PROJECT REPORT ON

Smart Buildings: Integrated Resource Optimization Using Sensor Network

UNDER THE GUIDANCE OF

PROF. AVINASH ASLEKAR

TOWARDS PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE AWARD OF

MASTER OF BUSINESS ADMINISTRATION IN TELECOM MANAGEMENT

॥वसुधैव कुटुम्बकम्॥

SUBMITTED BY

Dennis Marcell V	14020541012
Gatha Kapadiya	14020541014
Sandeep Sharma	14020541019
Mohit Nemani	14020541066
Aniruddha Maurya	14020541088
Dipti Chodnekar	14020541102
Snehlata Pareek	14020541138

Batch 2014-2016

Symbiosis Institute of Telecom Management

(Constituent of Symbiosis International University)

Pune 412 115

Symbiosis Institute of Telecom Management

(Constituent of Symbiosis International University)

Pune 412 115

Certificate

This is to certify that the research project titled **Smart Buildings: Integrated Resource Optimization Using Sensor Network** is a bona fide work carried out by the within signed students of 2014-16 Batch

Dennis Marcell V

Gatha Kapadiya

Sandeep Sharma

Mohit Nemani

Aniruddha Maurya

Dipti Chodnekar

Snehlata Pareek

Under the guidance of Prof. Avinash Aslekar

Towards the partial fulfillment of the requirements for the award of Master of Business Administration in Telecom Management (MBA – TM)

_____ _____

Signature of Guide

Prof. Avinash Aslekar

Signature of Director

Prof. Sunil Patil

Table of Contents

Executive Summary

Worldwide, buildings account for about 40 percent of total energy consumption and contribute a corresponding percentage to overall carbon emissions. Buildings used by businesses and public service organizations make up a large part of this footprint, whether they are office buildings, retail stores, hotels, schools or hospitals.

The government of India has launched an ambitious and transformational scheme to develop 100 Smart Cities. These smart cities will be enabled by a number of smart solutions including those targeted to infrastructure, energy, transport, utilities, environmental sustainability, and communication. Government and civic authorities are key enablers for significant portions of civic and administrative infrastructure, utilities, and public amenities. However, individuals, private building owners, and businesses can also contribute by making private and public buildings smarter. After all, the smarter the buildings, the smarter the city will be.

The key to a smart building is integration: linking building systems together and then connecting the building automation system to enterprise systems. Integration is enabling facility executives to reap smart-building benefits, both in new construction and also by gradually transforming existing buildings into smart buildings.

Many buildings currently have the capability to become smart buildings. But facility executives often fail to take advantage of those capabilities, not realizing that the advanced technology in their building systems is a platform for a smart building.

The research project provides insight into various verticals that help in the making of a smart building.

Introduction to Smart Buildings

"A smart building is still a cost premium. But by spending upfront, it's possible to reduce costs dramatically" says Robert Knight of Environmental Systems Design.

People spend 80 to 90 percent of their lives in buildings, making buildings an integral part of their ecosystem. With the advent of new technologies, the role buildings play is being redefined from a static environment to a more dynamic and interactive space that impacts the lifestyles, wellbeing, and productivity of their occupants.

Smart buildings depend on intelligent building automation systems to seamlessly integrate and manage a facility's core systems, such as HVAC and lighting, among others. But there is no single set of capabilities that defines all smart buildings. Rather, the smart building concept is a dynamic process that enables an organization to use integration to tap the power of systems that are in a building today, while also providing a path to future improvements.

Smart-building integration begins by linking such core building systems as lighting, power meters, water meters, pumps, heating and chiller plants with sensors and control systems. At a higher level, elevators and access control systems enter the picture, along with shading and more advanced concepts. Integration can also encompass the fire alarm system to further improve safety.

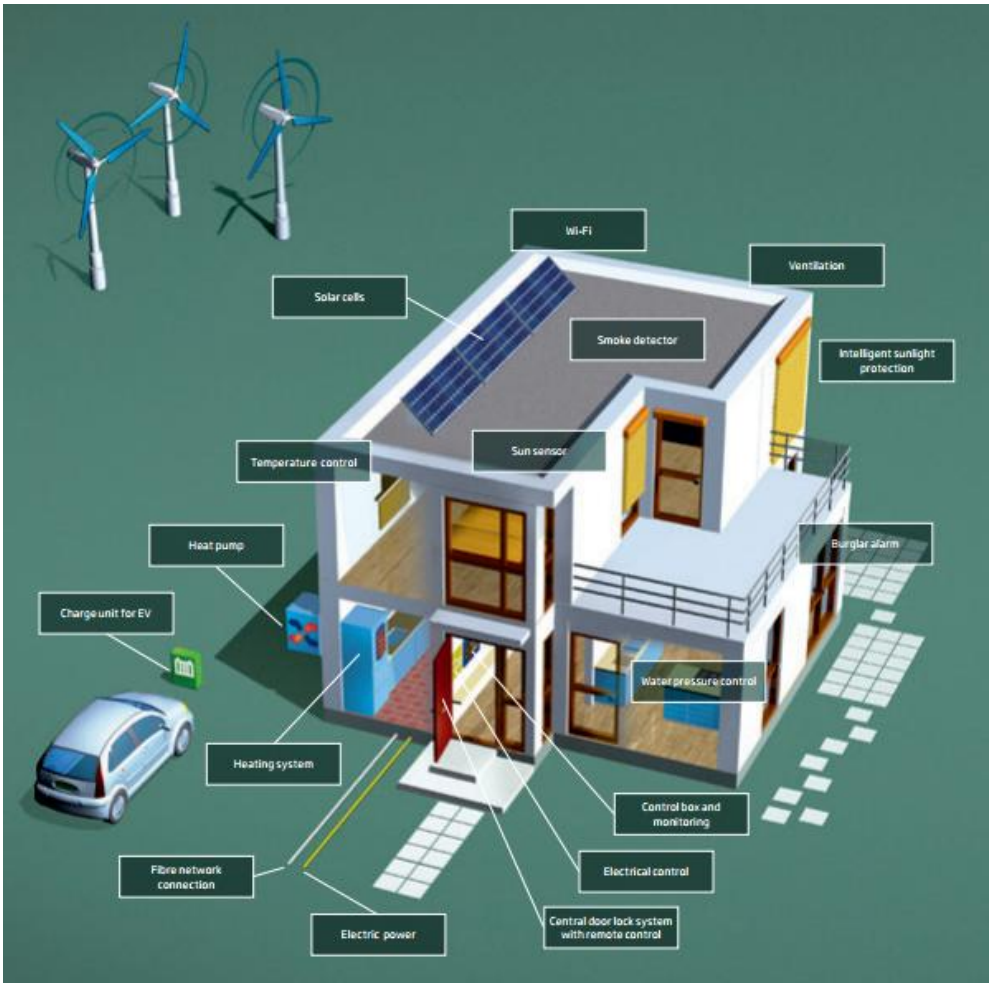


Fig 1: Potential features of Smart Buildings

Smart Buildings - IT Security

A smart building management security plan deals with risk throughout the design, installation, and operation phases of a system's lifecycle. Many real estate companies focus their efforts on creating a secure design and take minimal steps to maintain security moving forward. Only by creating and executing a plan to address security throughout the entire lifecycle of the system, can an organization effectively manage risk.

Intelligent Building Management System (iBMS) security is a relatively new concern for real estate industry. Once proprietary, stand-alone systems, intelligent building management systems are now routinely networked to other systems including IT data centers, remote access servers, and public utilities. Many proprietary technologies have been phased out in favor of industry standard solutions. This has resulted in substantial growth in the use of open protocols.

While these innovations offer real benefits to iBMS consumers, their use requires careful assessment of their impact on security. To mitigate the security risks, organizations should apply best practices for securing their systems.

This module presents the key aspects of securing an iBMS throughout the design, installation, and operating phases of its lifecycle. Best practices for addressing various aspects of security are described, including network infrastructure protection, threat detection and mitigation, and device hardening. The goal is to provide responsible parties with the basic knowledge to develop a comprehensive plan that addresses the iBMS security needs of their organization.

The information presented is general and should not be interpreted as a one-size fits all approach to security. Any well-balanced security plan takes into account the size of the facility, the impact of a potential breach, and projected installation and operation costs. Each organization should evaluate its tolerance for risk, quantify its willingness to invest in mitigation measures, and act accordingly.

Design for security

The primary focus of the design phase is to establish a boundary around the iBMS and provide ways to control and monitor access. The decisions made during this phase determine many of the security options available in later phases. Therefore, it is essential to solicit input from the people who will be responsible for the installation and operation of the system. Physical security, network infrastructure and device selection are important elements of the design process.

1. Physical Security

No security plan is complete unless it addresses the need for physical security. Physical security prevents unauthorized access to the iBMS devices, networks, and information. Without it, intruders have the means to circumvent all other methods of protection.

Consider the following when making design decisions:

- Combine multiple barriers to access; such as building, room, and cabinet access control.
- Locate mission critical devices in access controlled areas or in locked cabinets. Prevent unauthorized physical access to network devices such as routers, firewalls, and switches.
- Protect communication cable runs with conduit or ruggedized cable chases.

2. Network Infrastructure

The network is the conduit that allows information to flow between the iBMS, the enterprise system, and the outside world. Intruders able to tap into the network can disrupt the flow of information. The example architecture diagram on the next page illustrates these practices.

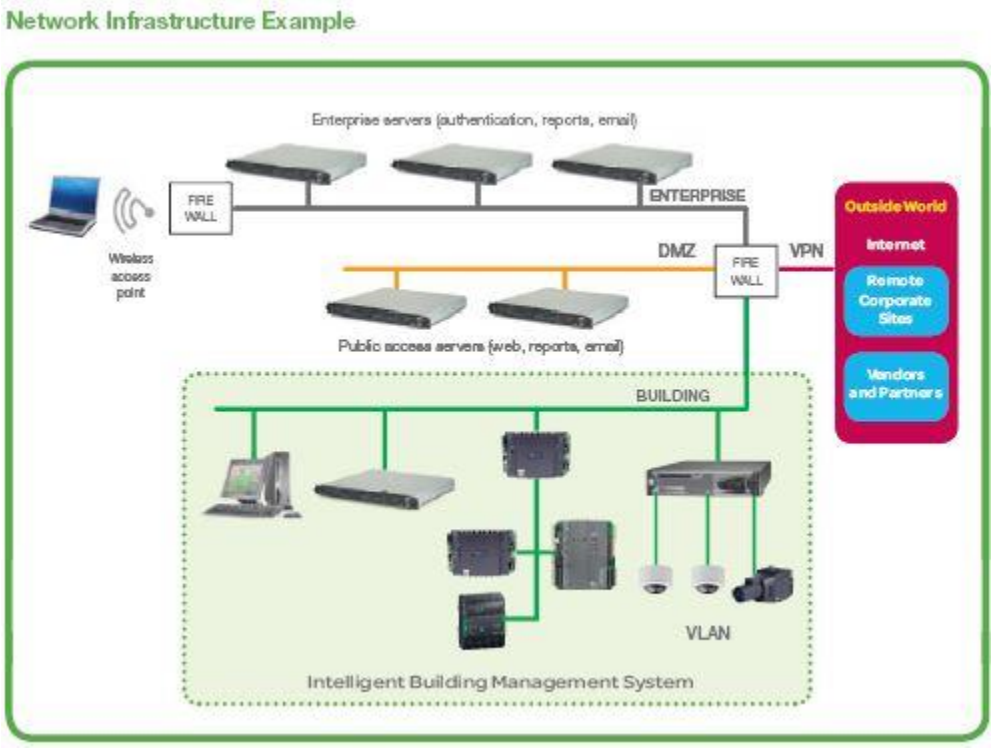


Fig 2: Example of a Network Infrastructure

Limit Network Access Points

iBMS should be isolated as much as possible. Locating it on a virtual local area network (VLAN), for example, ensures that building traffic, including broadcasts to all nodes, remains within the logical boundary. Each network entry and exit point must be secured. By granting access only when a valid reason exists, risk can be minimized and keep security costs down.

Installation of close circuit cameras

Cameras should be in sync with iBMS system in monitoring of overall building .Cameras should be connected through LAN and provide continuous display of every in and out from security check point.

Use Firewalls to Control Access

Firewalls contribute to security by controlling the flow of information into and out of network entry points. Using a set of user defined configuration rules; a firewall determines which traffic will be allowed to pass through and on to the network. Traffic that doesn't satisfy the configured rules is rejected. A single best practice applies to adding firewalls to your network design. Place a firewall at every transition point into or out of the iBMS network. Providing recommendations for the proper selection and placement of firewalls is a detailed endeavor and is beyond the scope of this document.

Manage User Access

Secure user access is achieved through the use of authentication and authorization. Authentication is the means by which a user's identity is confirmed. Once authenticated, a user is authorized to perform certain functions as defined by their role within the organization.

- Restrict user access by capitalizing on solutions commonly deployed by IT departments, such as Central Authorization, Password Control, User Management, and Network Monitoring. Examples include Active Directory, Kerberos, and Radius.
- Further restrict user access by establishing authorization requirements for individual devices such as routers, servers, embedded controllers, and workstations. The type of device will dictate the best approach.
- Consider stronger authentication methods for critical host devices such as:

Smart Cards or USB tokens

Biometric Authentication limits access based on a physical or behavioral characteristic such as a fingerprint. Two-Factor Authentication limits access to users with both a password and a physical token.

Restrict Remote Access

Providing iBMS access to remote users presents a unique set of security challenges. Addressing these challenges requires building additional protections into the network infrastructure. Even then, remote access should only be considered for systems that already have sufficient protection against external threats. Best practices for providing remote access include:

- Use a secure connection, such as a VPN, which provides encryption and authentication of remote sessions.
- Use secure protocols and applications such as HTTPS, SSH, and SCP/SFTP whenever possible and avoid Telnet and FTP.
- Evaluate the risks associated with SNMP (Simple Network Management Protocol) before incorporating it into your design. When using SNMP, limit access to authorized system administrators with known IP addresses.
- Restrict remote access by using Two-factor Authentication and by limiting access to required users only, such as system operators.

- To provide public access to information, create a demilitarized zone (DMZ), place a server within the zone, and mirror the required information onto the server.

Wireless Technology

Wireless networking technology offers several advantages over wired technology including lower installation costs and greater design flexibility. These advantages must be weighed against the increased security risk associated with its use. Best practices for the use of wireless technology are as follows:

- Choose wireless devices with built-in firewalls and support for the highest level of encryption available.
- Harden wireless access devices by following these steps:
- Replace the default administrator name and password with strong alternatives.
- Change the default System ID (SSID or ESSID).
- Disable all identifier broadcasting.
- Enable user authentication such as directory services or 802.1X.

Install with Security

In preparation for system installation, consider the following:

- Throughout the installation process, the iBMS may be particularly vulnerable to attack.
- Update new and legacy equipment with the latest security patches.
- Security measures, particularly those designed for enterprise networks can sometimes interfere with proper iBMS function. Anti-virus software, for example, has been known to disrupt workstation performance by consuming large amounts of processor time. While this occurs infrequently, it is important to have a method in place for evaluating system performance as security features are brought online.

The goal in this phase of the process is to properly configure the security features of each system component. Configuring firewalls, hardening system devices, configuring user accounts, and enabling threat detection are all tasks that contribute to secure system installation.

Configure Firewall Rules

Firewalls use a set of rules, established by the user, as the basis for determining which traffic is allowed to pass in or out of the network. For example, a rule might block all access to a specific IP address or port. Proper configuration of firewalls is essential to securing the network and should only be performed by experienced personnel. Best practices for configuring firewalls include:

- Use a combination of rules to both permit authorized traffic and deny unauthorized traffic.
  A typical approach is:
  - Create rules that explicitly deny access
  - Add rules to permit only the required access

- Add a broad-based rule to deny access to all remaining traffic
- Confirm that the firewall can detect TCP "SYN-flood" attacks by tracking the state of a TCP handshake (stateful firewall).
- Include rules to restrict outbound network traffic in order to minimize the spread of damage in the event of a breach.

3. Selection of Devices

Evaluate each device to determine what ports and services are available, and whenever possible, disable any that do not have a planned use. Port scanning applications can help expedite the identification process. Be sure to disable ports and services that were used temporarily for device commissioning but won't be needed during operation.

Removable media, such as USB memory sticks and compact discs, are often the source of malicious software. The safest solution is to prevent the use of all removable media, by mechanically blocking ports, for example. For those applications where removable media is necessary, take measures to restrict port access and enforce media checking procedures (i.e. anti-virus scans).

Enable the security features built into each device including encryption, firewall capability, access control, intrusion detection and prevention, and user authorization.

Host Devices

- Install anti-virus software from a reputable vendor (i.e. Symantec, McAfee) and enable its automatic update features.
- Install and configure firewall software.
- Enable automatic operating system updates. Centrally managed updates are preferable.

Configure User Accounts

User accounts establish access levels to the domains within a system. Best practices for configuring user accounts include:

- Replace all default vendor passwords with strong alternatives (twelve characters minimum with a mix of letters, numbers, and symbols). Likewise, remove all default logins (i.e. administrator) and system IDs.
- Disable every user's access to the system by default and add permissions only as required.
- Restrict each group of users to the lowest level of privileges necessary to perform their role.
- Prevent duplication of passwords across multiple sites.
- Use expiration dates to require users to periodically change passwords.

Enable Threat Detection and Mitigation

Measures to detect and limit the impact of security breaches are an important component of any security plan. Consider the following best practices for detecting and mitigating threats:

- Create logs to monitor all aspects of the system including physical access, network activity, device activity, and firewall configuration. Consider system performance when setting logging parameters and collect log files in a central location to prevent unauthorized modification.
- If you are using an intrusion detection system, take the time to thoroughly understand the capabilities and limitations of the system you selected before configuring the alerts and active response rules that will govern its operation. Configuration rules should reflect the operating behavior of your network which may differ significantly from those of a typical enterprise network.

Operate Securely

The need to address IT security does not end once a system has been installed. System monitoring, account management, patch management, and firewall maintenance are all important to operating a system securely.

Monitor the System

Through vigilant monitoring of system parameters, security breaches will be detected earlier and steps to limit the spread of damage can be taken. Monitoring guidelines include:

- Treat alerts from intrusion detection systems with the highest priority.
- Proactively scan the network for new hosts and out-of-date systems.
- Routinely review system logs for irregular activities. Indicators such as numerous failed login attempts, unusual credential card use, and increases in network load can provide early signs of a breach.
- Create an incidence response plan which describes the actions to be taken when system irregularities are detected.

Maintain User Accounts and Access Lists

When a user changes flat or leaves altogether, it is important to have a documented procedure in place to remove or alter the level of access they have to the overall system. The procedure should address all types of access including physical, remote, network, and device level access.

Manage Security Patches

Security patches provide protection against the never-ending flow of new threats. A good patch management plan combines policies, procedures, and qualified personnel in an effort to close security gaps without major disruption to the system. Best practices for patch management include:

Take Inventory

List of the devices that will require periodic security updates should be maintained. The list should include network devices such as routers, firewalls, and VPN concentrators, as well as application and operating system software.

Use Trusted Sources

- Vendor issued firmware updates, service packs, and hot fixes should be used.
- Whenever possible, use patches with digital signatures. A digital signature validates a patch's source and integrity.
- Stay up-to-date on newly released patches and vulnerability reports.

Develop a Plan for Installation

A patch installation plan should include the following:

- A method of prioritizing patches. Most patches are routine updates that can be implemented according to a schedule. Others require immediate action to close a critical gap in security.
- Pre-approved patch installation tools that provide change management and security audit features.
- Procedures for vendor certification of patches, testing of patches prior to installation, and a staged installation process to minimize the risk of disruption from the change.
- The verification of digital signatures. Signed security patches should be verified just prior to installation to ensure that they have not been tampered with internally.

Develop a Backup and Recovery Plan

A backup and recovery plan should identify responsible parties, list the items to be backed up, and provide specifics such as backup intervals, locations, and number of versions to retain. Verify that recovery procedures work as expected.

Firewalls Require Special Attention

Firewalls must be properly managed by trained personnel to ensure continued system security. A firewall management plan should be developed to address the following requirements:

- Regular review of firewall configuration
- Strict change control measures
- Continuous monitoring of logs and relevant statistics

Build iBMS Security Awareness

Personal training is the key to building awareness about the role each person plays in maintaining security within a building. Training should include:

- Proper handling of account credentials
- Roles and responsibilities of each person in maintaining security
- Reasons behind various security policies and procedures
- Ways to recognize and respond to attempts by others to garner private information for the purpose of compromising a system (social engineering).

Security training works best if participation is mandated and the training itself is monitored for effectiveness.

Perform Security Audits

Periodic security audits provide the means to ensure that systems, policies, and procedures devoted to security are effective and that no gaps exist. Security audits may include:

- Attempts to gain network or server access (penetration testing)
- Evaluation of past breaches to determine if potential for exploitation has been eliminated
- Attempts to acquire passwords from users
- Checks to verify that security procedures are being followed and security systems are not being bypassed
- Assessment of protection against new types of threats

An effective audit provides a comprehensive assessment of an organization's security and informs an ongoing process of improvement.

Smart Buildings - Energy Management

Almost 70 % of total generated electricity is consumed in buildings. Nowadays in buildings we have humans and IT equipments which consume a lot of energy such as desktop computers, monitors, printers, and servers; they are of mixed use today. A modern mixed-used building typically has four major energy-consuming subsystems:

- Lighting
- IT equipment
- HVAC and
- Miscellaneous plug-load devices

Energy consumption of lighting, often thought of as quite significant, is actually low, while HVAC and plug-load devices (which include IT devices) are the major contributor. Various devices are left powered on irrespective of definite use or requirements. Computers and monitors powered on whole day even when they are not being actively used; this is also the case for several other plug-load devices, such as desk lamps, space heaters, and fans.

The energy consumption of HVAC and plug load devices has concerns for both energy costs as well as the environment, and going forward this problem will only get worse. Therefore, the solution for smart building should reduce energy usage, and should have control over the HVAC system and plug-load devices.

Building actuation is the ability to directly control the operation of various building systems (e.g. turning off HVAC or turning off a plug-load device), with one of the crucial goal being the reduction of energy consumption by shutting off idle equipment and reducing energy waste. This is important for two reasons. First, for energy efficiency reasons, simply powering off excessive loads will reduce overall energy usage while faintly impacting building inhabitants. Second, reducing energy heaps during times

of peak-demand to the grid can lead to considerable money savings. This ability of reducing energy usage, called *demand response*, will be important for utilities going forward. Being able to actuate different building subsystems, both for energy efficiency and demand response reasons, is therefore of critical importance in the design of a smart building.

In this paper we tried to describe several energy-saving architectures that can be developed to actuate the IT equipment such as PCs, and other plug-loads for a building. We also discussed about the challenges that needs to be faced if we truly want smart buildings a reality.

IT Equipment and Lighting

Actuation for IT equipment such as computers might not be best done through direct plug-load control. Instead software can be installed on individual computers that allow access to the power management features of the system. Specifically, the software will be able to put the computer to power saving sleep modes. This functionality can be combined with *occupancy sensors* to reactively put the computer to sleep when the user is no longer occupying the room.

One issue that arises when putting computers to sleep is that they lose all network connectivity when in sleep mode. This problem discourages people from putting their computers into sleep. To solve this, we can use the *Sleep Server architecture* that allows computers to go to sleep while maintaining network connectivity.

Techniques to manage lighting loads have already been extensively examined in both industry and in research. Electronic ballasts have been used to facilitate demand response management for light fixtures while centralized lighting controls can be used to remotely actuate installed lights throughout the building. Coupled with occupancy and user context, the smart building server can also turn off or reduce lighting when a room becomes unoccupied.

Miscellaneous Plug-Load Devices

Actuating plug-load devices is also important towards improving building energy efficiency. Many devices are left on, even when the user is not present, and thus significant aggregate energy is wasted when all of these devices are accounted for. A natural way to remotely actuate devices is at the level of each outlet; a connected plug-load meter such as Synergy Energy Meter (SEM) can disconnect the electricity and shut off the device.

A mechanical relay is connected to the MSP430 in SEM that allows it to turn on or off the electrical load plugged into the meter, while our software allows remote management over the wireless network.

The smart building server can utilize occupancy to determine when to control plug-load devices. For certain types of devices, this can make sense - lamps and monitors for example can be shut off when their locations become unoccupied without any significant impact. As the occupancy changes are

detected, the smart building server will send commands to turn off or on the connected device to the energy meter.

Architecture

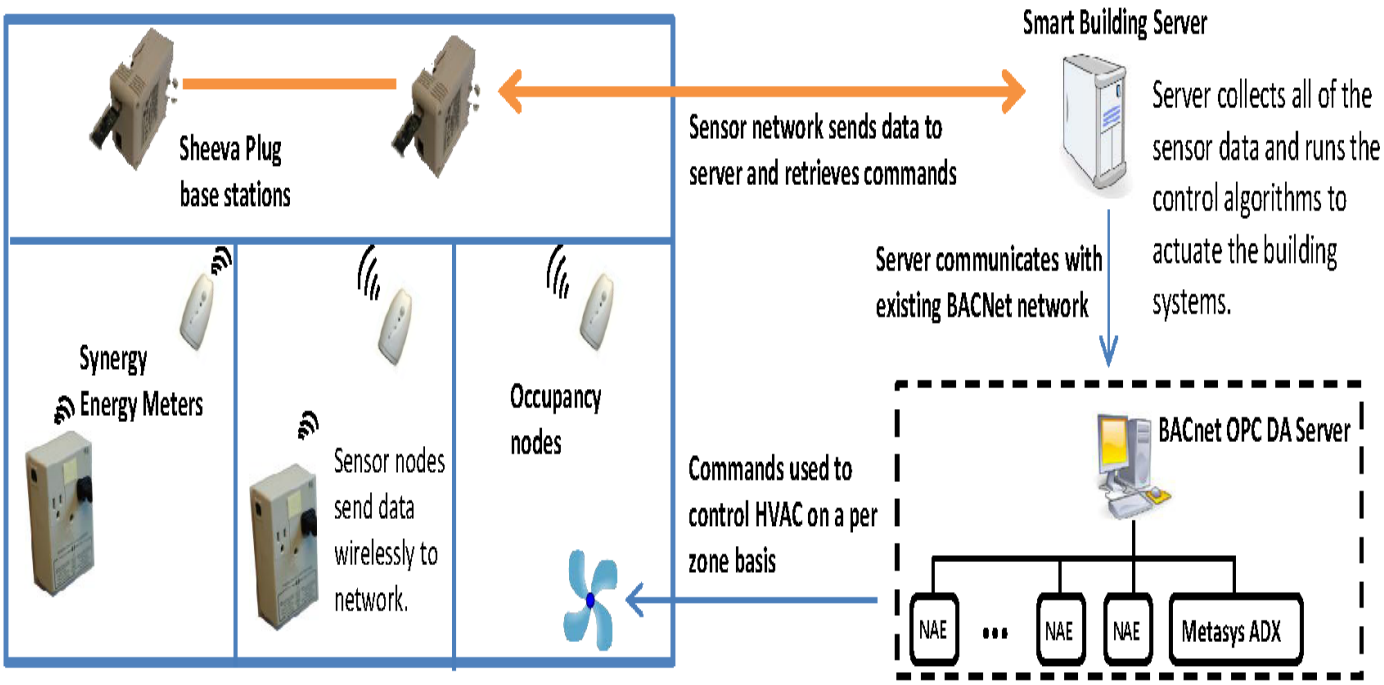


Fig 3: Overall architecture of the building actuation system, including the smart building server, wireless sensor nodes, base station, and connection to the facilities.

Sensor Variables

When specifying an occupancy sensor, the below variables are relevant.

Technology	Choose method of motion detection that will best meet the application need.
Sensitivity	Determine how sensitive the sensor should be to movement so that it effectively detects minor and major motion without nuisance switching (false-on/off). Sensors are now available which provide automatic adjustments of time delay and sensitivity. In these models, manual set-up and subsequent adjustments are unnecessary.
Coverage area	Specify range (ft.) and coverage area (sq.ft.) for the motion detector based on the desired level of sensitivity.
Mounting	Locate the sensor for maximum effect.

Time delay	Determine how long the sensor should wait before turning out the lights when the space is unoccupied to be convenient for users but also maximize energy savings. Sensors are now available which provide automatic adjustments of time delay and sensitivity. In these models, manual set-up and subsequent adjustments are unnecessary
Cut off	Determine whether the occupancy sensor's coverage area must be restricted so that it will not monitor adjacent areas that should not be monitored (such as a hallway outside a controlled private office).
Special features	Specify special features for the sensor based on available offerings from manufacturer and application need.

Table 1: Sensor Variables

Position of sensors

Mounting Configuration	Description
Ceiling	Appropriate for large areas that feature obstacles such as partitions, in addition to narrow spaces such as corridors and warehouse aisles. Units can be networked for control of areas that are larger than what can be controlled by a single sensor. Typically 2-3 times higher installed cost than wall switch sensors, but can be very economical for controlling large zones.
High wall and corner	Similarly appropriate for coverage of large areas that feature obstacles.
Wall switch (wall-box)	Appropriate for smaller, enclosed spaces such as private offices with clear line of sight between sensor and task area. Relatively inexpensive and easy to install.

Table 2: Sensor Positions

Comparison between US, PIR and DT sensors

Mounting Location	Sensor Technology	Angle of Coverage	Typical Effective Range*	Optimum Mounting Height
Ceiling	US	360º	500-2000 sq.ft.	8-12 ft.
Ceiling	PIR	360º	300-1000 sq.ft.	8-30+ ft.

Ceiling	DT	360º	300-2000 sq.ft.	8-12 ft.
Wall switch	US	180º	275-300 sq.ft.	40-48 in.
Wall Switch	PIR	170-180º	300-1000 sq.ft.	40-48 in.
Corner wide view	PIR/DT	110-120º	To 40 ft.	8-15 ft.
Corner narrow view	PIR	12º	To 130 ft.	8-15 ft.
Corridor	US	360º	To 100 ft.	8-14 ft.
High mount	PIR	12-120º	To 100 ft.	To 30 ft.
High mount corner	DT	110-120º	500-1000 ft.	8-12 ft.
High mount ceiling	DT	360º	500-1000 ft.	8-12 ft.

*Sensitivity to minor motion may be substantially less than noted above, depending on environmental factors.

PIR = passive infrared, US = ultrasonic, DT = dual-technology

Table 3: Comparison of Sensor Technology

The future smart buildings must be able to reduce its energy usage, and effective control over the lighting system and plug-load devices. We define building actuation as the ability to directly control the operation of various building systems (e.g. turning off lighting or turning on a plug-load device), with one of the key goals being the reduction of energy consumption by shutting off unused equipment and eliminating energy waste.

This is important for two reasons. First, for energy efficiency reasons, simply powering off unnecessary loads will reduce overall energy usage while minimally impacting building occupants. Second, reducing energy loads during periods of peak-demand to the grid can lead to substantial monetary savings. This ability of reducing energy usage, called demand response, will become a priority for utilities going forward. Being able to actuate different building subsystems, both for energy efficiency and demand response reasons, is therefore of critical importance in the design of a smart building.

Two current standards exist that are popular for wireless sensor networks in buildings - *ZigBee* and *6LowPan*; both utilize 802.15.4 radios and are geared towards low-power wireless networks.

Smart Buildings - Fire Detection and Alarm Systems

The main aspect of fire protection is to check and identify a developing fire emergency system in a timely manner, and to inform the building's residents and fire emergency services. The anticipated fire scenario, building type, number of occupants, contents and mission can provide several main functions. They provide a means to identify whether the fire developed through manual or automatic methods and second, alert building occupants for evacuation. Transmission of an alarm notification to the fire department and shutting down of electrical, air handling equipment or special process operations is an important facet of the system.

Control Panels

Control panel is the spearhead of fire detection and alarm system. Responsible for monitoring the input devices such as manual and automatic fire detection components, and then alarm activation devices such as warning, lights, horns, emergency diallers, and building controls. Control panels may range from simple units with a single input and output, to complex computer driven systems monitoring several buildings over an entire campus.

There are two main control panel arrangements:-

1. **Conventional fire detection and alarm systems** (point wired) were the standard method for many years providing emergency signalling. In a conventional system one or more circuits are routed through the protected space or building. One or more detection devices, along each circuit are placed. In conventional alarm system, all alarm initiating and signalling along with system's hardware including multiple sets of wire, relays (closing and opening), and assorted diodes. Due to this arrangement, these systems are actually monitoring and controlling circuits, and not individual devices.

2. **Addressable systems** (intelligent) represent the current state-of-the-art in fire detection and fire alarm technology. Monitoring and controlling capabilities of these systems include initiating and signalling each alarm device by using microprocessors and system software. Therefore each intelligent fire alarm system is like a small computer operating a series of input and output devices.

A constant signal sent by microprocessor over circuit initiating device to inquire its status. An active monitoring occurs rapidly, providing regular updates after 5 seconds. The fault detection is also done by the addressable system monitoring the condition of each circuit, identifying any faults whatsoever. It provides the capability to specifically identify fault location and initiation of mitigation process.

If a fire alarm detector recognizes a condition indicative of a fire, a quick reset by the control panel is attempted first. In case of a genuine smoke or fire condition, detector re-enter alarm mode in quick succession of reset attempt.

These systems offer many advantages over conventional used systems. Ability to monitor the status of each detector and as a detector becomes dirty, the capability of the microprocessor to recognize decreased capability, thus providing maintenance alert. This feature, known as **Listed Integral**

Sensitivity Testing, allows facilities personnel thus servicing only those detectors that specifically need attention rather than time consuming cleaning of all units.

We can use the advanced systems like FCI 7200 for the maintenance power system using the features like drift compensation. The detector sensitivity adjusted to check for dust conditioning. It helps to check the hot detector condition which can result in obscuring detectors optics. The control panel alerts maintenance for service procedure.

Modification of these systems like adding or deleting the detector, uses connecting or removing the device used for addressable circuit and it brings a change in memory section. The member section uses panel as personal computer with the information downloaded in the microprocessor of the panel.

3. Flame Detectors

Flame detectors are the third type of automatic detection system and this imitate human sense of sight. They operate on the Technologies like infrared comma ultraviolet or combination of these two Technologies. Approximately 4000 to 7700 angstroms of operational energy is used to indicate the range of this system sensing equipment recognize this fire signature and send a signal to alarm panel.

The main advantage of the smoke detector system is the ability to identify fire which is still in its Inception. Due to this they provide additional opportunity to the emergency first now for responding and controlling the Fire before sever damage Packers they are preferred detection method for life safety and higher value application. The main disadvantage of smoke detectors is that they are very expensive to install as compared to the thermal sensors and are resistant to INR advertent alarms still when properly selector and design they are very reliable for fire detection system and have low probability of false alarm.

Advantage of flame detection is their reliability even in case of hostile environment .The high value energy and transportation applications employs this technique where the reliability of other similar detectors is very low.

The main disadvantage of low flame detection Technology is that the very expensive and labor intensive to maintain. Flame detectors must be look directly at the fire source where is the thermal and the smoke detectors can identify the fire signatures from distance.

The addressable systems have unique operating characteristics which can be of disadvantage for these systems. Therefore the service technicians required for this type of flame detection Technologies must be properly train before employing them in this field the training program which can range from 3 to 4 days course is very necessary and on continuous rate because of new method developed recently.

Alarm Output devices

After receiving an alarm notification, the fire control system must tell somebody that an emergency is underway. This is the main function of fire alarm system the signaling components here mainly consists of audio and visual alerting system components and are composed of primary alarm

output devices. Mainly the component used for fire alarm sounding devices is bells, horns, chimes etc. Bells are appropriate for most of the building needs and applications. Horns are well-suited where loud alarm devices are required. Chimes are mainly used for soft alarm tone preference such as Healthcare facilities and traders. Speakers are also use alarm sounding option and suited for large multi-storey building. Visual alerting system are required in places where is levels are quite high or hearing impaired equipment are present.

Another Function of output function is emergency response notification. The most common of this include telephone and radio signal which can be communicated constantly true monitoring centre.

There are other output functions like shutting down the electric equipment such as computers air handling fans and shutting down operation such as chemical movement through piping in alarm area. We can also activate fans to extract smoke which is a common function in these type of situations. We can also activate that start of gaseous fire extinguishing systems or sprinkler system.

Fire sprinklers

This is direct application techniques of water onto flames and heat in case of fire sprinkler which causes the cooling of combustion process and prevents the ignition of adjacent combustibles. This system is most effective during the initial frame growth when the fire is very easy to control. If properly selected fire sprinkler can detect the fire heat and begin The Separation process within moments after flame appears. This will help India result significant left damage otherwise without the sprinklers.

The main benefit of the fire sprinkler systems are:

1. Identification and control of a developing fire: system response at all times under control is instantaneous
2. Immediate alert: the system will notify the occupants immediately and the emergency response
3. Less heat and smoke damage: very less smoke and heat damage occur when the fire is extinguished in the early phase
4. Life safety: the staff, visitors and fire fighters will have less danger since the fire is checked
5. Design flexibility: fire control system help to minimize the demand on 5 for smoke barrier placement there is a lot of permissibility design and operation based on presence of fire sprinkler system
6. Enhanced security: less demand on security forces thus minimizing intrusion and theft opportunities
7. Less insurance expenditure: Insurance underwriter will offer let's premiums in the case of Sprinkle protected property

Water Mist Technology

This is one of the most promising automatic extinguishing technologies available to the industry as well as common public employing fine water droplets for Mist system. NSPA 750 defines three

pressure results for water mist Technologies: low, intermediate and high pressure system. Marioff's rigorous testing system shows that the high pressure water mist Technology constantly delivered on following points:

- Better penetration in the seat of the Fire
- Superior coverage the volume
- Improved cooling effect with better mixing of gases and evaporation rate
- Low system weight
- Less water consumption

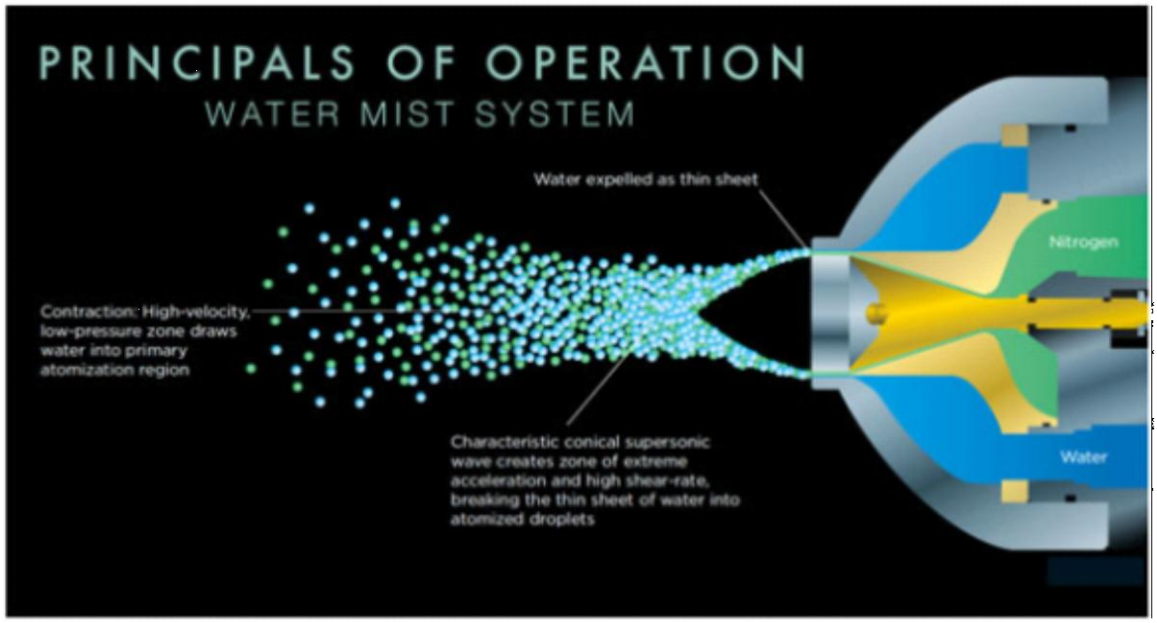


Fig 4: Water Mist technology- Operating Principle

The potential locations where the system can be used are the places where reliable water supply is nonexistent, places even the water sprinkler discharge are very high and the building where the construction and aesthetics do not allow usage of standard water sprinkler system. Mist system also appropriate for environmental concerns and demise of Halon 1301 gases.

This system has been approved by number of domestic as well as International marine organizations for land based applications, with listings in European countries where their effectiveness is recognized. Some of these systems are also used in the North American countries for land based uses.

Mist discharge based systems employ limited water quantities at higher pressures than sprinkler system. The pressure ranges from 100 to 1000 psi with the high pressure reducing large quantity of fine spray. The produce droplets are in the range of 50 to 200 microns in diameter resulting in exceptionally high efficiency cooling and fire control. With less water requirement Hindi kisses approximately 10 to 25% of standard water volume is required so the water saturation which is mainly associated with the

normal firefighting procedure is highly reduced benefit associated with Mist based fire safety system is lower aesthetic impact and less environmental effect.

Typical water Mist system consists of following components:

1. Water supply: Based on piped building system or dedicated tank management. Other options include dedicated water or nitrogen storage cylinders which can be used for Limited duration.

2. Piping and nozzle: For low pressure system generally 20 to 35% smaller sprinkling piping is used, for high pressure the piping is even smaller with 0.50 to 0.75 inch diameters as per norm. Nozzles are activated automatically by the fire seat and of automata to cover a certain size.

3. Detection and control equipment: Mist discharge can be controlled by selecting highly intelligent detector system such as advanced technology of VESDA smoke detection system. These systems are state of art fire detection technology which provides very early warning in case of a fire development.

Drawback of the mist system:

The main drawback of the mist system is the high cost which can be in the range of 50- 100% higher than the standard fire sprinkler. This can be possibly reduced by installation of labour savings. In the rural applications where reliable sprinkler systems are expensive, mist technology based fire sprinklers can be compared with less costly. Also contractors who are associated with this technology are limited.

Integration of Fire Alarm system with Smart Building systems

Today's fire alarm systems are partially integrated with the building systems. In case of fire occurrence, fire detection and alarm system activate various fire safety measures like smoke control pressurization and smoke exhaust system. They also activate elevator recall, release system, flashing of exit signs and fire suppression system. However the integration of these systems with the building is at a very nascent level. In spite of having similar functionality between building service system and fire safety systems and security systems, or HVAC systems and lightning systems, the integration is present but still there is a limited level of Information sharing among these systems. Various building systems don't involve HVAC, lightning fire safety for common communication protocol. The main reason behind this is fragmentation of the building and the communication industry. There is a reluctance to change the established practices as well as lack of standardization the communication protocols which don't allow the building systems to communicate with each other. Also many tenants and developers prefer to have less degree of system integration for the favor of excessive complexity and potential system failure or slowdown in central control.

Various methods and concepts are developed to enhance integration of building systems and to increase the reliability of this integrated system. Efforts are also made to enable inter-operability between different Communication protocols. The most commonly used protocol are BACnet, LonWorks,

CAN, NEST, EHSA and CAB. These protocols have a detailed set of rules and procedures to follow for all communication aspects.

BACnet prefers hierarchical communication system model in which whole system is divided into number of subsystems each having separate Central Processing Unit. Coordination between these subsystems is activated by hardware interconnection. This method simplify the maintenance and the damage caused by the CPU is only limited to local level. This system is suitable for traditional processing and communication. However BACnet doesn't support dynamically structured network.

Other Communication protocols like LonWorks preferred network integration as there is no centralized Processing Unit. There is employment of just intelligent field cabinets. Each intelligent cabinet works as node of the system and have people status as to the other nodes, and controls local as well as zoned energy management systems all alarm functions as well as smoke control functions. Microprocessors employed are able to support advanced diagnostics and manage local building functions. Nodes are able to communicate with each other and are accessed through a central station. This type of network integration helps to check affected area, and fire command station is able to communicate with other fields cabinets on the network loop by transmission of data on two directions. Response is very fast in this case because there is no need for the CPU to scan and process the whole system.

Smart Buildings - Water Management

Smart water management (SWM) can assume a key part in the change of urban areas of formed and forming nations into smart and sustainable cities (SSC), if satisfactory strategies, stern management, and expansive partner inclusion are coordinated into its arranging and usage. Through continuous observing, productive operation, enhanced choice making, and upgraded execution and management conveyance, SWM can guarantee that a city's development is not accomplished to the detriment of its water assets. Further points of interest, for example, expanded income in utilities, diminished operational expenses and expanded open association place SWM as a practical, smart reasonable answer for location urban water challenges and to make urban communities smart.

As developing encounters recommend, activities on Smart water frameworks have been more viable when actualized as a feature of more extensive vital ways to deal with water management. Hence, endeavors in this field must be facilitated and cooperative energies worked over the different areas and partners included in water management. In the meantime, encounters have exhibited that open private associations can be viable in encouraging development. Further endeavors ought to be made to reinforce the linkages between the utilities, commercial enterprises and colleges, keeping in mind the end goal to grow new research on shrewd water management, rising difficulties and opportunities, and in addition novel water ventures.

Recognizing that both specialized and non-mechanical advancements assume a part in the compelling operation of smart water frameworks, it is imperative that ICT improvements are joined by developments in the plans of action of water utilities, and by advancements as far as water use toward the end of the pipes, in order to expand the commitment of ICTs in this field.

Proper strategies and measures are vital to bolster the improvement and arrangement of shrewd water frameworks (e.g. water evaluating, instruction and data, rivalry for non-local customers). In like manner, as smart water arrangements keep on developing and their reconciliation to extend in urban situations, the significance of normal gauges for equipment and programming will keep on rising.

Urban Water Issues

Urban communities depend on numerous utility foundation frameworks that are portray by their many-sided quality, and also by high venture and management costs. In the coming future, it is normal that urban communities and other urban focuses will go up against asset apportioning challenges connected with an expansion in populace stream, vitality issues because of the decrease of fossil fuel assets, picking up speculation overheads, curving upkeep and management costs because of maturing base and shameful area asset use, among others. Smart and new supportable frameworks are required to minimize the effect of these developing difficulties.

In view of the connection introduced up to this point, the procurement of perfect and dependable water constitutes a key zone for the working of urban frameworks. Quick urbanization, destitution and urban rot, frail political management and management, lacking and insufficient foundation, under speculation and valuing issues, are among the key, and commonly re-implementing elements that encroach upon a city's water management framework. These components are further exacerbated by the effects of environmental change and other natural stressors, at last elevating water management challenges, and obliging the accessibility and the nature of urban water assets. The interconnected and dynamic nature of urban water management challenges is illustrated in Figure 5:

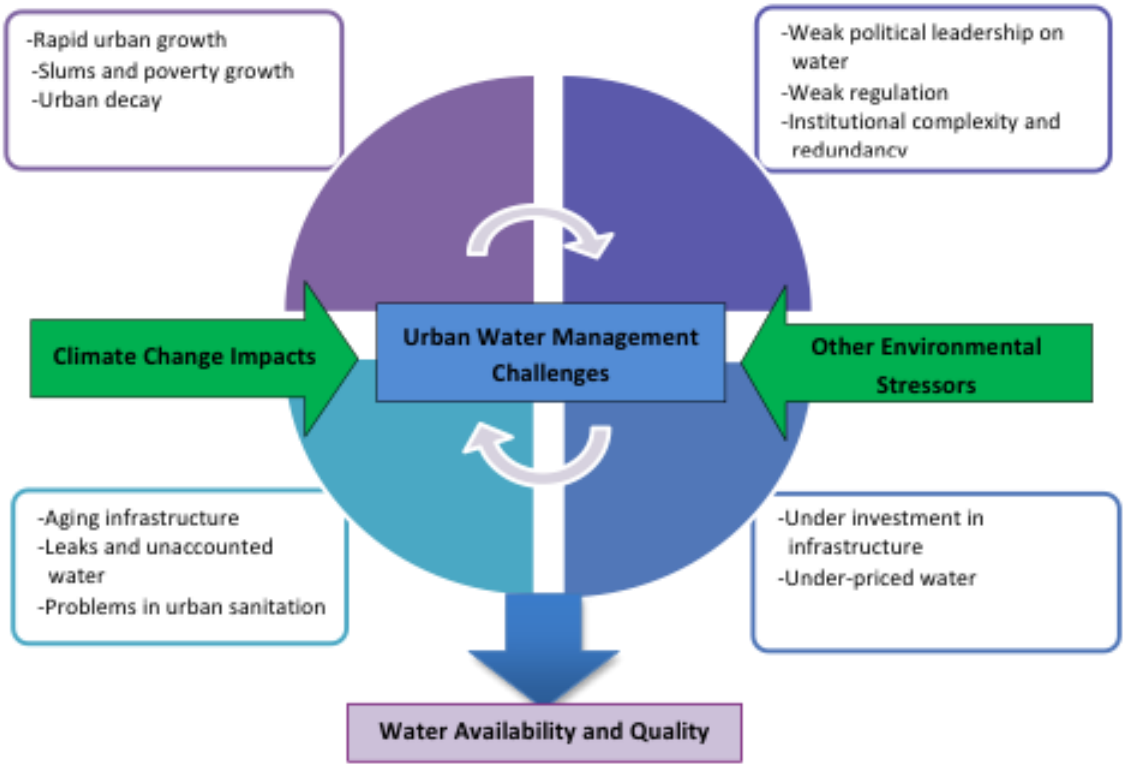


Fig 5: Influencing factors on urban water management challenges

Smart Water Management in Smart Cities

Water management is nearly connected with water asset improvement and ecological assurance, and it likewise involves appropriate management of the interest for open managements and cost viability. Hence, urban water management must guarantee access to water and sanitation base and managements oversee rain, waste and tempest water and additionally overflow contamination, relieve against surges, dry spells and water borne illnesses, while in the meantime protecting the asset from debasement. As recognized in the past segment, quickened urbanization, particularly in the creating scene, combined with expanding attentiveness toward water security despite environmental change and maturing base, have tested the powerful execution of these procurements. In today's incorporated worldwide economy, developments in information transfers have made a significant chance to address these water challenges inside of urban communities, whilst enhancing urban water management.

Perceiving the difficulties confronted by the water segment, partners from the scholarly world, enterprises and the ICT division has created water knowledge instruments that utilization ICTs to reduce urban water issues. The pretended by smart water frameworks in advancing the proficiency, viability and adaptability of water and wastewater base resources and their

management constitutes a subject of expanding consideration. ICTs offer significant chances to enhance the profitability and effectiveness inside of the water division, with the point of adding to the maintainability of the asset. These advancements permit the nonstop checking of water assets, giving ongoing observing and measuring, making upgrades in demonstrating and issue finding, in this manner empowering legitimate upkeep and improvement of all parts of the water system.

The expanding accessibility of more shrewd, ICT-empowered intends to oversee and ensure the planet's water assets has prompted the advancement of Smart water management (SWM). The SWM approach advances the practical utilization of water assets through co-ordinated water management, by coordinating ICT items, arrangements and frameworks, went for augmenting the financial welfare of a general public without bargaining the earth. SWM can be connected to numerous divisions (e.g. commercial ventures, agribusiness) and urban situations.

In urban communities, SWM endeavors to accomplish three fundamental objectives through the usage of ICTs, in particular:

(a) Coordinated water asset management and circulation,
(b) Upgraded ecological assurance, and
(c) Feasible procurement of open managements and monetary endeavors.

Inside urban situations, the usage of SWM can make huge changes in water conveyance, diminishing misfortunes because of non-income water, and upgrading waste-water and tempest water management.

The part of SWM water quality and unwavering quality, guaranteeing legitimate management of green frameworks, diminishing water misfortune because of spillage, lessening operational expenses, and enhancing client control and decision. These enhancements expand the proficiency of the water division, while adding to its financial manageability since districts and water utilities are better ready to recuperate costs from non-income water, including the location of illicit associations.

SWM tools can be categorized in the six main areas listed below. It should be noted that the examples provided are not limited to these areas, but may overlap several others, as seen in Figure 6.

1. Data acquisition and integration (e.g. sensor networks, smart pipes, smart metres).
2. Data dissemination (e.g. radio transmitters, wireless fidelity (WiFi), Internet).
3. Modelling and analytics (e.g. geographic information system (GIS), Mike Urban, Aquacycle, assessing and improving sustainability of urban water resources and systems (AISUWRS), and urban groundwater (UGROW).

4. Data processing and storage (e.g. software as a service (SaaS), cloud computing).
5. Management and control (e.g. supervisory control and data acquisition (SCADA), optimization tools).
6. Visualization and decision support (e.g. web-based communication and information systems tools).
7. Restitution of data and information to cities' technical services and to the end users (e.g. Tools for sharing information on water and on services).

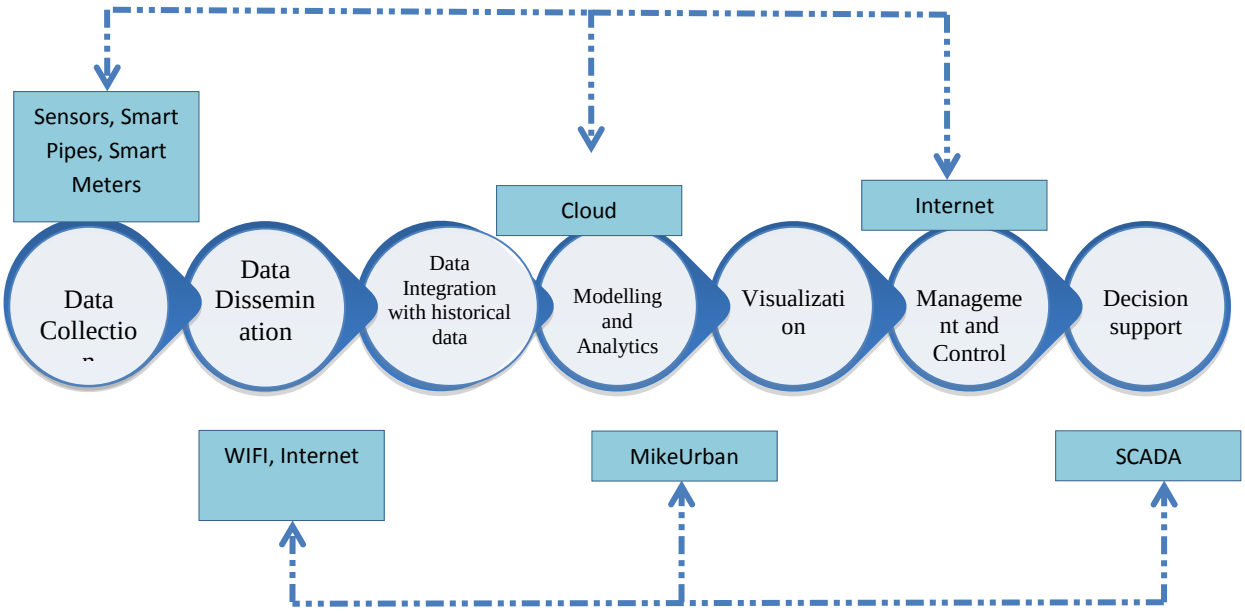


Fig 6: Schematic representation of smart water management technologies and tools

As illustrated in Figure 6, SWM technologies often overlap a series of functionalities that are key for the effective operation of urban water systems. The following section will explore in more detail the role of each of these technologies, and their contribution to SWM.

Smart Water Management Technologies

Smart water Management technologies are currently applied to many different areas of water management, as illustrated in Figure 7.

At the point when connected to urban communities, the accessibility of dependable information to upgrade operations can enhance choice making at numerous levels. Numerous imaginative ICT apparatuses have been created in backing of cutting edge urban water framework frameworks, enhancing execution, expand productivity, and diminish costs, diminish

repetition, and lower natural effects, among others. Some of these Smart advances are clarified beneath:

Smart pipes and sensor networks

Smart channels fuse multifunctional sensors that can sense strain, temperature and weight oddities, and additionally measure water stream and quality amid management, to furnish administrators with constant checking and investigation highlights, while guaranteeing more secure water supply dissemination. Associating Smart pipes with a remote processor and receiving wire empowers information to be exchanged straightforwardly to a war room, furnishing water chiefs with the apparatuses expected to recognize and find potential breaks progressively.

Smart pipes were at first created for the transportation of oil, gas and perilous fluids. Throughout the years, their appropriateness to water systems has gradually been figured it out. New innovative work in models for water appropriation is expected to keep on propelling open water supply frameworks.

Remote sensor systems give the innovation to urban communities to all the more precisely screen, and some of the time control, their water supply frameworks unpredictably utilizing diverse parameters. Some Smart sensors can recognize stream rates down to 0,3 m3/hr (5 liters/minute), empowering early-spill identification and in this way decreasing the danger of channel break. The framework reports pipes stream estimation information with weight and acoustic estimation consolidates this data to GIS information and sends programmed alarms to distinguish the area of conceivable breaks, along these lines permitting the prioritization of repair work.

Sensors can likewise be consolidated to improve the water utilized as a part of watering system, measuring parameters, for example, air temperature, air moistness, soil temperature, soil dampness, leaf wetness, environmental weight, sun oriented radiation, trunk/stem/organic product distance across, wind speed/course, and precipitation. Urban applications range from park watering system to business watering system frameworks, empowering better management and a more exact assignment of water assets between areas.

Sensors can be joined to evaluate the water nature of surface water, and also treated water sewage inside of urban areas. As of now, numerous checking undertakings (e.g. testing the concoction state of water, residue, or fish tissue for quality evaluations) are still directed physically, requiring HR for examining and further lab investigation.

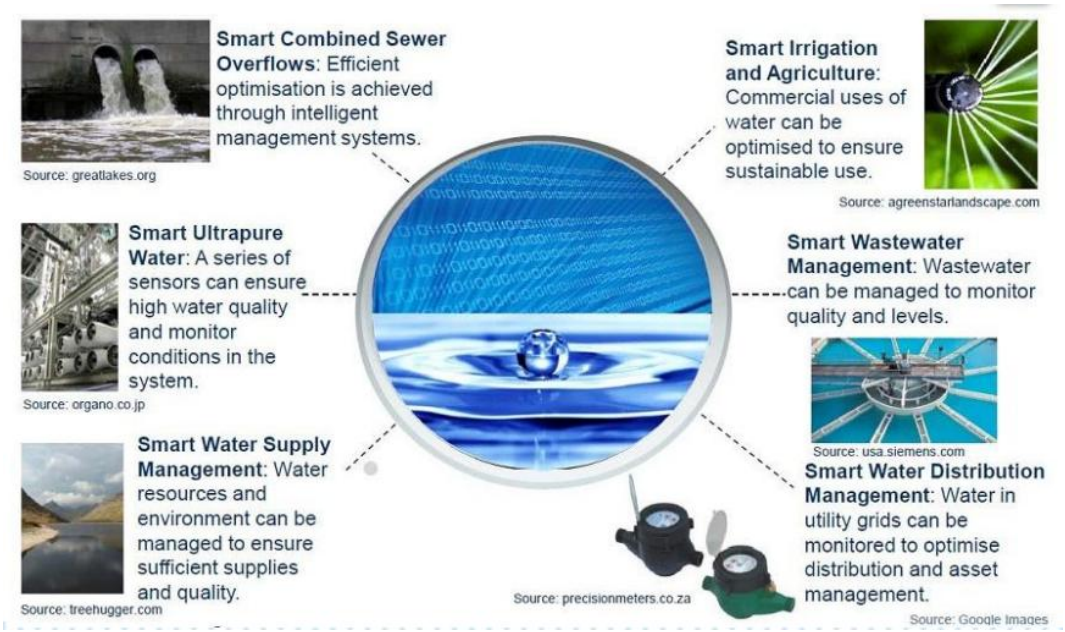


Fig 7: Current implementation of smart water Management technologies and tools

These sensors are connected through smart sensor interfaces like IEEE 1451 standard, with reliable wired and/or wireless network technologies (e.g. WiFi, ZigBee, International Society of Automation (ISA100)), mobile network). Thus, the system is easily expandable to cover the broader water sector. Intelligence is integrated through the use of automatic control technologies and computer technologies, in order to ensure sample pre-treatment, sensor measurement, data collection, processing and analysis, and system communications.

Major tasks for smart sensor networks in water quality monitoring include the following:

- Identify and characterize changes in existing or emerging trends in surface water quality over time.
- Gather information to design or assess specific pollution prevention or remediation programmes, or to provide information in a timely manner to allow quick response to emergencies, such as spills and sewage leakages.
- Determine whether programme goals – such as compliance with pollution regulations or implementation of effective pollution control actions – are being met.

Coordinating smart pipes and sensors inside of the urban framework empowers key capacities, for example, the identification of occasions in light of the observing of stream rate, channel weight, stagnant focuses, moderate stream areas, channel spillage, reverse, and water quality

to be checked, which constitute information expected to streamline the operation of ebb and flow systems.

a. Smart metering

Smart meters are electronic gadgets with cutting advance metering infrastructure (AMI) that backings on-line measuring of electric, warmth, gas, and water utilization. These gadgets are quickly advancing in light of business sector powers and legislative regulations. On account of water utilization, Smart meters ordinarily comprise of an implanted controller that interfaces with a metering sensor, a remote transmitter, and additionally correspondence augmentation and a 10-to-15-years-lifetime battery, as there is no mains control supply accessible for water meters. The meters are associated with a system of information lumberjack which takes into account the persistent observing of water utilization of a city, a building, a business or a home. The advancement of Smart meters empowers a two-way correspondence when required between the meter and a focal framework by transmitting information, which should be possible through various channels (e.g. radio correspondence, power line, Internet, phone). As smart water meters are battery controlled, the principle correspondence channel depends on radio correspondence between the smart meter and the system of RTUs, then on GSM/GPRS (or proportionate) up to the focal framework.

Smart meters commonly gather utilization information, and afterward transmit this information to an entryway that interfaces with the local area network (LAN), home area network (HAN) and wide arear network (WAN).

The LAN comprises of the metrology or estimation capacity of the meter, while the HAN is associated with the clients' system. Because of the showcase elements of HAN, it effortlessly permits availability to utilization information through an easy to understand interface, permitting clients to look at and track their water utilization. As HAN capacities are vitality expending those can be supplanted by a web access to Home Data and gathered by means of the LAN and the WAN. WAN is overseen by the utilities and permits them to track, screen and bill utilization.

Smart metering likewise permits water utilities to give clear water utilization data which can help clients to track and control their water use, and distinguish prompt investment funds on their bills, therefore empowering better dispersion system and utilization arranging because of its continuous observing capacities.

b. Communication modems

Correspondence arrangements incorporate Bluetooth, Wireless M-Bus correspondence, worldwide framework for versatile interchanges/general bundle radio management (GSM/GPRS), and Ethernet, among others. These arrangements permit remote perusing of

sensors and meters by the immediate exchange of constant or time-stamped information to the focal management arrangement of the utility or water power. The information is then made accessible online for client data framework (CIS), geographic data frameworks (GIS), distributed computing or supervision and information management apparatuses, supporting enhanced choice making inside of the framework. Such specialized gadgets fused with smart meters/sensors can likewise give alarms to powers (e.g. reverse stream, release ready, misrepresentation caution, and battery levels, water quality alerts).

A majority of these sorts of correspondence arrangements guarantee spatial excess and empower an extensive variety of scope between inaccessible structures, lodging homes, and different locale. In the conventional accumulation frameworks, impressive measures of time would have been squandered finding and measuring focuses, particularly in remote areas.

c. Geographic information systems (GIS)

Geographic data frameworks (GISs) permit to catch, oversee, break down and show topographical data for underground resources depiction and choice making. GIS has an extensive variety of uses in different areas (e.g. regular assets, utilities, transportation, open security and guard). Their mix can enhance information management particularly of extensive volume ventures, since they give superb results show (especially in pressure driven recreation demonstrating), along these lines empowering extra examination to educate choice making.

GIS permits perception and examination of water assets and human movement information by connecting geographic data with clear data. This is very significant to urban water management in evaluating water quality and everyday operations on a local and regional scale. Different issues, for example, flooding can likewise be relieved by the utilization of topographical data, by recognizing basic territories that are at danger. This is fundamental in the improvement of peril maps, and in the arranging of crisis reactions. GIS use offers more hearty investigation, expanded effectiveness and lessened expenses.

By integrating information from resource satellites, GIS can cover large river basins which are occupied by some cities. Combined with local rainfall patterns, meteorological and hydrological data, as well as drainage systems, geographical information and interfaces improves urban storm water management by strengthening drainage management and enhancing rainwater reuse, thus helping to reduce the prevalence of urban flooding.

d. Cloud computing

Distributed computing utilizes an outer registering power capacity which is outside the limit of a client's own particular foundation, to run projects or applications. Cloud situations commonly empower the accompanying functionalities: screen and oversee figuring without human association, wide system access to permit registering managements to be conveyed,

access more than a few systems and heterogeneous gadgets, technologic capacity to scale up or down computational assets quickly and as required, capacity to share over numerous applications, and also to track applications/inhabitants for charging purposes.

Cloud frameworks in urban settings likewise permit high effectiveness and high usage of pooled assets for a superior equalization of workload and calculation through numerous applications, furnishing urban water supervisors with an extensive variety of conceivable outcomes in PC displaying and information stockpiling. Urban surge management is another region where distributed computing is progressively utilize. Past their innovative hobby, different issues like information protection, security and proprietorship must be plainly approved by the Cities preceding any huge sending of Cloud registering arrangements.

e. Supervisory control and data acquisition (SCADA)

At the point when consolidated into water management frameworks, supervisory control and information securing (SCADA) are PC controlled frameworks that contain an expansive assortment of correspondence frameworks, permitting to screen and control water treatment and appropriation, and in addition wastewater accumulation and treatment. The framework takes into consideration supervision through information procurement and management, and can prepare and send orders inside of the framework. The correspondence framework might include radio, direct wired associations or telemetry. Utilities have been utilizing SCADA frameworks overseeing continuous alerts and productively work plants and systems.

For some situation, SCADA frameworks are going past their local functionalities by suggestion discretionary modules on displaying or streamlining. a couple of cases of larger amount applications can be recorded, for example, deciding times of top water use, distinguishing potential framework holes, and setting charging rates, among others.

All around speaking SCADA frameworks have added to lessen the working expenses of utilities, and have enhanced water conveyance to family units, organizations and industry. The checking and control functionalities of SCADA frameworks can help utilities to ensure their foundation and avoid extreme debasement. The usage of SCADA has been related to 30% reserve funds on vitality used to oversee water frameworks, 20% decrease on water misfortune and 20% lessening in disturbance. Utilization of SCADA as a feature of urban frameworks can likewise upgrade fiasco readiness through tempest water management, and backing the remote operation and observing of real dams and weirs.

f. Models, optimization tools and decision support

Model-based water management has developed throughout the years to enhance the quality, amount and operations expenses of the worldwide water supply through far reaching

demonstrating applications. These demonstrating programming consolidate, to some degree, forms saw in this present reality (e.g. through comparisons, calculations and situations) and contain different information reporting and representation devices for deciphering results from water dispersion channeling frameworks, water quality observing information, and wastewater management frameworks, among other applicable data for choice backing.

Various models have been utilized by urban water administrators, for example, Mike Urban, Aquacycle, AISUWRS and UGROW, among others. Models, streamlining devices and choice bolster devices for system management of urban water assets add to ascertain and figure utilization, diminish costs through the improvement of operations, plan and assess techniques, furthermore to direct helplessness studies to advise procedure outline.

SMW Recommendations

The integration of smart water management technologies through realistic, measureable timelines and adequate implementation processes can deliver immediate visible and measureable results in urban water distribution and wastewater management. Through co-ordinate actions, holistic management, stakeholder involvement, adequate investment, and appropriate technology, SWM can improve both the reliance and sustainability of the water systems and networks.

By protecting the safety and reliability of water supplies, increasing the resilience of water infrastructure, reducing flooding and overloads of wastewater systems, decreasing energy consumption, lowering operational costs while increasing customer choice and control, these systems can enable a sustainable water environment for cities to grow and thrive in.

Recent advances in technology and interconnectedness, once appropriately harnessed, can foster the conditions needed to promote sustainable water resource management in the face of rapid urbanization, water scarcity and climate change.

This will enable cities to conduct the following tasks:

- Collect easily real-time data and measurements through sensor networks and low-cost innovative communications and protocols.
- Make better informed decisions through the use of advanced analytics which translate the raw data into actionable intelligence.
- Improve the efficiency, performance and optimization of infrastructure through real-time management systems.

The traditional independent system approach to urban water supply, wastewater disposal and storm water management will no longer be able to endure the increasing

pressures faced by the water sector. However, the co-ordination of multiple sectors through SWM networks can contribute to ensure the sustainability of urban water management system. Figure 04 illustrates some of the SWM tools that play a role in water distribution control systems.

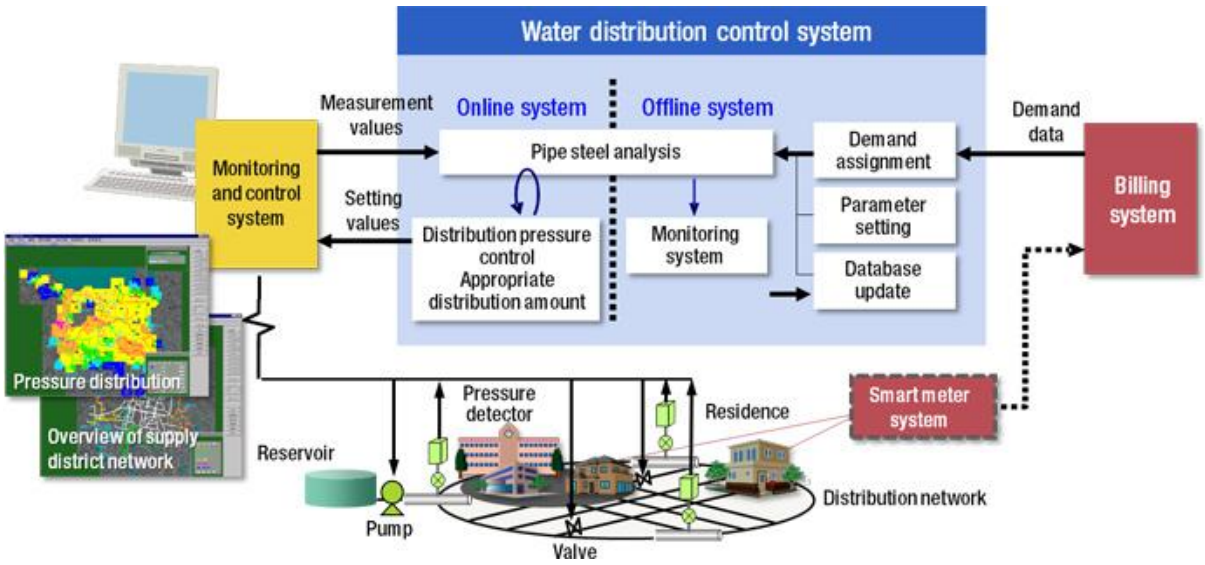


Fig8: Smart water management tools

SWM also generates economic, social, and environmental benefits through water resource sustainability, which, in turn, contributes to the comfort, security and well-being of urban residents.

Some of the benefits associated to water and wastewater management include:

- **Economic savings**: SWM tools can greatly reduce non-revenue water by identifying leaks and illegal connection, regaining revenue necessary to maintain the infrastructure. SWM enables sustainable water use, thereby reducing the amount of water abstracted, treated and distributed which reduces operational costs.
- **Improved services**: Smart metering can improve the relationship between the water utilities and the customers by providing more transparent water consumption information. Improved monitoring and operations prevents supply interruptions and disruptions within the water distribution network, for example, in the event of sewerage and storm water overflows. Better management relieves pressure on water resources that may be scarce during periods of drought.
- **Improved wastewater management**: These benefits are associated to improvements in the performance and economic efficiency of the wastewater treatment, as well as enhanced monitoring that helps prevent infrastructure overload.
- **More efficient treatment**: Improved water quality monitoring throughout the systems utilizing sensors creates the possibility of source control of resource pollutants and the use

of natural systems, thus reducing the potential treatment required for water supply systems, or the separation of specific pollutants in wastewater.

- **Environmental protection and enhancement**: Reduced demand and improved environmental monitoring helps to maintain and restore ecosystems that rely on a healthy aquatic environment.
- **Reduced carbon emissions**: Improved management results in less energy consumed for the abstraction, treatment and distribution process of water resources, thus helping to reduce a city's carbon footprint.
- **Flood control and storm water management**: Improved weather awareness and prediction through weather intelligence allows cities to plan more effectively their flood prevention strategies, as well as to manage urban drainage systems and storm waters accordingly.
- **Greater resilience**: Reliable data reduces inaccurate forecasts and predictions, as well as the uncertainty surrounding future demand and supply availability, thus improving decision-making for water investments and strategies. Improved operational control and monitoring can also help to prioritize infrastructure maintenance. At the same time, improved decision-making strengthens the capacity of centralized sewers and treatment facilities to cope with the pressures of urbanization.

Smart Buildings - Parking

According a data available with MAP OF INDIA, car density in India is increasing more than China. Increasing number of vehicles is introducing very well-known problem of parking in all segments. Parking space has become an acute problem in India, as with every passing day number of cars is increasing and the parking space is limited. Whatever little spaces have been left are clearly not enough for increasing number of vehicles. Condition in Metro cities like Delhi, Mumbai is even worse.

Searching for a parking space is a routine (and often frustrating) activity for many people in cities around the world. This search burns about one million barrels of the world's oil every day. As the global population continues to urbanize, without a well-planned, convenience-driven retreat from the car, these problems will worsen.

What should we do?

Smart parking is the first step in the right direction. It involves using low-cost sensors, real-time data collection, and mobile-phone-enabled automated payment systems that allow

people to reserve parking in advance or very accurately predict where they will likely find a spot. When deployed as a system, smart parking thus reduces car emissions in urban centers by reducing the need for people to needlessly circle city blocks searching for parking. It also permits cities to carefully manage their parking supply. According to a report, Smart Parking could result in 2, 20,000 gallons of fuels saving till 2030 and approx. 3, 00,000 gallons of fuels saved by 2050, if implemented successfully.

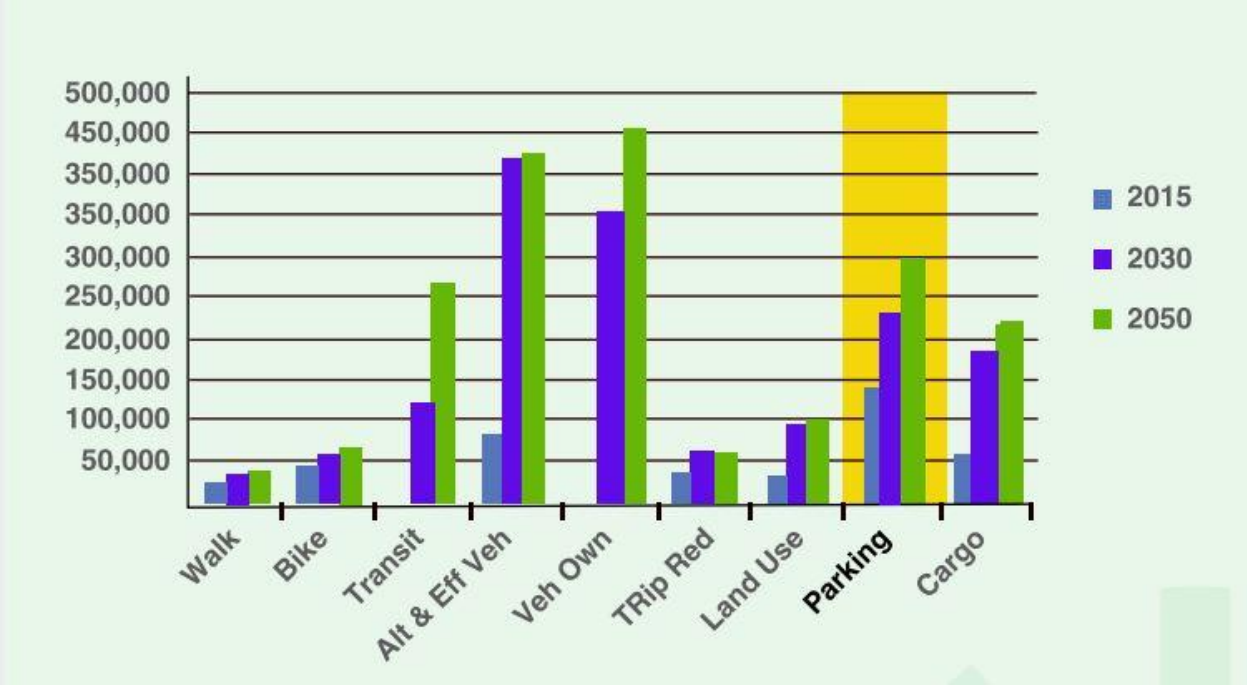


Fig 9: Graph showing potential saving of fuel

Smart Parking would enable the following:

• Accurately predict and sense spot/vehicle occupancy in real-time.

• Guides residents and visitors to available parking.

• Optimize Parking Space Usage

• Simplifies the parking experience and adds value for parking stakeholders, such as drivers and merchants

• Help traffic in the city flow more freely leveraging IoT technology.

• Enables intelligent decisions using data, including real–time status applications and historical analytics reports

• Smart Parking plays a major role in creating better urban environment by reducing the emission of CO2 and other pollutants

• Smart Parking enables better and real time monitoring and managing of available parking space, resulting in significant revenue generation

Smart parking work flow analysis

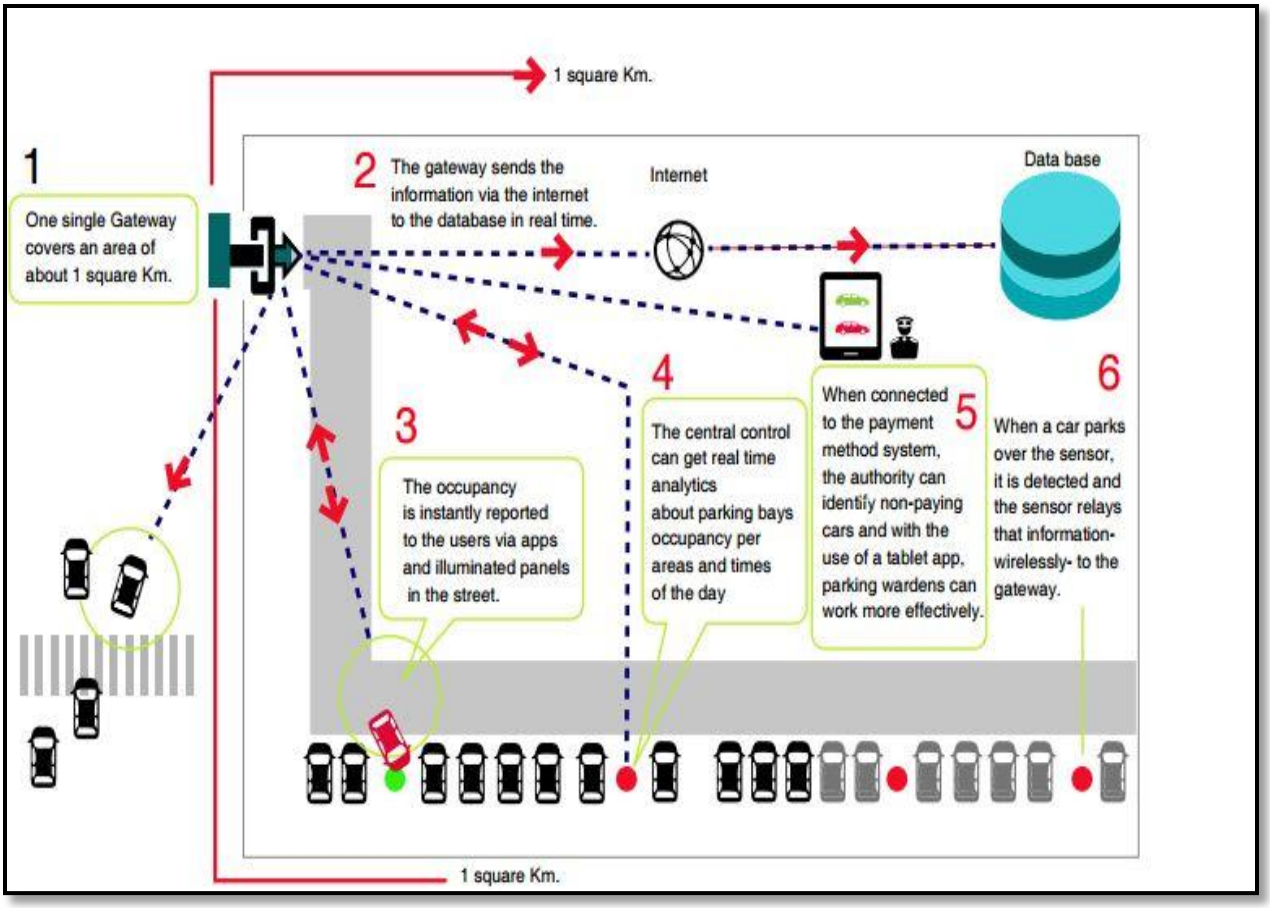
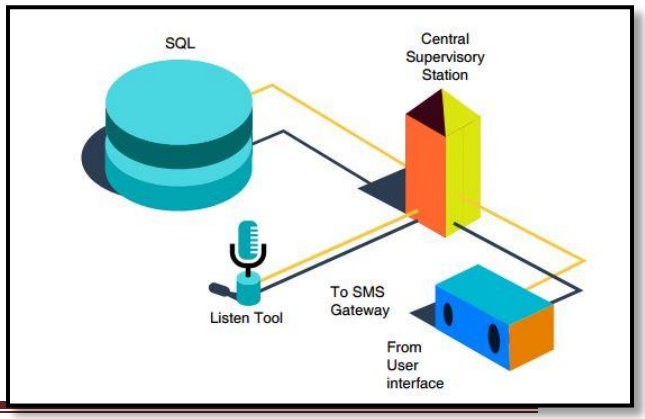


Fig 10: Smart Parking – Workflow

Parking assistance system description

• The Parking Assistance System includes three modules-Monitoring modules, Control module and a displaying unit. Along with above three modules it will also have centralized supervisory system to maintain a data base of parking space and will have a SMS gateway



• The monitoring module includes ultrasonic sensors/ ambient light sensor which identifies the

free parking spaces and transmits the Information to control unit through Zigbee

• Apart from detecting the car the sensor also provides additional information like the stretch of time the car has been parked and also its health status.

• The control units process the information and send the information to Centralized supervisory system.

• Centralized supervisory system receives information of parking space from the controller through UDP. It then sends the information such as slot allotted, time parked, billing information to the user's mobile phone

Typical scenario for Smart Parking

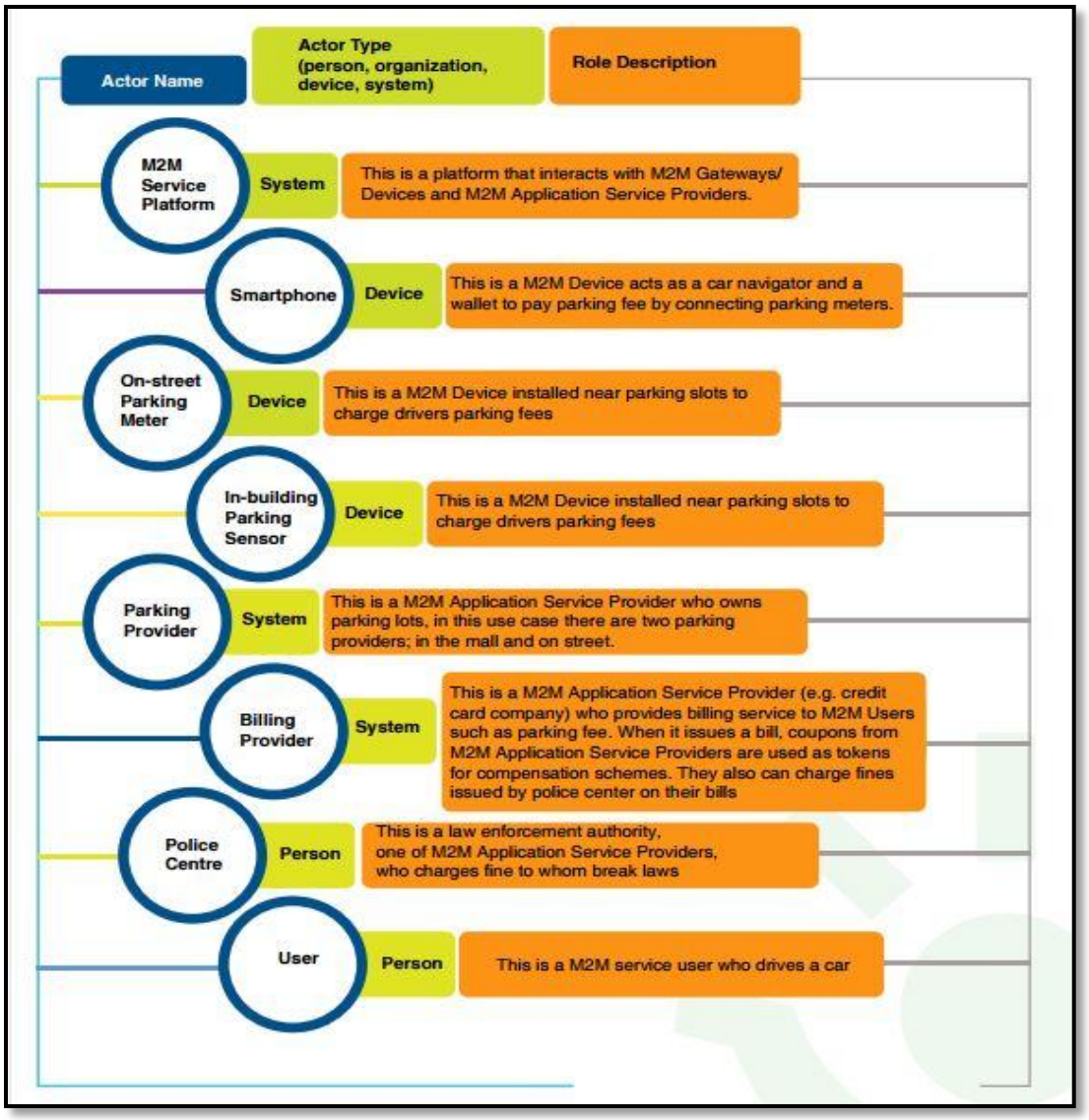


Fig 11: Smart Parking Scenario

Types of Smart Parking Systems

Today we can find several smart parking facilities in most of the major cities. Customer and the parking operator are benefited by the smart parking service in different ways:

1. Space availability can be determined before entering the garage and/or parking level

2. This type of system significantly reduces traffic and air pollution – by minimizing the time required to locate open spaces.

3. Future parking patterns and trends can be predicted from the system data and this data can be used to minimize the vehicle thefts.

4. Staff requirements are also reduced to control the traffic.

5. The parking operator can use the system data to develop or improve pricing strategies.

Recommended Architecture

Hardware Architecture

Each vehicle is deployed with a short range wireless transceiver and a simple processor. The transmission range is 1m. It can be one of the current short range devices, such as Zigbee devices, Bluetooth devices and infrared devices. Both wireless transceiver and processor are fitted into the TRD.

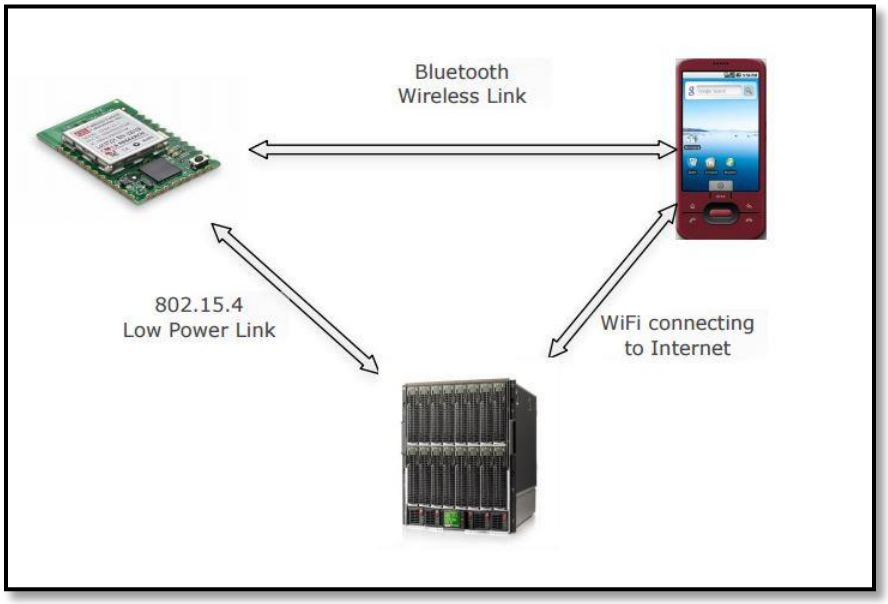


Fig 12: Hardware Architecture

The infrastructure for a parking provider consists of a wireless transceiver, parking belts, InFrared Devices (IFD) and a control computer. The wireless transceiver can be part of a

Wireless LAN (WLan) network. It is used to transmit the parking information (for example, the capacity of empty parking spots, and the position list of empty parking spots) and reservation information. The parking belts and IFD, as shown in Figure 5, will work together to check-in a vehicle. The IFD at the parking spot connects to a signal light. A yellow light means empty spot. A blue light means filled spot. A red light means misfiled vehicles which will be charged a fine. In some scenarios, vehicles may use a spot to back up or pass through. To prevent misdetection of vehicles, we use both IFD and belts to double check if the vehicles are behaving correctly.

Software Architecture

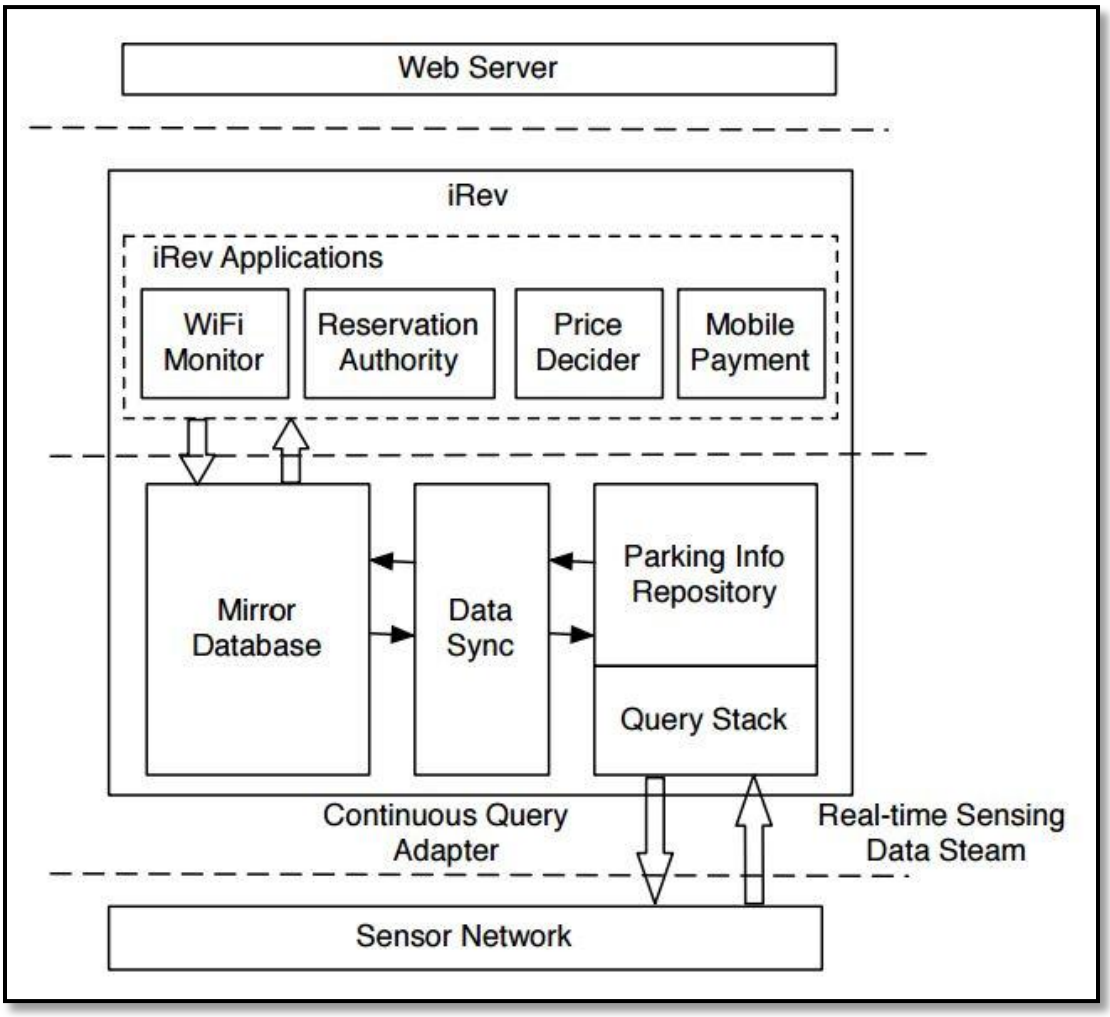


Fig 13: Software Architecture

In the software architecture, we propose several modules shown in Figure. The architecture consists of four modules:

• Driver Module is responsible for the communication with hardware devices. The driver module consists of the sensor driver for belts, communication driver for the vehicle's short range transceiver, and IFD driver for vehicle detection.

• Communication Module receives and transmits messages between a sender and a receiver. For Vehicle-to Infrastructure (V2I) communication, this module simplifies the communication process and performs error control, for example verifying the checksum and correcting errors. In general, the purpose is to improve communication speed and enhance message correctness because the communication response time is strict.

• Function Module is the core function of the parking system, including monitor, check-in, reservation, advertisement management. Thanks to the subscription to the driver module and the communication module, the function module can talk to hardware devices and transmit/receive data without having to know the details of the lower levels.

Control section

The control section is at the entrance of the parking area, for checking in and checking out process of the vehicles, to maintain the database we need. The personal computer, for communication with monitoring area Zigbee is required, for displaying information LCD panels are used. The RFID reader is used to read the RFID tags and will only allow the authorized vehicles to avoid the possibilities of car theft.

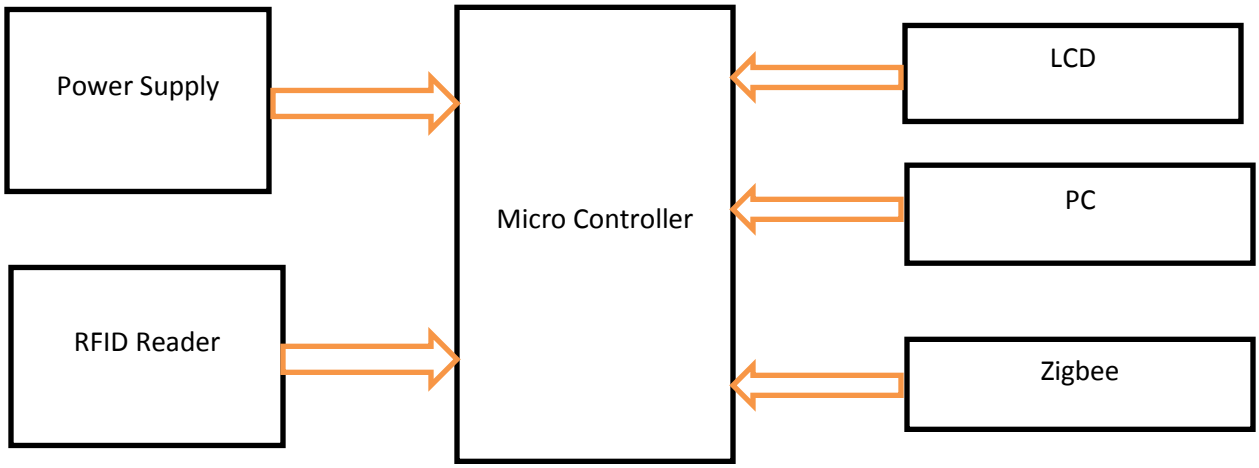


Fig 14: Control Section

• Application Module manages the whole parking system. The main function of the application includes account management (cash, credit/debit management), operation management, fault tolerance and maintenance management.

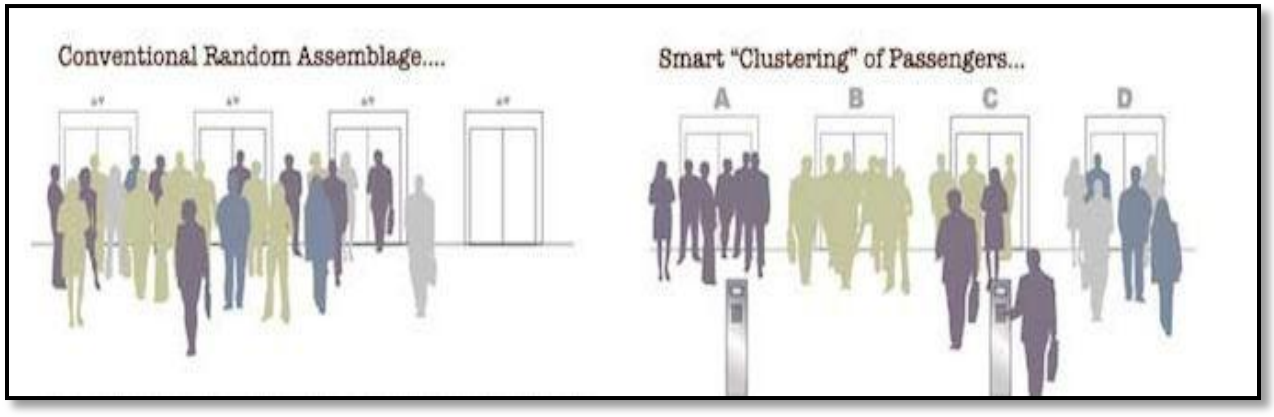
Smart Elevator System

Smart elevators are designed to transform the simple act of traveling between floors. Instead of pushing a button to go up or down, passengers first select the floor they want. Then they are directed to the elevator that will take them to their destination with the fewest number of stops. And because smart elevators make fewer stops, they use less energy. Building owners like them because they mean fewer large crowds forming in lobbies waiting for the next car.

Smart elevators can also calculate the weight of their passengers to prevent too many people from getting on. It can also slow down if a disabled person is boarding.

How it works?

The passengers first enter in their desired floor as they approach the elevators. The keypad sorts them into groups of similar destinations and assigns specific elevators to each passenger. So passengers going to floors 26, 28 and 32 would be assigned one elevator, while passengers who keyed in floors 50, 54 and 55 would take another. In cases when every second is necessary, the Smart elevators can also detect employees via their ID badges.



On the way down, full elevators skip floors to minimize wasted stops. The Smart Elevator monitors each car's current weight, and ceases to make stops once the weight passes a certain limit. The system also tracks traffic patterns and remembers the most frequently called floors. The decrease in trips preserves equipment longer as well.

Instead of responding to problems, service engineers will have access to real-time data and take measures to prevent elevator breakdowns before they occur. In addition, because of the two-way flow of data, technicians can remotely put an elevator into diagnostics mode, or send it to another floor. It all adds up to less travel time, better efficiency, and reduced costs. The solution also seeks to take much of the guesswork out of repairs. The system contains an intelligent information loop: data from elevators is fed into dynamic predictive models, which continually updates datasets via seamless integration with the Intelligent Systems Service.

When the elevator reports that it has a problem, it sends out an error code and the three or four most probable causes of that error code. In effect, the field technician is being coached by this expert citizen. With up to 400 error codes possible on any given elevator, "coaching" can significantly sharpen efficiency in the field.

The System Architecture of the Integrated Model of the Elevator Control System for an Elevator

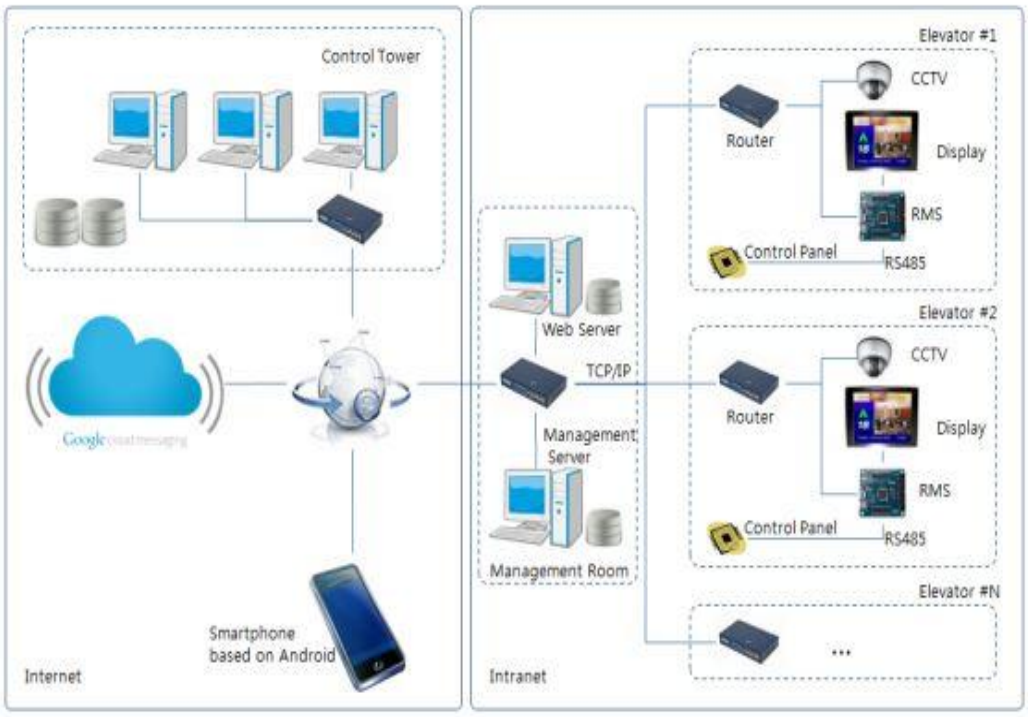


Fig 15: System Architecture – Smart Elevators

Integrated Control Services of an Elevator System based on IT

In the operation of the elevator, the devices of the emergency control service such as CCTV, emergency bell and monitoring system are utilized in the elevator system mainly. The emergency bell is connected to a management office and a guardhouse directly. It can contact the manager when occurring emergency situation by calling. This situation has disadvantage that it takes a lot of time to solve the emergency situation when the manager is not exist. In addition, it is difficult accurate assessment and recognition about the situation of the problem because the caller delivers their situation and location orally. For solving of these problems, a different approach that the caller can connect other manager around any time is required when the manager absence.

In addition, the monitoring system has lack of aggressive problem-solving skills because the managers identify the elevator situation manually. An important element of elevator accidents handling is securing safety and faster processing. For this purpose, the emergency control system needs approaches to be diagnosed by the elevator specialists and to solve the problem

in the fastest way. Recently, with expansion of IT convergence technologies, the elevator service environment is rapidly changing. Mainly, the services have evolved to improvement of the user convenience and advancement services. And also there are various services such as notice and information service, elevator call and boarding service, elevator diagnostic and checking service so on

Recommendations

Government and Policy makers:

- Widen the focus of incentives and guidelines for green buildings to include safe and productive buildings
- Drive a smart city experience for the public by focusing on making public buildings smarter
- Create guidelines and stronger policies for driving private sector participation in the 100 Smart Cities initiative by focusing on key private sector buildings

Users, Owners and Developers:

- Enhance building smartness by focusing on all three aspects: asset capability, asset coverage, and asset uptime
- Use vertical-specific strategies to drive building smartness effectively and efficiently

Industry Associations, Consultants, Architects, and Service Providers:

- Building on increased awareness and impact of the green building movement, push similar research on benefits of safe and productive buildings as well
- Deploy best practices and benchmarks identified in this white paper
- Educate users and owners, and advocate smart building benefits to policymakers
- Demonstrate the economic argument for smart buildings to make smarter cities

Other areas of making smart buildings productive are

- Focus on indoor environment comfort, quality and control systems. Improve productivity and user experience by making wireless communication and data infrastructure seamless and available across the building. Also improve systems for people, vehicle and cargo movement management

- Focus on fire detection and notification. Given the need to manage access and information security in these offices, need to improve surveillance and intrusion monitoring. Improve access control and screening systems for people and vehicles. Improve disaster response, worker safety and personal protection, and gas and water leakage detection and notification systems

Future Smart building Opportunities

Cloud-based approach

Cloud computing is set to transform information technology, by making third party applications readily available as a service over the internet. For smart building solutions, this will deliver several benefits:

• Accessibility: Aggregating and analyzing data from disparate sources is at the core of any smart building solution. The cloud is ideally suited to providing a universally available platform for managing building data mashed up with contextual information and made accessible for a variety of users and devices.

• Scalability: With thousands of sensors and controls, modern buildings generate large volumes of data. As the data volume and diversity of sources increases, a cloud-based architecture provides the scalability required to process massive volumes of data at an affordable cost. Abundant computing power allows complex modeling, such as correlating external temperature, cloud cover, and wind conditions with building access activity to refine heating, air conditioning and lighting patterns.

• Ease of deployment: Cloud technology can provide a secure and uncomplicated connection between off-site servers and on-site equipment.

Automation and real-time analytics

The next generation of smart building solutions will allow organizations to automatically adjust building controls based on real-time data. For example, by monitoring the security badge access information for a building (as a proxy for the number of employees present), HVAC systems could be automatically adjusted to account for increased or decreased conditioning requirements. As an alternative, location and presence data from laptops or mobile phones could be used. Such solutions will rely on real-time analytics applied to incoming data streams, along with complex event processing, to execute automated adjustments to building controls.

For example, statistical analysis, simulation and predictive modeling can be applied to determine how many AC's need to be turned on, based on forecast occupancy levels and outside weather conditions.

Integration with utilities and city infrastructure

With increasing adoption of smart building solutions, the built environment will achieve new efficiencies in energy use and improvements in occupant comfort. But this is only part of the story. Electricity grids are being upgraded with intelligent controls and two-way communication. As individual nodes of the smart grid, buildings will become active participants in managing energy demand and supply in a connected environment that includes power plants, transmission infrastructure and even electric vehicles.

For example, if a substantial share of employees in an organization were to use electric cars that are plugged in during the day, the campus could use the combined battery capacity to lower peak demand drawn from the utility at certain times during the day. Likewise, demand response technology can be used to shed loads in buildings when electricity consumption peaks, saving cost for utilities and building managers.

As buildings become increasingly networked, they play a crucial role in the development of energy-smart cities that unify the concepts of resource management and information technology on a municipal level.

Conclusion

The new intelligent building technologies incorporating multi-function sensors and wireless sensors will reduce false alarms, speed response times, reduce expenditure on sensors as well as reduce fire-related losses. Real-time control system will enable the monitoring and control of service systems and fire safety systems with increased efficiency and reduced costs for building management operations, more efficiently distinguish between the fire and non-fire threats, and quick retrieval of property and life from these situations

However, there is a possibility of new types of risks emerging from application of intelligent building technology. Robust Sensor technologies will be needed to prevent false alarms, accurately distinguish between fire and non-fire threats, and ensure safety of vital information such as the location of occupants in case of data overload. Internet based monitoring and control of building service systems need to be secure and reliable to prevent occurrences of false alarms to the building occupants and fire brigades.

Integrated building systems will need to ensure that fire emergencies do not crash the building service systems while giving priority to fire safety over other building activities. Close examination building system integration need to be conducted in order to determine whether sufficient redundancy is provided by a fully integrated building system to provide adequate fire safety.

Additional work is needed to overcome the problems like fragmentation of the building and among the communication industries reluctance to change established practices, lack of universal communication standards and the complexity of intelligent building systems all have slowed intelligent building progress.

References

- IEEE Paper 'A Reservation-based Smart Parking System' by Hongwei Wang and Wenbo Hey Published in: Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on 10-15 April 2011
- 'Smart Parking System (SPS) Architecture Using Ultrasonic Detector' by Amin Kianpisheh, Norlia Mustaffa, Pakapan Limtrairut and Pantea Keikhosrokiani in International Journal of Software Engineering and Its Applications Vol. 6, No. 3, July, 2012
- 'The Design and Implementation of the Integrated Model of the Advertisement and Remote Control System for an Elevator' by Woon-Yong Kim and SoonGohn Kim in International Journal of Smart Home Vol.8, No.3 (2014)
- 'From Buildings to Smart Buildings – Sensing and Actuation to Improve Energy Efficiency' by Thomas Weng and Yuvraj Agarwal in IEEE Design and Test, Special Issue On Green Buildings
- 'Smart Buildings Make Smart Cities' A white paper authored by Honeywell and Ernst & Young LLP
- http://www.prnewswire.com/news-releases/advanced-sensors-for-smart-buildings-237011401.html
- https://sftool.gov/learn/about/426/plug-loads
- http://www.doi.gov/archive/greening/energy/occupy.html
- http://www.sciencedirect.com/science/article/pii/S0360132311001739
- http://doi.ieeecomputersociety.org/10.1109/MDT.2012.2211855
- http://www.researchgate.net/publication/264582853_From_Buildings_to_Smart_BuildingsSensing_and_Actuation_to_Improve_Energy_Efficiency
- http://www.smartcitieschallenge.in/
- https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=A6V10434248
- http://info.senseware.co/blog/smart-building-water-management-good-for-your-business-and-the-planet
- http://www.marketsandmarkets.com/Market-Reports/smart-building-market-1169.html
- http://www.noveda.com/smart-buildings
- http://www.automatedbuildings.com/news/apr09/articles/sinopoli/090330013642sinopoli.htm
- http://www.libelium.com/smart_parking/
- http://dx.doi.org/10.1155/2013/107975
- http://forbesindia.com/blog/businessstrategy/buildingasmartcitylandscapeinindia/