technology/devices/application is generally proprietary in nature as standards have started involving in the recent past. We are aware that variety of social and economic activities are interdependent and in today's digital world, it is possible to link them through networks and applications to achieve enhancement in efficiency and development of new services. This is possible only when there is interoperability among devices/networks/applications. This requires standardization and development of harmonized specifications.

Towards achieving this objective, TEC in consultation with stake holders from government, industry, standards bodies and sector users, took up study of four sectors to begin with namely Automotive, Health, Power, Safety and surveillance. Four working groups (WG), one for each were formed with the participation from stakeholders as mentioned above. As it is also necessary to work out architecture for M2M domain and also service delivery models, Gateway and Architecture WG was also formed. All the groups have overwhelming participation. Chairmen, Rapporteurs & Co-rapporteurs have been elected by the WGs themselves. Joint Working Group is chaired by Sr. Deputy Director General and Head TEC.

These groups have carried out use case studies and analysis for respective sectors. Beginning the year 2014, these groups have worked relentlessly. This can be gauged from the fact that there were about 50 conference calls and four Face to Face (F2F) meetings combined of all groups and lot of many interactions within the groups. Services and Development (S&D) Division of TEC coordinated and managed the entire activity of formation of working groups, holding meetings, preparation of the reports etc.

The reports contain use cases in the sectors & their technical analysis, key challenges in implementation and the way forward. Suggestions for way forward those have emerged, require action by various stake holders as well as by TEC and the Working Groups. TEC and the Working Groups will continue further work and it is planned to bring out next release of Technical Report after further study as early as possible.

I express my sincere thanks to all the Chairmen, Rapporteurs and Co-rapporteurs and members of the Working Groups as well as the participating stakeholders as organization and as persons whose enthusiastic support and untiring efforts have made it possible to bring out these detailed reports.

Ultimate aim is to identify the areas for development of standards, harmonize Indian standards with international standards and development of product specifications ensuring interoperability. India being a big market for M2M, there is enormous potential of manufacturing devices and networking products for M2M in India. Let us all join hands to become part of the 'Make in India' programme of the Government of India.

I hope that the report will provide guidance to the stakeholders to plan standardized deployments in the concerned sectors. I also hope that the stake holders will provide their continued support to TEC to carry out further work in M2M domain. We will be enriched in our work through valuable suggestions from any quarter.


(A.K.Mittal)

**Sr. Deputy Director General & Head
Telecom Engineering Centre**

Contents

List of Contributors	i
Executive Summary	iii
1. Introduction	1
2. What is M2M Communication?	2
3. Need of M2M Communication in Safety & Surveillance	3
4. Conceptual Description of M2M Communication in the Safety & Surveillance Sector	4
5. Use Cases in the Safety & Surveillance Sector	5
5.1 Vehicles with Video Surveillance & Video Tracking Systems	5
5.2 Women / Citizen Safety using smart phones / wearable devices	8
5.3 City-wide Video Surveillance Systems	9
5.4 Video Surveillance for Banks, ATMs, Jewellery Stores, and Similar Establishments	11
5.5 Home Safety /Smart Home	12
5.6 Citizen Response Management System (CRMS)	13
5.6.1 Mobile Platform for Patrolling Vehicles	13
5.6.2 Computer Aided Dispatch (CAD)	14
5.6.3 Call Centre	15
5.6.4 Interactive Voice Response (IVR) for Call Centre	16
5.7 Employee Registration	17
5.8 Crime & Suspect Reporting	18
6. Communication technologies & Standards Available for Use in Safety & Surveillance Sector	20
6.1 WAN Communication Technologies	20
6.2 Comparison table of various protocols/technologies of M2M communication in safety and surveillance	20
6.3 Last mile Communication technology options for the Safety and Surveillance	22
6.4 Important requirements for the Safety and Surveillance Systems.....	22
7. Key Challenges	23
7.1 Interoperability and standardization	23
7.2 Availability of M2M connectivity	23
7.3 High Bandwidth availability and network latency	23
8. Way Forward	23
9. Use Case Analysis	23
9.1 Title	23
9.2 Objective	23
9.3 Background	23

9.4	Description	24
9.4.1	Scenario #1: Generating Panic Alert	24
9.4.2	Scenario #2: Device & User Registration.....	24
9.4.3	Stakeholders.....	25
9.4.4	Information Exchanges.....	25
9.4.5	Potential New Requirements	26
10.	References	27
11.	Abbreviations	28

Figures

Figure 1 - Conceptual Representation of M2M Communication.....	2
Figure 2 - M2M Connectivity & Platform	4
Figure 3 - M2M Framework for Safety & Surveillance Platform.....	5
Figure 4 - Panic Button Workflow	8
Figure 5 - Citizen safety mobile platform.....	9
Figure 6 - Security Surveillance Systems.....	11
Figure 7- Sample Interface for Patrolling vehicles	14
Figure 8 - Sample Control Room Dashboard.....	15
Figure 9 - Employee Registration & Verification.....	18
Figure 10 - Crime Reporting & Suspect Identification Model	19
Figure 11 - User Generating The Panic Alert.....	24
Figure 12 - Notification Workflow	24

Tables

Table 1 - Benefits & Limitations of protocols & their frequencies	20
Table 2 - Abbreviations	28

List of Contributors

A. Joint Working Group (JWG) Chairman:

Name	Designation	Organization	Email Address
A K Mittal	Sr. DDG	Telecommunications Engineering Centre (TEC)	srddg.tec@gov.in

B. Joint Working Group (JWG) Secretariat:

Name	Designation	Organization	Email Address
Sushil Kumar	DDG(S&D)	Telecommunications Engineering Centre (TEC)	ddgsd.tec@gov.in

C. Working Group (WG) Chairs:

	Name	Organization	Designation	Email Address
Chairman	Neelesh Mantri	Tata Teleservices Limited (TTSL)	DGM(M2M, Utilities & Smart Cities)	neelesh.Mantri@tatatel.co.in
Rapporteur	Om Gangwar	Reliance	DGM	om.gangwar@relianceada.com
Co-Rapporteur	M. Salim Beg	TEC	Director(LTE)	dirlte.tec@gov.in

D. Primary Authors

Name	Organization	E-mail Id
Neelesh Mantri	Tata Teleservices (TTSL)	neelesh.mantri@tatatel.co.in
Rohit Singh	Smart24x7 Response Services	rohits@smart.org.in
Kannan Natarajan	Mediatronix	kannan.mtx@gmail.com

E. Contributors

S. No.	Name	Organisation
1.	Sushil Kumar	TEC
2.	M. Salim Beg	TEC
3.	Rajiv Kumar Tyagi	TEC
4.	Ms. Anupama	C-DOT
5.	Ms. Mini Vasudevan	Ericsson
6.	Ms. Reena Malhotra	DoT
7.	Venkat	CG Global
8.	Dinesh Sharma	ETSI
9.	Murali	IVIS
10.	Munish Kumar	OVT
11.	C.P. Singh	Smart24x7 Response Services
12.	Sai Pratyush	Tata Teleservices
13.	Alok Mittal	STMicroelectronics

F. Joint Editorial Team:

S. No.	Name	Organization
1.	A K Mittal	TEC
2.	Sushil Kumar	TEC
3.	A.Bhattacharya	C-DOT
4.	Anuj Ashokan	TTSL
5.	Sriganesh Rao	TCS
6.	Niranth Amogh	Huawei
7.	Hem Thukral	India Smart Grid Forum (ISGF)
8.	Alok Mittal	STMicroelectronics
9.	Rohit Singh	Smart24x7 Response Services
10.	Sharad Arora	TTSL
11.	Raunaque Quaiser	STMicroelectronics

Executive Summary

Safety of the citizens is a key area of concern for countries around the world. The government is putting a lot of focus to safeguard its citizens. Safety and Surveillance is also one of the components for the Smart City initiatives of the government. Continuous monitoring of the city, raising alarms and communicating to the relevant authority are some of the primary needs. Communication technologies can play a key role in reducing the crime rate and increase Safety and Surveillance for the citizens.

This document is a Technical Report of the Telecommunication Engineering Centre (TEC) on the Safety & Surveillance systems. Apart from introducing and explaining the need of M2M communication in the Safety & Surveillance Systems, the report has also identified the use cases, which include Surveillance and Tracking of Vehicles, Women/Children Safety using Smart phones and wearable devices (wrist band), City-wide Video Surveillance, Citizen Response Management System, Home Safety for local Smart Home and so on. Further, the key challenges in the implementation of M2M in this sector have also been identified.

This report has also mentioned the communication technologies being used in various safety and surveillance use cases. Further, the women safety use case has been described in detail after detailed deliberations and discussions with key stakeholders such as Security Service providers and solution vendors. The working group has suggested way forward to address the challenges and take up further work in this sector.

The System should be implemented in such a way to accommodate the future needs and other variants of safety paradigms. The devices and solutions to be used should be scalable and work on the pre-defined standards, so that new devices and solutions can be integrated with ease.

1. Introduction

Safety and security is paramount, and the government has taken various initiatives to safeguard its citizens. Safety & surveillance ensures a safe and secure environment, not just limited to video surveillance, emergency response, and technology enabled smart premise. The ability to initiate emergency communication is to request help when needed, and should be able to work with existing telecom network. By use of technology the location of the users in distress may be transmitted to the emergency responders through an automated process.

Surveillance can be used for various purposes, including real-time monitoring and alerts to prevent theft, to improve efficiency, and also to ensure safety.

Security threat can emerge from many sources like terrorism, snooping, safety threats for women; theft etc. Due to this, there could be far reaching consequences like loss of human life, property and change in behavioural pattern, many of those being irreversible.

Safety and security M2M applications are relevant to all of the domains such as home, medical and industrial. M2M has dramatically expanded the scope of available home security and safety products. Today it is possible to remotely monitor & manage your house from anywhere across the globe. With an intelligent sensor network, it is possible to detect whether you have left the gas on or the water tap running before you left for work.

Furthermore, besides detecting such problems, you can also rectify them if you have the required actuators installed at home. You can remotely close the main gas valve as well as the water valve. If you have detected that lights in some of the rooms were left on, those can be turned off remotely as well. When someone breaks into your home, you can be automatically alerted and promptly asked for a suitable course of action to take such as calling the police, sounding an alarm or waiting for your arrival. In addition, the covert cameras installed in the house can be remotely prompted to start recording every action of the intruder to be used as valuable legal evidence. Such intelligent systems deliver much more than what the best watchdog or a loud and expensive traditional alarm possibly can.

2. What is M2M Communication?

It refers to the technologies that allow wired / wireless system to communicate with the devices of same ability. M2M uses a device (sensor, meter etc.) to capture an 'event' (motion, video, meter reading, temperature etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information. A conceptual picture is shown below in Figure 1:

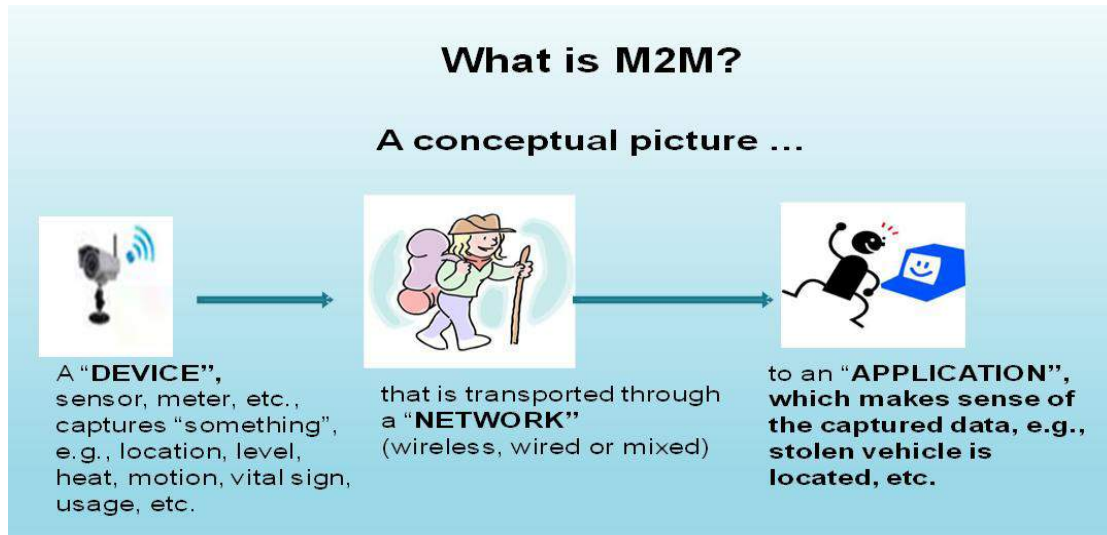


FIGURE 1 - CONCEPTUAL REPRESENTATION OF M2M COMMUNICATION

The enabling technologies for M2M / Internet of Things are sensor networks, RFID, M2M, mobile Internet, wired & wireless communication network, semantic data integration, semantic search, IPv4 / IPv6, etc. In wireless communication Wi-Fi, ZigBee, 6LoWPAN, Bluetooth technology may be used for short range connectivity of devices / devices to the gateway and GSM 2G/ 3G/ 4G or WiMAX for connecting M2M gateway to server.

IPv4 addresses are going to exhaust. Standardization and adoption of IPv6 in telecom and ICT organizations will provide an opportunity of having billions of devices which can be IP enabled and seamlessly addressable through mobile or wired broadband connections

M2M is a subset of Internet of Things. Internet of Things is a more encompassing phenomenon because it also includes *Human-to-Machine communication (H2M)*.

Various sectors such as Power, Automotive, Health, Safety & Surveillance and Agriculture etc. may be transformed to smart systems by using M2M / IoT.

3. Need of M2M Communication in Safety & Surveillance

India has 129 police officers for every 100000 citizens. According to a UN report, the worldwide average is close to 350 officers per 100,000 citizens.¹ This translates equipping officers with the right technology to manage the massive population of 1.2 billion of the country. Technology helps citizens connect with authorities promptly. Following reasons are attributed to M2M enablement as a solution for safety & surveillance.

- i) M2M devices can be made to run on 24x7 basis providing continuous monitoring. Communication channels deployed can enable seamless communication between devices.
- ii) Human intervention in processes leads to delay and errors.
- iii) The authorities are enabled to give standard response to all citizens within pre-determined duration.
- iv) M2M devices auto-detect the incident using video and audio capture, intrusion, gas leak detection, high temperature, motion detection, and heartbeat triggers alerts with location of incident to the appropriate authority.
- v) Event Triggered by Citizens (Press SOS Button, Call Authorities, SMS, IVR, Break Glass, etc.) will broadcast the location and details of citizen to the Authorities.
- vi) Back end systems are able to auto identify location of distress and notify the appropriate agency. In the event of fire, the local fire department is notified. In case of medical emergencies, the nearest hospital/doctor is notified.
- vii) Back end systems can identify responders available in the vicinity and alerts them about the user in distress, along with location coordinates.
- viii) Auto dispatch of Emergency Vehicles will bring down the response time of authorities.
- ix) Since all device activities will be recorded and time stamped, incidents of fake alerts and occurrence of incidences will also get documented.

¹ <https://www.osac.gov/pages/ContentReportDetails.aspx?cid=15911>

4. Conceptual Description of M2M Communication in the Safety & Surveillance Sector

The various elements in M2M communication include a Wide Area Network (WAN)/Backhaul Network, Neighbourhood Area Network (NAN)/Field Area Network (FAN), Home Area Network (HAN), sensors, home gateway, Data Concentrator Unit (DCU)/Gateway and an application/data centre. Presence of a home gateway would be decided by the nature of the application that is being catered to. In addition, a Backbone/Core network should also be present. Figure 2 depicts a typical conceptual description of M2M communication with respect to Safety & Surveillance applications.

(Please note that this is for reference only)

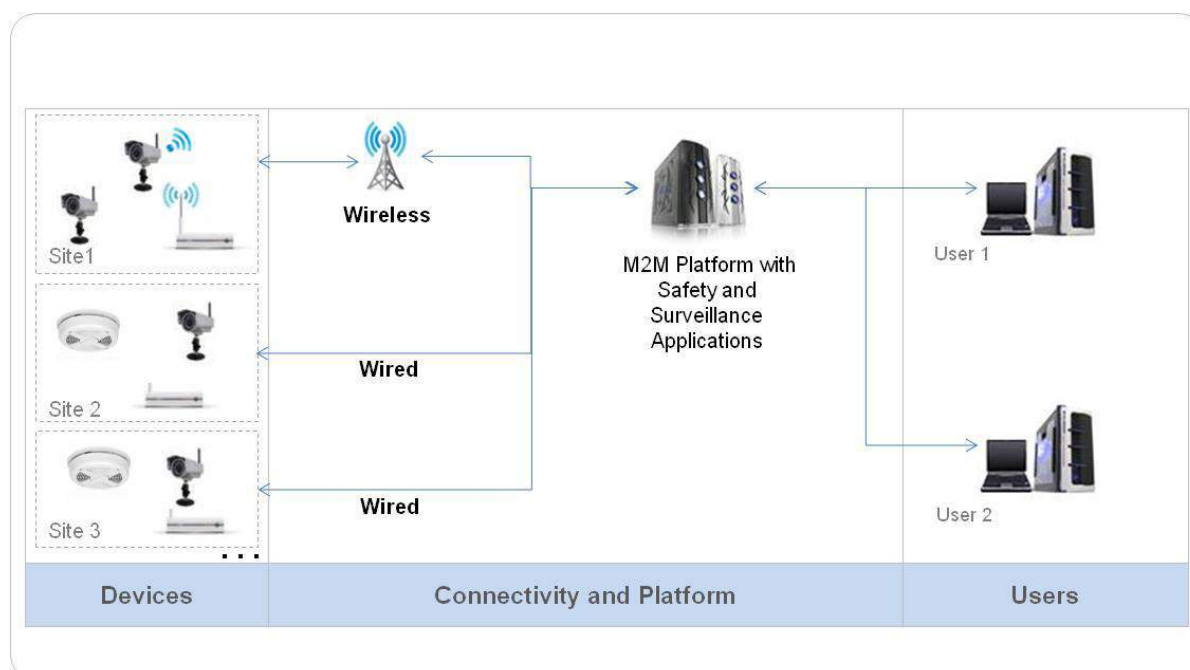


FIGURE 2 - M2M CONNECTIVITY & PLATFORM

A typical M2M communication model for safety and surveillance solution should enable devices such as sensors, cameras and gateways to communicate with the M2M cloud platform applying the same process without variations. This ensures different use cases to be implemented promptly, ensuring robust and interoperable solutions. This would enable security agencies to perform centralized and distributed monitoring. Centralized M2M cloud platform would also enable the system to scale up, when required. APIs can be integrated to extend benefits to other verticals. The system is so designed that it accommodates public and private emergency agencies. This will introduce flexibility on the part of the government to utilize private service providers efficiently.

5. Use Cases in the Safety & Surveillance Sector

There are numerous options that provide safety & surveillance solutions, but the challenge is in selecting the one that links seamlessly with existing systems and one that provides round the clock services. The target should be to reduce number of devices that offer enhanced safety and surveillance. The figure 3 shown below depicts the model for various applications of safety and surveillance solution.

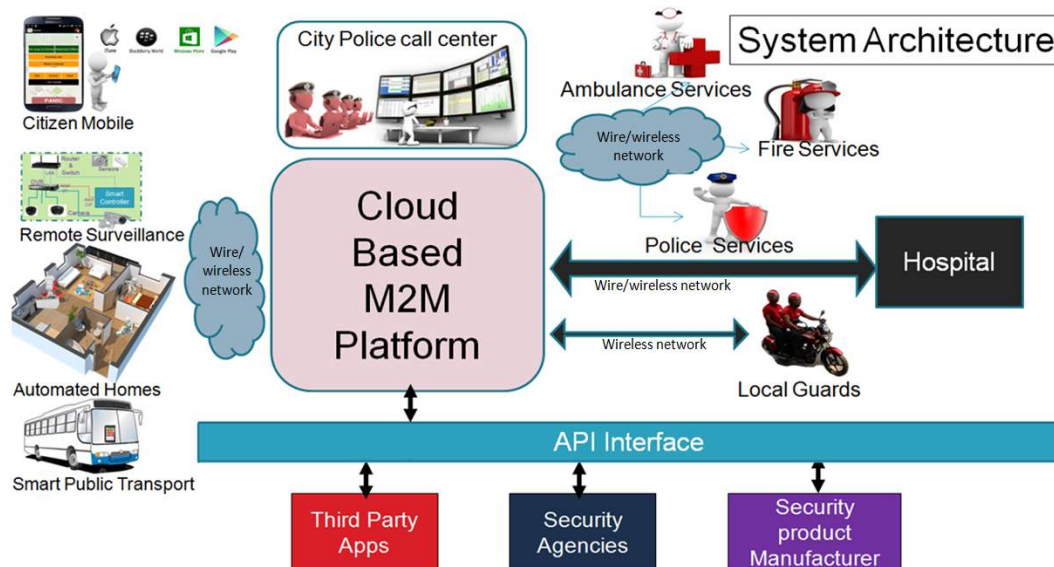


FIGURE 3 - M2M FRAMEWORK FOR SAFETY & SURVEILLANCE PLATFORM

Safety and surveillance finds its application in the following verticals.

- Vehicles with video surveillance and vehicle tracking systems.
- Women/citizen safety using Smartphone/wearable devices.
- City-wide video surveillance systems.
- Video surveillance for banks, ATM, jewellery stores, and other establishments.
- Local smart home wireless networks for home security.
- Citizen response management system (CRMS).

Exploring Key Use Cases in Safety & Surveillance Sector

The following are some of the key areas where M2M communication can be used in the Safety & Surveillance sector:

5.1 Vehicles with Video Surveillance & Video Tracking Systems

This use case describes video surveillance inside transport vehicles with vehicle tracking system.

M2M Communication

1. Local connectivity between devices includes primary wired Ethernet, and the option for wireless panic buttons.

2. Wireless 2G/3G connectivity is useful for remote tracking/remote viewing from control room.

The local and remote connectivity will be based on the components (vehicle mounted and control room) being used for Surveillance and tracking solutions.

Vehicle mounted modules/sub systems are as follows:

1. Video Surveillance System (VSS) using cameras
2. Vehicle Tracking Subsystem (VTS)
3. Panic button and siren interface (wired/wireless)

Control room components are as follows:

1. Central Control Room Hardware (CCRH)
2. Central Command and Control Software (CCCS)

Existing Scenario

At present, in most installations, video surveillance and vehicle tracking modules work independently and need independent connectivity to control room. Additionally, each module has an independent architecture with no compatibility between products from different manufacturers.

It is better to have a common interface specification for each subsystem. Products that can be identified for standardization are as follows:

1. Video Surveillance subsystem (VSS)
2. Vehicle Tracking Subsystem (VTS) with panic button and siren interface
3. Central Command and Control Software (CCCS)

Connectivity between components of Surveillance and Tracking System

1. 2G/3G wireless modem/router can be used for sending/receiving information from VSS and VTS modules to control room.
2. The sub-systems connect with each other through wired Ethernet.
3. Panic buttons and sirens are wired, supervised and tamper proof.

Video Surveillance Subsystem

720P and higher HD IP cameras offer better resolution and face identification.

The IP camera has local storage for a set recording duration. The camera should have minimum two video streams as follows:

1. 720P HD or higher resolution with H.264 compression
2. VGA/CIF JPEG stream

HD video at 3 fps or more must be used for recording and storing content. As per demand, either HD stream or JPEG stream could be viewed at the control room depending on 2G/3G network availability. Camera housing should be rugged. Cameras may have optional Infrared illuminators. All cameras are connected to the wireless modem through Ethernet links.

For remote live viewing, video can be streamed using RTSP protocol or sent as individual JPEG frames depending on network bandwidth. It should be possible to download any video clip over Ethernet.

Vehicle tracking module with panic button interface and siren.

- i. GPS based VTS module should have a rugged and tamper-proof enclosure.
- ii. Vehicle tracking module periodically sends GPS position of vehicles and other status parameters to the central control room via the common wireless modem. This also serves as 'keep alive' message to the control room.
- iii. Vehicle tracking module should have inbuilt battery to send out information to the control room even in the absence of vehicle battery connection.
- iv. VTS module should be capable of connecting to multiple numbers of supervised panic buttons. Panic buttons should be tamper proof and active type so that disconnection or tampering of any panic button could be detected by vehicle tracking module, and could trigger notification to control room.
- v. VTS should also have a link to a supervised siren with tamper proof features.
- vi. VTS serves as central controller of the vehicle surveillance system and connects with the central control room. In case vehicle ignition is off, it periodically sends status commands to central command room. To reduce power consumption, VTS module can switch to low power sleep mode in between transmissions. During this period, VTS module can switch off power to cameras also, to save over all power consumption.
- vii. VTS can also send GPS information as UDP packets to IP cameras for embedding with recorded video.

Control Room Software

Control room software can have common features like live tracking, playback, and geo-fencing etc.

Standardization

Control room software should prefer the use of common communication protocol to communicate with bus-mounted hardware.

- i. Control software would require VTS module protocol for connection, configuration, data request, alarm notification, acknowledgement, etc..
- ii. Control software to VSS communication protocol may have commands for live video streaming request, configuration change, etc.

BLE Panic Buttons in Bus

BLE Panic buttons can be deployed in buses to raise emergency alerts. These panic buttons will connect to smart devices over Bluetooth and when triggered, it will send a notification to a smart device, which will trigger an alert to the control room over cellular network publishing current GPS location of the bus. Figure 4 below depicts the workflow of the Panic Button.

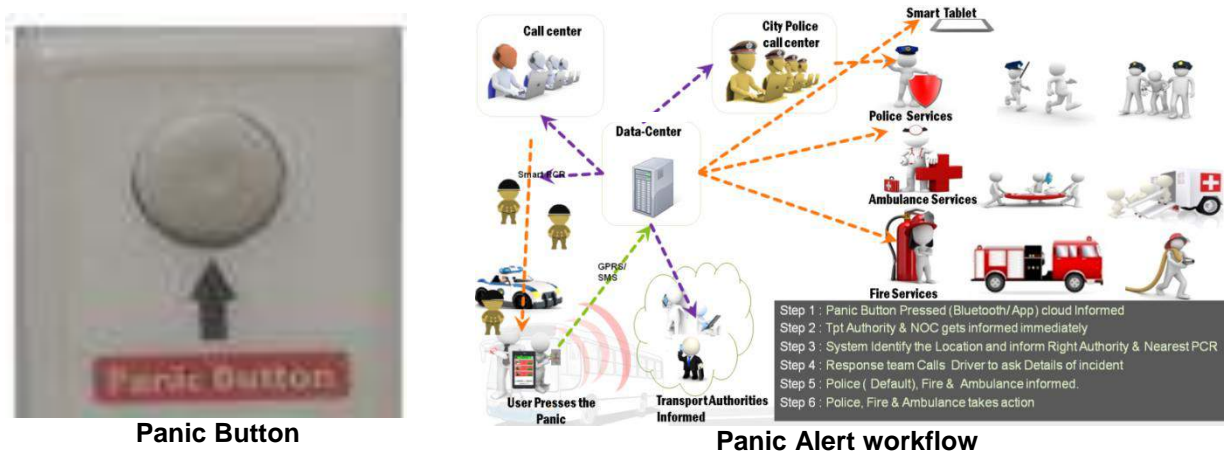


FIGURE 4 - PANIC BUTTON WORKFLOW

Registering the Drivers

In order to provide enhanced level of safety in the transport sector, drivers and buses should be registered to the centralized system. This will enable the linking of the drivers & buses and further can be linked with routes they would be operating on. The same solution can also be extended to corporate drivers employed, for the pick and drop of the employees.

5.2 Women / Citizen Safety using smart phones / wearable devices

This use case describes specific handheld devices such as smart phone and/or wearable devices for personal safety, primarily for women. These handheld or wearable devices will generate alerts to a central control room during emergencies publishing GPS location data of the person.

M2M Communication

- Connectivity between handheld devices and control room is over 2G/3G/4G wireless networks.
- Local connectivity between Smartphone's and other wearable devices such as wristbands is over Bluetooth.

Mobile App Based Alerts

The mobile platform service entirely depends on the cellular network as it uses the same to communicate with the server applications. Primarily, the Smartphone application will use the Internet connection and if it fails then it should switch over to the SMS services for communication. Location of the user should be identified using GPS and if GPS signal is not available, the application should use the technique of Triangulation to fetch the location with the help of mobile towers. In case the system fails to get the location by GPS and Triangulation, it should allow the user to provide the address explicitly by entering the same manually.

In case of SMS based alert mechanism, the alert should be sent directly to SMS receiver platform and that should trigger the alert to control room interface. Mobile notifications and SMS should be used as mode of communication by the server applications to communicate with the mobile platform.

For non-smart phone users, the system should provide SMS and an IVR services to trigger panic alerts. There should be few pre-configured options for the user to report the incident location.

Apart from notifying the agency, the mobile platform should also inform near and dear ones of the user. In case relatives have the same platform on their mobile, they should be able to track the user and check, where the help has reached. The mobile platform application should also provide an 'I am Unsafe' action button, for users to inform near and dear ones only and not the agency. This recorded data can be used for the purpose of analysis and to increase the patrolling of unsafe areas.

There should be a provision of automatically dialling of an emergency number from the mobile application, for the selected service (pre-defined or user selected), once the alert is generated by the user. The platform should also provide an option to select department and agency services like Police, Fire, and Ambulance. The mobile application should record the audio and click images, once the panic alert is generated by the user, and communicate the same to the appropriate agency. Figure 5 below depicts the generation of panic alert and an interface to select the appropriate services.

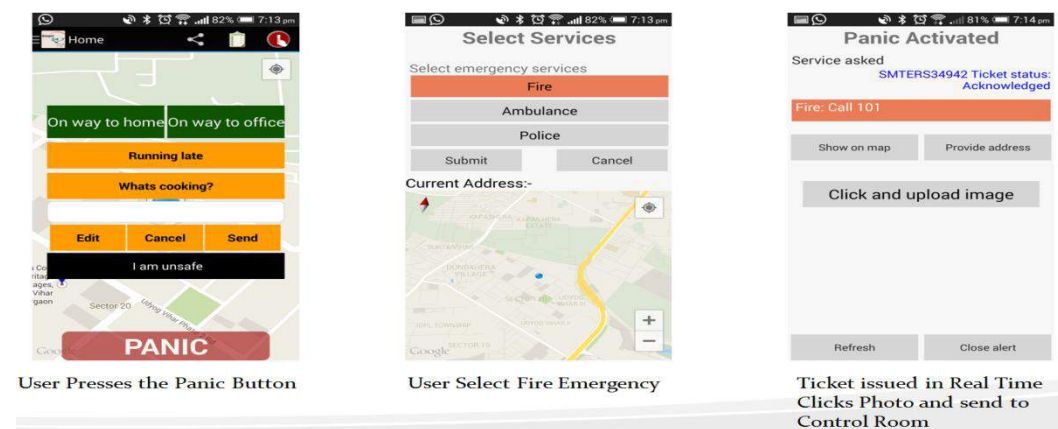


FIGURE 5 - CITIZEN SAFETY MOBILE PLATFORM

Wristband Connected to Smartphone

It is possible to connect a wristband to mobile phone over BLE. The power consumption by BLE is very low and battery can last long before it requires recharging or replacement.

There should be a provision to deactivate a false or accidentally activated alarm using a password/duress code, over the mobile phone application interface. The provisioning should also be done to "Arm" and keep the mobile phone and wristband in 'Ready State' to automatically trigger the alarm in case of emergency. Alarm activation can be activated by a duly calibrated shock sensor.

5.3 City-wide Video Surveillance Systems

City surveillance Cameras should be able to view traffic situations, accidents, and incidents with clarity along with other objects on road. PTZ cameras can be used to zoom into any object on the road for detailed identification and recognition. Identification of face is not mandatory, except when using PTZ zoom facility. Fixed cameras may or may not be able to recognize faces, depending on the field of view of the camera.

M2M Communication Method

Video surveillance calls for high data rates in Gbps for city application and hence special considerations apply for this use case.

Dedicated connectivity using OFC, leased line connectivity can be provided by an ISP.

Typical Recommended Bandwidth/Data Rate

Fixed 2 Mega pixel camera require 4 - 5 Mbps data rate at 25 fps, while PTZ cameras (pan, tilt, zoom) will require 20-30% higher bandwidth.

Reduced frame rates can be used to reduce data rates/bandwidth requirements.

Required Frame Rate

For CCTV general application, 25/12/6 fps recording rates are sufficient at full resolution, depending on bandwidth availability and storage requirements.

Video Streaming Standards

Streaming should be unicast/multicast with H.264 compression and Universal Plug and Play (UPnP) feature. Multiple streaming capabilities should be possible at two resolutions. Camera parameters can be adjusted using camera web server application.

New ONVIF standard protocol, which works over HTTP is also recommended so that cameras are automatically identified and listed by the video management software. Out of many ONVIF standards, ONVIF –S standard camera interface is recommended due to simplicity. Even when using ONVIF, video streaming works using RTSP protocol.

Connectivity Recommendation

Connectivity for city surveillance installation can be done by using following options:

1. Dedicated wired connectivity such as CAT5/6, OFC, lease lines etc.
2. Leased line connectivity provided by an ISP. In this case, the system design, edge switches, streaming methods should be as per recommendations of the ISP.
3. The streaming data rate has to be limited to meet ISP's bandwidth limitations.
4. Wireless might be the only option in some cases. Typically, 5 GHz band is recommended due to limited interference. Some of the identified disadvantages of using the wireless connectivity are:
 - a. Airspace bandwidth always limited.
 - b. Line of sight link is required, and very tall masts may be required. This increases installation cost.
 - c. Interference with other devices leads to clogged networks.
 - d. Only free bands/spectrum licensed by Telecom Regulatory Authority of India (TRAI) for outdoors can be used.

As city surveillance is of critical nature, it is recommended to use wired connectivity as much as possible.

5.4 Video Surveillance for Banks, ATMs, Jewellery Stores, and Similar Establishments

Main purpose of camera for above use case is to prevent theft and unwanted intrusion, and sabotage during non-office hours and for internal security during office hours.

Cameras are mainly used for indoor and the immediate perimeter of any building.

Cameras should have night vision with true day and night ICR feature capability. If regular night illumination is not available, Infrared illumination should be provided. Night illumination for video surveillance should have power back up from UPS, as a mandatory feature. Video surveillance will always be enhanced with alarm sensors, as 24x7 manual monitoring is not possible. Figure 6 can be referred to identify the Connectivity and communication model for such surveillance systems.

M2M Communication Method

Local communication is through CAT5 IP networks with wired or wireless sensor connectivity.

Remote notification should be sent on 2G/3G/4G/ADSL networks.

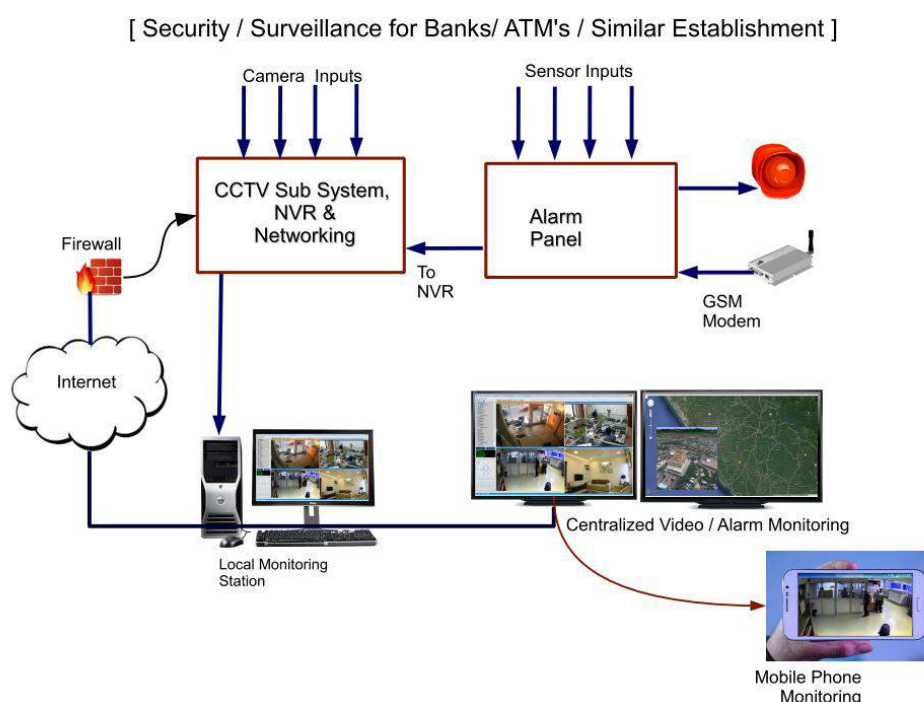


FIGURE 6 - SECURITY SURVEILLANCE SYSTEMS

Alarm Integration

Security Surveillance systems should have a provision to integrate the alarm sensors. Normally, alarm sensors like door switches, PIR sensors, and vibration sensors are integrated into the system using an alarm panel. Alarm panel should have an interface to the CCTV system.

Alarms with video streaming can be monitored locally inside the bank or from a remote location.

In case of remote monitoring, when an alarm notification is received, video can be verified first, before initiating an action.

Local siren should be activated by the alarm, and there should be option to manage the same from a remote monitoring station.

Connectivity

- a. Dedicated CAT5/6 cable is used for all internal connectivity. PoE feature will reduce, power cabling to camera sites. Large buildings may call for fibre optic cable links also for internal connectivity.
- b. For remote monitoring, ADSL lines can be used for alarm and video. Typically, 4 Mbps, ADSL connection may be sufficient to give upload speed of 512 Kbps.
- c. The alarm system may have GSM/GPRS connectivity as an added security, to enable remote notification to concerned officers on mobile phones and for central control room.

5.5 Home Safety /Smart Home

Times have changed and there is little possibility that there is some person round the clock to take care of your home. Leaving your home vacant or just with your kids inside is the usual practice now-a-days. Such a situation is ideal for house breaking or burglary. As a check against such possibilities an adequate home security system needs to be in place. Present generation security systems are not confined to locks and keys, but include surveillance devices, locking systems, and alarms. With all these devices the security of your home stands guaranteed.

Sensors may be installed to safeguard the homes by detecting motion, glass break etc. Further, sensors may also include PIR sensors, vibration sensors, asset tracking sensors, smoke, gas detectors, optical barriers along with video surveillance, and sirens.

Smart home applications should enable controlling of home devices like lighting, HVAC, other appliances and energy management, elderly care, child tracking, etc.

User can control all the sensors and other appliances over smart phones, tablets or dedicated keyboards.

M2M Communication Method

- a. 2.4 GHz global ISM band
- b. Sub 1 GHz ISM band (with advantages of being less crowded and better home coverage due to lower attenuation).

Most countries allow sub-GHz band for low power wireless applications. Examples of allowed bands in Europe are 433.05 MHz - 434.79 MHz and 863 MHz - 870 MHz bands. India has 865 MHz – 867 MHz free band for this purpose.

Wi-Fi networks shall be used in homes for connecting higher bandwidth devices like IP cameras.

Power consideration would be the main criteria, as sensors have to operate for 3-5 years from a primary cell.

Communication Technologies

- a. There are many technologies used for this use case, like ZigBee, Z-wave, 6LoWPAN Wi-Fi etc.
- b. 2G/3G/4G connectivity, along with wired broadband/ADSL, should be preferred for remote connectivity scheme.

5.6 Citizen Response Management System (CRMS)

Citizen Response Management System will be responsible for receiving emergency alerts, communicating with the user in distress and dispatching the patrolling vehicles, ambulances & fire brigade. As and when a user triggers a panic alert, the notification will be sent to the Control Room and a call will be established from the users' mobile phone to the authorized call centre. The call will be managed over IVR System and users mobile will act as an Automated Information System for sharing the location and other personal details of the user. Users mobile will also share the images and audio recording with the call centre and with Police Control room, if required.

The important components that will constitute an effective CRMS to handle any emergency situation are being discussed below.

5.6.1 Mobile Platform for Patrolling Vehicles

To address any emergency situation a solution is required to link the victim with the patrolling vehicles so that the total response time could be reduced and immediate assistance/help can be provided. To enable this, a rugged or tough pad like tablet should be installed in the emergency vehicles having informer cum victim locator application. Figure 7 can be used as a model for such applications. This application should help the respective department to:

- a. Track the vehicle
- b. Send the information of any alert generated in its geo-fenced area.
- c. Take the inputs/feedback on the case reported.
- d. Locate the victim's location on Google Map
- e. Communicate with control room & victims' relatives

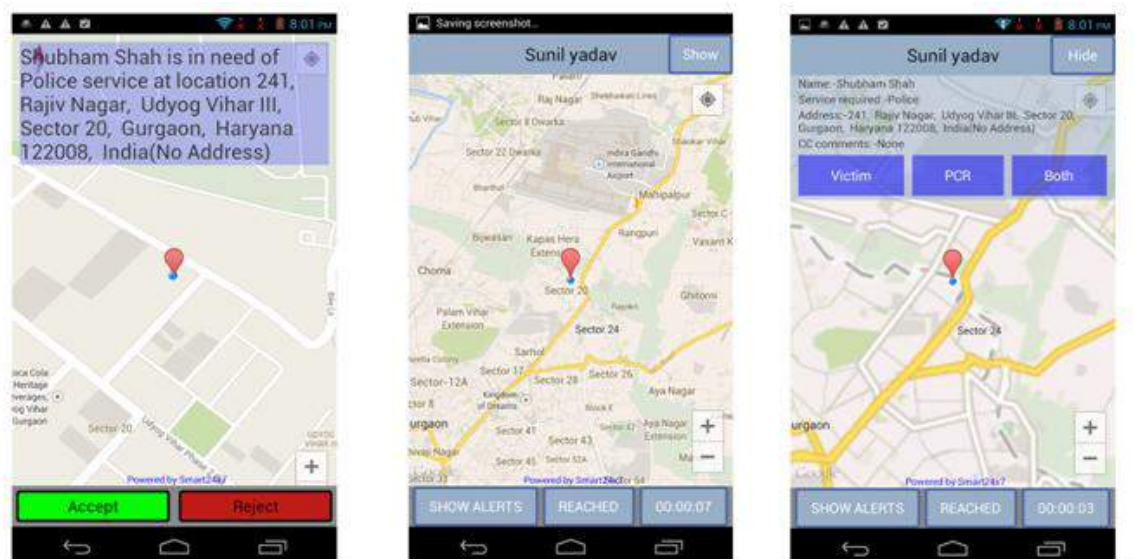


FIGURE 7- SAMPLE INTERFACE FOR PATROLLING VEHICLES

5.6.2 Computer Aided Dispatch (CAD)²

Once the Patrolling/Emergency Vehicles will be equipped with Informer cum locator solution, they can be dispatched automatically or by their respective Control Rooms to provide the help to the user in distress.

The Control rooms may choose to automatically deploy the Patrolling/Emergency vehicle, nearest to the location of the user in distress.

During the initial stage, the control room may opt for the manual dispatch of the vehicle from their application interface, as the system will be new and it will learn the intelligence to avoid the fake alerts over a period of time. To identify the genuine alerts, control room may be provided with a dashboard, communicating all the information about the user, audio & image proofs and summary of past history of the alerts from that user. Thereby enabling the control room to filter out the fake alerts and provide quality service to the users in real emergency. A third party call centre may also be hired/used to filter out the fake alerts for the control room.

Considering the fact that GPS accuracy might vary or the user might be at a different location than the location of actual emergency, following information, as shown in Figure 8, may be shared with the control room:

- Name of User
- Mobile Number of User
- GPS Location of User
- Time of generating the alert
- GPS Accuracy

² Ambulance dispatch in Health Document.

- f. Speed of users movement
- g. Actual Location of Emergency
- h. Audio recording
- i. Images
- j. Location of Victim on Google Map
- k. Location and status of patrolling vehicles on google map
- l. Elapsed time since incidence was first reported.
- m. Total Alerts for the day
- n. Currently Active alerts
- o. Total Alerts closed for the day

The above reported information helps the control room identify the nearest patrolling vehicle or response centre and assign the alert to the same. This will help in reducing the response time by a couple of minutes, which could help save an innocent's life or avoid the crime. In case the alert goes to some other jurisdiction control room, there should be an option to re-assign the ticket to the correct control room, which can act on the alert.

The Control Room Interface should also provide colour based identification on the status (New, PCR Deployed and PCR Reached) of the alerts received and the gender identification of the user who raised the alert. The interface should have a built in algorithm to intelligently identify the fake alerts and shows the count of alerts the user has generated in the past and also a detail of alert types like fake alert, genuine alert, test alert, and customer has refused etc, but this will require more rules as there may be multiple cases that may identify an alert as fake and system can learn over a time to handle the same. As and when an alert is received, the control room authorities may be informed by an automated audio that could be activated by the system.

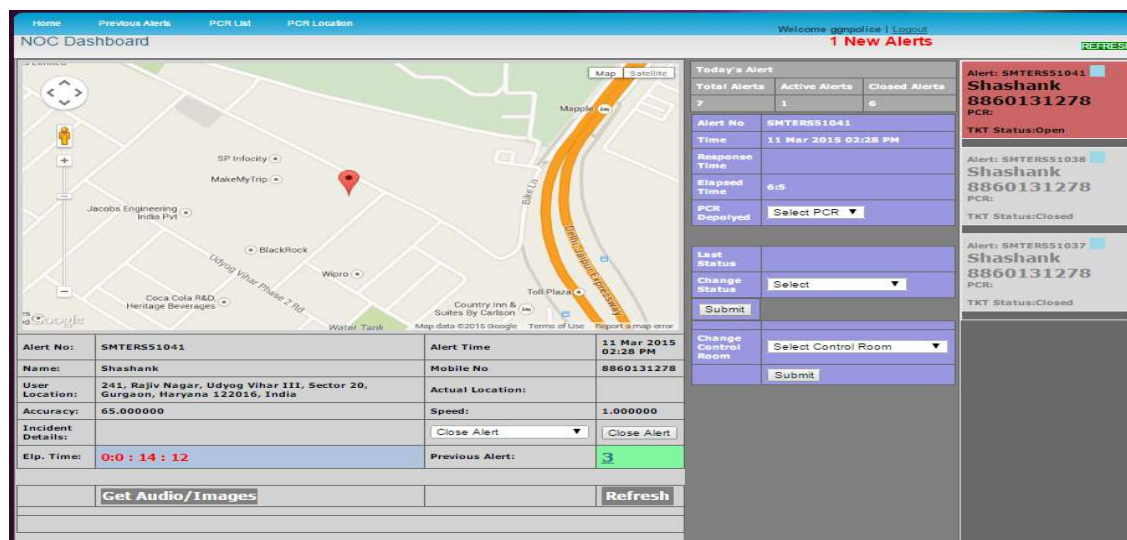


FIGURE 8 - SAMPLE CONTROL ROOM DASHBOARD

5.6.3 Call Centre

To avoid the additional work load of fake alerts and query handling a call centre should be setup. The call centre may be given the authority to filter out the fake calls by contacting the user who

generated the alert. If after verification, they report the alert as genuine, control room can get into action. This will reduce the calls to emergency agencies during initial launch of the system. The call centre should have two modules: One for Supervisor and one for call centre executives. Supervisor interface would empower the supervisor to monitor the status of alerts and performance of call centre executives. Detailed information of user in emergency may be provided on both the interfaces. This system should be programmed to generate a ticket number for every alert, for future references and communicate it to the user in emergency, emergency authorities and the call centre executive. The call centre may also be authorized to monitor that all the alerts are being addressed by the control rooms.

As Call Centre will only be responsible in assisting the government authorities, hence they should be provided an overview of the alerts with basic information only.

5.6.4 Interactive Voice Response (IVR) for Call Centre

One of the important parts of CRMS would be an IVR as it will manage all the calls to and from the call centre. An IVR may be setup to give the user in distress, a feel of immediate response and support.

A provision for Non-Smart phone users should also be provided to make the calls to the emergency number for reporting an incident and call centre executives should be able to communicate with the user, when they receive an emergency alert.

An Ideal IVR Solution may provide the following services:

- a. Calls can be received at the terminals by the executives
- b. Agents can make the call from the terminals using Microphone
- c. Call Conferencing can be done to loop in multiple people in a call
- d. Calls can be transferred to same & other groups agents
- e. Incoming Call Routing to agents can be done using groups and skills
- f. Call Waiting
- g. Custom On Hold Information with an pre-recorded audio
- h. Agent Wrap Up Time
- i. Call Recording
- j. Music/Information on Hold
- k. Agent Do Not Disturb Mode
- l. Agent on Break Mode
- m. Call Blocking
- n. Supervisor Panel for seeing Agents Logged-in and Logout Report
- o. Supervisor Panel for call recording Report
- p. Real time Monitoring
- q. On Agent Busy, IVR will get played
- r. Chat between agents

CRMS - Advantages to Agencies

- a. Paperless Processing
- b. Auto Identification of Male & Female Citizens

- c. Can check exact response of the Task Force
- d. More Secured Society
- e. Centralized monitoring
- f. Real-time MIS

CRMS - Advantages to State & District Level Control Room

- a. Paperless Processing
- b. Auto Identification of Male & Female Citizens
- c. Auto Assign the Ticket to Nearest Patrolling Vehicle
- d. Intelligent Computer aided Dispatch
- e. Real-time Information shared within Department
- f. Helps in Investigation
- g. Can check exact response of the Police Department
- h. More Secured Society
- i. MIS Submission to Senior Officers can be done in Real-time

CRMS - Advantages to Citizens

- a. Faster Response time from emergency agency
- b. Can Share important information about type of incident in real time with emergency agencies.
- c. Can see how the Emergency Van is coming towards them

5.7 Employee Registration

An extended level of safety can also be provided, by e-registering the employee with Police and getting the same verified. This will enable quick sharing of information across police control rooms and police stations and also help generate for them a Unique Registration Number (URN). This URN can be used to refer to their complete history of work and behaviour. Employer's feedback and report of any criminal activities will alert the new Employers before hiring the employee. Figure 9 shows the verification process by integrating the other existing databases.

Below process may be used to implement this solution at national level:

- Register the employee using the smart phone or web interface.
- Upload the ID proof, photo & address proof of the employee.
- The details as registered are sent to the local city Control Room Dashboard.
- Control room can assign the details for verification to the home town of the employee. This will send the details to the home town control room and then to the respective police station for verification.
- Police station can verify the details within the given time and update the same against the ticket number. In case they fail to give any feedback, automated calls can be made to avail the status of the query.
- The feedback will be sent immediately to the local control room where employee is registered.
- Based on the feedback of the control room, it updates the ticket status and the same will be sent to the employer as SMS/email.

Further to the registration of employees, the system may also be used to obtain feedback on an employee's behaviour. The employer may provide ratings to their employees, feedbacks on various aspects and hire or fire the employee based on the feedback.

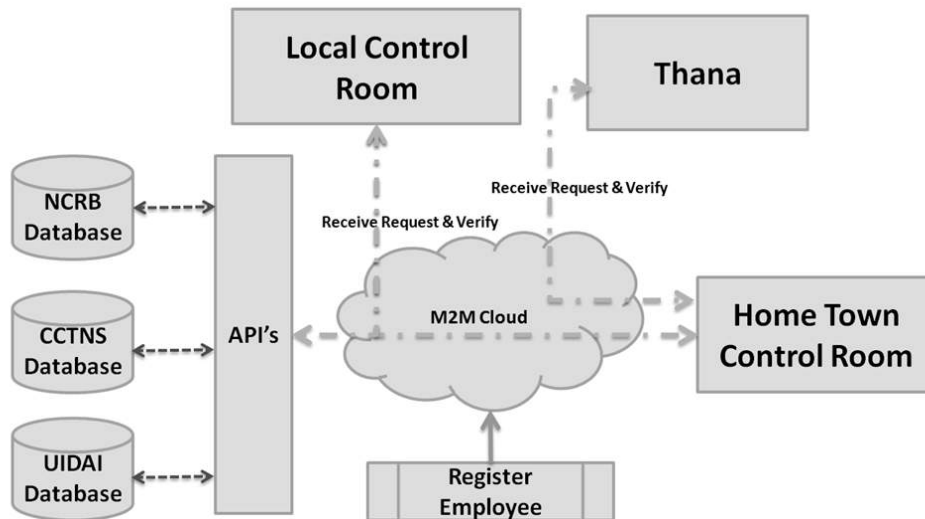


FIGURE 9 - EMPLOYEE REGISTRATION & VERIFICATION

5.8 Crime & Suspect Reporting

Smart phones and Cloud based M2M, if integrated with existing databases of safety & security agencies over the API's, may help identify the suspect against the criminal or terrorist activity. The identification might be done by comparing the images of crime or the free flow text describing the crime scene. Any user having mobile safety application can report the criminal activity and the same will be sent to the control room along with the images. Control Room investigation team can scan the databases for similar crimes and identify the suspects for the similar crime, reported earlier, in real time. This will reduce the suspect identification time and will enable the government agency to provide faster response and action. With time, the system may be provided with more of Artificial Intelligence to crack down or increase the security basis the past patterns of criminal/terrorist activities. Figure 10 shows the process for identifying the suspect against a crime.

Any proof collected after or before the crime, can be uploaded to the system and a real time check can be performed against the data available in CCTNS, NCRB or UIDAI database. This will enable the quick tracking of the criminal and reduce the crime rate.

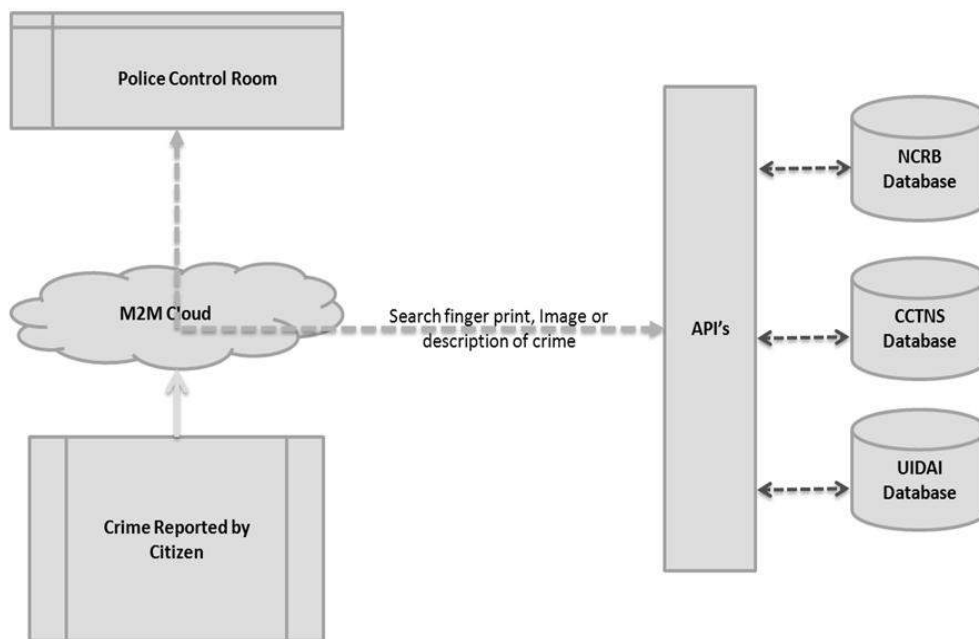


FIGURE 10 - CRIME REPORTING & SUSPECT IDENTIFICATION MODEL

6. Communication technologies & Standards Available for Use in Safety & Surveillance Sector

6.1 WAN Communication Technologies

For WAN connectivity, any of the following options could be used:

Currently prevailing and not limited to

- a. Wired : Leased lines / Broadband on Copper / Fibre
- b. Wireless : Point to Point dedicated radio link, Cellular communications 3G /4G LTE

6.2 Comparison table of various protocols/technologies of M2M communication in safety and surveillance

Content in the following table is to be treated as guidelines only. While making the comparison, the openness and standards-based nature of the technologies was not considered because the term 'open' is perceived in different ways by individuals/organisations. For example, some believe a standard is open if it is universally available to everyone or if it is available free of cost. Another perspective is that if a standard can be implemented free of cost, it is 'open'.

TABLE 1 - BENEFITS & LIMITATIONS OF PROTOCOLS & THEIR FREQUENCIES

Technology /protocol	Frequency band	Advantages	Limitations	Relevance for Safety and Surveillance
Wireless				
Low Power RF				
6LoWPAN – based RF Mesh	Various frequencies in the 800 MHz, 900 MHz & 2400 MHz bands typically	<ul style="list-style-type: none"> • Lightweight • Versatile (can be used with any physical and data link layer) • Ubiquitous • Scalable • Manageable and secure connectivity (IPSec is inbuilt) • Can be used in the sub-GHz range 	<ul style="list-style-type: none"> • IPv6 packets are bulkier • All low power wireless personal area networks are unreliable due to uncertain radio connectivity, battery drain, device lock ups, physical tampering etc. 	Home networks
Bluetooth	2.4 GHz	<ul style="list-style-type: none"> • Mature technology • Easy to implement 	<ul style="list-style-type: none"> • Low data security • Extremely short range • Only connects 2 devices at a time • Not very reliable 	Home networks / wearable devices
Wi-Fi	2.4 GHz, 5 GHz	<ul style="list-style-type: none"> • Mature technology • High home/office penetration 	<ul style="list-style-type: none"> • Limited range • Poor building penetration 	Home video security cameras., point to point video connectivity,

		<ul style="list-style-type: none"> • High data rates achievable • Easy to implement 	<ul style="list-style-type: none"> • High interference from other sources • Power consumption higher than those technologies that operate in the sub-GHz band 	
ZigBee, Z wave etc	2.4 GHz, 920 MHz, 915 MHz, 868 MHz, 780 MHz	<ul style="list-style-type: none"> • High market penetration in the home-automation domain 	<ul style="list-style-type: none"> • Low data rate networks, mesh technology 	Home sensor and automation networks
Cellular	For India, 900 MHz, 1800 MHz, 2100 MHz and 2300 MHz is allocated.	<ul style="list-style-type: none"> • Mature technology • Rapid deployment • Communication modules are low cost and standardised. 	<ul style="list-style-type: none"> • Unsuitable for online substation control due to reliability and coverage issues • Coverage not 100% • Reliability not the best • Short technology life-cycle (2G, EDGE, 3G, LTE etc.) 	Best for most remote monitoring applications in security and surveillance
Wire line				
OFC	Depending on application	<ul style="list-style-type: none"> • Extremely fast • Practically unlimited bandwidth • Very low attenuation 	<ul style="list-style-type: none"> • Installation may be expensive • Limited availability • High installation cost 	Best for city surveillance applications
ADSL	0-2.208 MHz	<ul style="list-style-type: none"> • Inexpensive (installation and use) • High SLA • Less installation time • Bonded DSL provides inherent redundancy 	<ul style="list-style-type: none"> • Low data security • Lower throughput • Higher latency 	Remote monitoring for home and other establishments :
Ethernet	16 MHz, 100 MHz, 250 MHz, 500 MHz, 600 MHz, 1 GHz, 1.6-2.0 GHz	<ul style="list-style-type: none"> • Inexpensive (installation and use) • Excellent throughput • Low installation time • Easily scalable 	<ul style="list-style-type: none"> • Lowest data security • Lowest SLA • Highest latency • Bursts of additional bandwidth not possible 	Most proven video / data surveillance back bone.

6.3 Last mile Communication technology options for the Safety and Surveillance

Currently prevailing and not limited to

- a. 6LoWPAN-based RF mesh
- b. Wi-Fi
- c. WiMAX
- d. ZigBee
- e. Bluetooth
- f. Wired(OFC, Leased Line)

6.4 Important requirements for the Safety and Surveillance Systems

1. Devices should comply with IPv6, specifically for the devices directly connected to the public network. For non-IP devices, the routers should have IPv6 compatibility.
2. Cameras need to have sufficient inbuilt storage to ensure Zero data loss.
3. The upload speed available in the network for each camera should be minimum 256 Kbps, however 1 Mbps speed will provide improved resolution.
4. ONVIF as preferred protocol for Cameras

7. Key Challenges

The sector today faces a number of challenges pertaining to M2M Communication. Some of the major challenges are mentioned below:

7.1 Interoperability and standardization

Interoperability at the device level, data transport level and software level is one of main challenges. For example, For Transport security, interoperability and compatibility between GPS tracking systems, control room software, video surveillance subsystems from different manufacturers is a main challenge. Similar situations exist for alarm integration, IoT devices etc. Without interoperability, life cycle of the system will get limited due to lack of support, or product becoming obsolete from a manufacturer.

7.2 Availability of M2M connectivity

Ubiquitous availability of radio connectivity of sufficient bandwidth on mobile networks at all physical locations may be a limitation in full use of wearable devices, transport security etc. Further, surveillance projects will require OFC networks which require significant investment.

7.3 High Bandwidth availability and network latency

Video surveillance like applications requires high bandwidth to perform real time monitoring and transfer the videos having better resolution. In the absence of Optical Fibre connectivity or non-availability of required bandwidth, proper working of such system will be difficult.

8. Way Forward

1. Interface and Protocols for various M2M use cases in the safety and surveillance, like transport security, General CCTV + Alarm integration etc. need to be standardized.
2. Device Identification mechanism, Authentication, Self-discovery should also be a part of standardization
3. As large number of applications will emerge, there is a need to study the requirements of spectrum, PLC channels etc.
4. As security & surveillance Systems are already in use, there is need to standardize RF bands for such devices.
5. A framework needs to be created for access to national databases like UIDAI, CCTNS, NCRB, etc for security & surveillance systems as depicted in the use cases.

9. Use Case Analysis

9.1 Title

Women Safety

9.2 Objective

This chapter explains use case analysis for woman safety. In the workflow of Women Safety Platform, panic alert is generated by the smart phone application or the wearable device.

9.3 Background

Women in distress can generate the panic alert by using their Smart Phone and all the stakeholders i.e. police, near & dear ones, etc. will be notified about the personal details and location of the women.

9.4 Description

9.4.1 Scenario #1: Generating Panic Alert

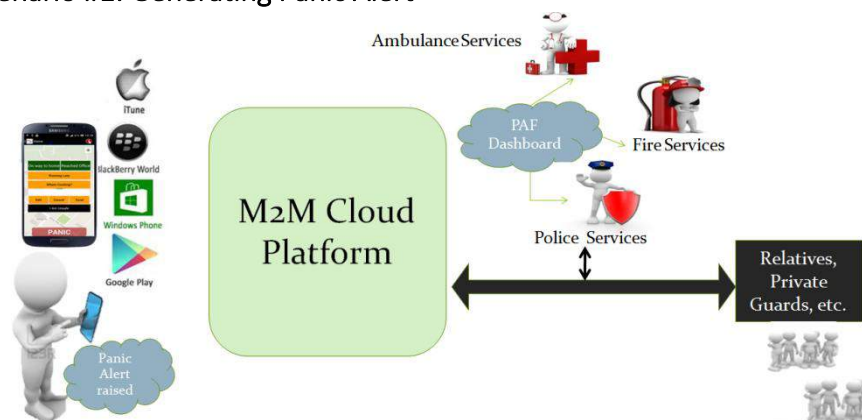


FIGURE 11 - USER GENERATING THE PANIC ALERT

This clause describes the use case where a user in emergency triggers the panic alert using the mobile application, as shown in Figure 11.

It also shows that the M2M Cloud platform informs the relatives, private agencies and respective government authorities (Police, Fire, Ambulance). This is shown in Figure 12.

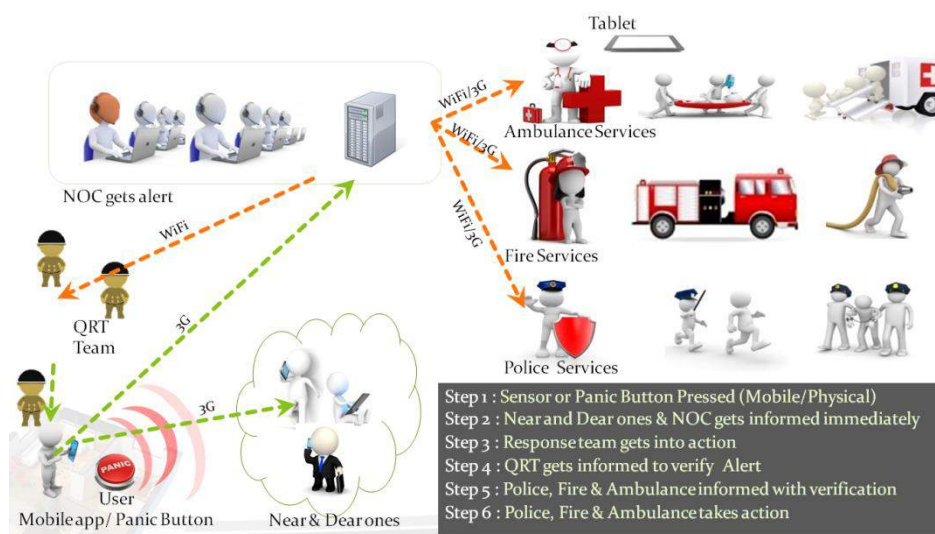


FIGURE 12 - NOTIFICATION WORKFLOW

9.4.2 Scenario #2: Device & User Registration

Once the user downloads the application on their smart phone; they should fill in the personal information and upload their image. The registration screen will also ask the user, whether they want to generate the panic alert using the power button of their smart phone.

As soon as user submits the information for upload, the device id of the mobile also gets transferred to the M2M registration engine. The M2M registration engine then pushes an OTP

notification to the smart phone and this act as the validation and ensures that the application is installed on the phone whose number is provided and not on other phone.

This validation will help avoid the abuse of the system by users.

Primary Contacts

Once the personal information and device is registered with the M2M platform, the user will be provided with an interface to add the primary contacts to the system. These contacts will be notified by the M2M safety services in case any panic alert is triggered by the user. When the user will add the primary contacts, M2M contact registration service will send an SMS to the contact added as primary contact in to the system.

Panic Alert Notification

As and when the user will generate the panic alert, M2M Platform will get notified over the 2G/3G/4G networks and then it will execute the notification services as selected by the user. The notification services will send the alert to security agency, as selected, local guards, if available, and near & dear ones. The M2M Platform will also be provided with the location details of the user triggering the alert and this location information will further be shared with all the stakeholders. This will work like an informer for the victim and further will be used to dispatch the patrolling vehicles or help using an automated algorithm or through manual process.

9.4.3 Stakeholders

Victim: Victim is the user in emergency. This is the stakeholder who will initiate the panic alerts and all the respective authorities will get informed. Victim should have a smart phone or a wearable device to trigger the alerts.

QRT Team: QRT Team could be a corporate QRT or private agency providing safety and security services through marshals/guards. These could also be security guards of the society or a corporate. They would be having a smart device or web dashboard for receiving the alerts from the victims.

Security Agencies: These are the government agencies like Police, Fire, Ambulance, etc. They can further have vehicles that could also be linked with M2M devices for quick response and locating of the victim. They would also be having a smart device or web dashboard for receiving the alerts from the victims.

Relatives: These are the near & dear ones of the victims, whom the victim might want to communicate in case of emergency. The M2M cloud will notify this stakeholder through SMS or in-app notification and the progress of help as well.

9.4.4 Information Exchanges

Registration

The smart phone application with M2M device capabilities is attached to the wireless network and performs registration in the M2M system. Registration includes the capability to maintain information describing phone details (Device Id, OS, version, etc), the user of the device, and the primary contacts that will be notified in case of any emergency.

Primary Contacts

Capability to add the near & dear ones to the M2M system from the application installed on device with M2M capabilities.

Data Delivery

Capability to securely deliver data to the intended device (e.g. Control room, Patrolling vehicle) or M2M application entity (e.g. primary contacts phone) in the appropriate format and confirm delivery.

9.4.5 Potential New Requirements

Right now, there are wearable products in the market that can communicate with the smart phone to raise the panic alerts over BLE, but there is a need to launch more wearable devices equipped with GSM & GPS.

10. References

- <https://www.usenix.org/system/files/conference/nsdr12/nsdr12-final2.pdf>
- <http://transition.fcc.gov/pshs/public-safety-spectrum/4-9GHz-Public-Safety-Band.html>
- <http://www.onvif.org/>
- <http://www.ti.com/lit/an/swra048/swra048.pdf>
- <http://www.ti.com/lit/wp/swry006/swry006.pdf?DCMP=ep-con-lprf-sub1range&HQS=ep-con-lprf-sub1wpaper-b-whip-kr>
- http://www.analog.com/library/analogdialogue/archives/40-03/wireless_srd.pdf
- <https://www.osac.gov/pages/ContentReportDetails.aspx?cid=15911>
- <http://www.smart24x7.com>

11. Abbreviations

TABLE 2 - ABBREVIATIONS

Abbreviation	Full Name
ADSL	Asymmetric digital subscriber line
ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
BLE	Bluetooth Low Energy
BT	Bluetooth
CCCS	Central command and control software
CCTNS	Crime & Criminal Tracking Network & System
CCTV	Closed Circuit Television
CIF	Common Intermediate Format
CMOS	Complementary metal-oxide semiconductor
DOF	Depth of field
ERS	Electronic Rolling Shutter
FOV	Field of View
GIS	Geographic information system
GPRS	General packet radio service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HD	High Definition
ICR	Infrared Cut Filter
IP66	Ingress Protection rating 66
IPv6	Internet Protocol version 6
IR	Infra-Red
ISM	Industrial, Scientific and Medical Band of Spectrum Like 2.4GHz, 865-868MHz
ISP	Internet Service Provider

Abbreviation	Full Name
LAN	Local Area Network
LTE	Long-Term Evolution
M2M	Machine-to-Machine
NCRB	National Crime Record Bureau
OFC	Optical Fibre Cable
ONVIF	Open Network Video Interface Forum
PIR	Passive Infrared (sensor)
PLC	Programmable Logic Controller
PoE	Power over Ethernet
PTZ	Pan-Tilt-Zoom
QRT	Quick Response Team
RTSP	Real Time Streaming Protocol
TRAI	Telecom Regulatory Authority of India
UDP	User Datagram Protocol
UIDAI	Unique Identification Authority of India
USB	Universal Serial Bus
VGA	Video Graphics Array
VSS	Vehicle Surveillance System
VTs	Vehicle Tracking System
WAN	Wide Area Network



TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA