CHAPTER 3

INTERNET OF THINGS APPLICATION EXAMPLES

This chapter provides a sample of applications than can be provided with/by the Internet of Things (IoT), although any such survey is invariably incomplete and is limited in the temporal domain (with new applications being added on an ongoing basis). We look at applications that are already emerging and/or have a lot of current industry interest. Related to IoT applications, proponents make the observation that (1)

> "... there are so many applications that are possible because of IoT. For individual users, IoT brings useful applications like home automation, security, automated devices monitoring, and management of daily tasks. For professionals, automated applications provide useful contextual information all the time to help on their works and decision making. Industries, with sensors and actuators operations can be rapid, efficient and more economic. Managers who need to keep eye on many things can automate tasks connection digital and physical objects together. Every sectors energy, computing, management, security, transportation are going to be benefitted with this new paradigm. Development of several technologies made it possible to achieve the vision of Internet of things. Identification technology such as RFID allows each object to represent uniquely by having unique identifier. Identity reader can read any time the object allows real time identification and tracking. Wireless sensor technology allows objects to provide real time environmental condition and context. Smart technologies allow objects to become more intelligent which can think and communicate. Nanotechnologies are helping to reduce the size of the chip incorporating more processing power and communication capabilities in a very small chip.

Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications,
First Edition. Daniel Minoli.

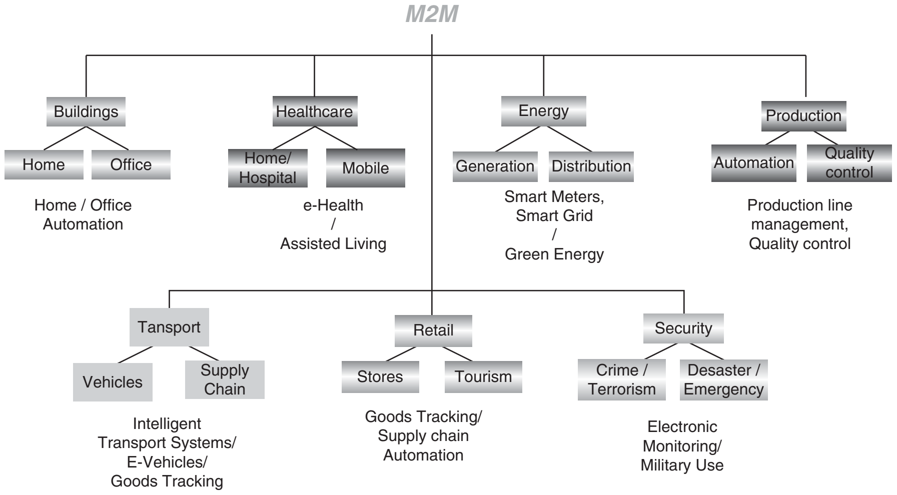
M2M
Buildings
Home
Office
Home / Office Automation
Healthcare
Home/ Hospital
Mobile
e-Health / Assisted Living
Energy
Generation
Distribution
Smart Meters, Smart Grid / Green Energy
Production
Automation
Quality control
Production line management, Quality control
Tansport
Vehicles
Supply Chain
Intelligent Transport Systems/ E-Vehicles/ Goods Tracking
Retail
Stores
Tourism
Goods Tracking/ Supply chain Automation
Security
Crime / Terrorism
Desaster / Emergency
Electronic Monitoring/ Military Use

FIGURE 3.1 Grouping of applications in the M2M context.

3.1 OVERVIEW

Table 1.2 offered a taxonomy of applications, although no claim is made here that this taxonomy is complete or fully normative; in the same vein, Figure 3.1, partially inspired by Reference 2, depicts a grouping of applications, particularly in the machine-to-machine (M2M) context. As should be clear by now, some of the possible short-term applications include the following: building automation and remote control (facilitating efficient commercial spaces); smart energy (supporting office building/home energy management); healthcare (providing health and fitness monitoring); home automation (giving rise to smart homes); and retail services (enabling smart shopping). A longer list of applications includes, but is not limited to, the following:

- Public services and smart cities:
  - Telemetry: for example, smart metering, parking metering, and vending machines
  - Intelligent transportation systems (ITSs) and traffic management
  - Connecting consumer and citizens to public infrastructure (such as public transportation)
  - In-building automation, municipal, and regional infrastructure
  - Metropolitan operations (traffic, automatic tolls, fire, and so on)
  - Electrical grid management at a global level; smart grids (SGs)
  - Electrical demand response (DR) at a global level
- Automotive, fleet management, asset tracking:
  - e-Vehicle: for example, navigation, road safety, and traffic control

  - Driver safety and emergency services
  - Fleet management systems: hired-car monitoring, goods vehicle management
  - Back-seat infotainment device integration
  - Next-generation global positioning system (GPS) services
  - Tracking: asset tracking, cargo tracking, and order tracking
- Commercial markets:
  - Industrial monitoring and control, for example, industrial machines, and elevator monitoring
  - Commercial building and control
  - Process control
  - Maintenance automation
  - Home automation
  - Wireless automated meter reading (AMR)/load management (LM)
  - Homeland security applications: chemical, biological, radiological, and nuclear wireless sensors
  - Military sensors
  - Environmental (land, air, sea) and agricultural wireless sensors
  - Finance: Point-of-sale (POS) terminals, ticketing
  - Security: Public surveillance, personal security
- Embedded networking systems in the smart home and smart office:
  - Smart appliances: for example, AC-power control, lighting control, heating control, and low power management
  - Automated home: remote media control
  - Smart meters and energy efficiency: efficiencies obtained by exploiting the potential of the SG
  - Telehealth (e-health): Assisted Living and in-home m-health services (including remote monitoring, remote diagnostic)
  - Security and emergency services: integrated remote services

Table 3.1 provides some examples by category as defined in 3GPP machine-type communication (MTC) documentation (3). MTC is the term used in 3GPP to describe M2M systems.

In recent years, ETSI has published a number of use cases for IoT (specifically for M2M) applications in the following documents:

- ETSI TR 102 691: "*Machine-to-Machine Communications (M2M); Smart Metering Use Cases.*"
- ETSI TR 102 732: "*Machine-to-Machine Communications (M2M); Use Cases of M2M Applications for eHealth.*"

TABLE 3.1 Examples of MTC Applications as Defined in 3GPP TS 22.368 Release 10

Category	Specific Example
Consumer devices	Digital camera Digital photo frame eBook
Health monitoring vital signs	Remote diagnostics Supporting the aged or handicapped Web access telemedicine points
Metering	Gas Grid control Heating Industrial metering Power Water
Payment	Gaming machines POS Vending machines
Remote maintenance/control sensors	Elevator control Lighting Pumps Valves Vehicle diagnostics Vending machine control
Service area MTC applications	Backup for landline Car/driver security Control of physical access (e.g., to buildings) Security surveillance systems
Tracking and tracing fleet management	Asset tracking Navigation Order management Pay as you drive Road tolling Road traffic optimization/steering Traffic information

- ETSI TR 102 897: "*Machine-to-Machine Communications (M2M); Use Cases of M2M Applications for City Automation.*"
- ETSI TR 102 875: "*Access, Terminals, Transmission, and Multiplexing (ATTM); Study of European Requirements for Virtual Noise for ADSL2, ADSL2plus, and VDSL2.*"
- ETSI TR 102 898: "*Machine-to-Machine Communications (M2M); Use Cases of Automotive Applications in M2M Capable Networks.*"
- ETSI TS 102 412: "*Smart Cards; Smart Card Platform Requirements Stage 1 (Release 8).*"

The International Organization for Standardization (ISO) has published the following relevant document, among others:

- ISO 16750: "*Road Vehicles—Environmental Conditions and Testing for Electrical and Electronic Equipment.*"

Some of these (ETSI-covered) applications are discussed in the sections that follow.

3.2 SMART METERING/ADVANCED METERING INFRASTRUCTURE

The European Technology Platform for Electricity Networks for the Future defines an SG as: "an electricity network that can intelligently integrate the actions of all users connected to it—the consumers, the power generators, and those that do both—in order to efficiently deliver sustainable, economic, and secure electricity supplies." A key element of an SG is a smart metering network that enables automated metering capabilities on the customer side (downstream). On the upstream, the utility acquires the capability for real-time grid monitoring and for information processing of significant network events; this includes fault detection, isolation, and resolution. Specifically, a smart metering network enables a utility company to (i) remotely connect or disconnect power to individual customers, (ii) remotely or automatically update the grid configuration, (iii) collect power consumption data in variable time intervals, and (iv) modulate customer loads automatically during critical demand periods. The SG is also able to automatically detect theft and is able to notify the utility if a meter is tampered with. Smart appliances and SG devices are often referred to being as "DR-enabled." Some of the consumer benefits of smart metering include the elimination of domicile/site access issues, improved billing accuracy, and cost savings derived from DR/demand management in conjunction with incentivized tariffs (4).

The general goal is to monitor and control the consumption of utilities-supplied consumable assets, such as electricity, gas, and water. Utility companies deploy intelligent metering services by incorporating M2M communication modules into metering devices ("the thing"); these intelligent meters are able to send information automatically (or on demand) to a server application that can directly bill or control the metered resource. The ultimate objective is to improve energy distribution performance and efficiency by utilizing accurate real-time information on endpoint consumption. A variation of this application for metering of gas, electricity, and water is a pre-payment arrangement: here a consumer can purchase a specific volume of gas, electricity, water, and so on by pre-payment; the information about the purchased volume is securely transmitted to the metering device and then securely stored on the M2M modules. During use, the actual information about the consumed volume is transmitted to the M2M module, and when the purchased volume has been consumed, the supply can be stopped (via a secure actuation capability) (5, 37). See Figure 3.2 for an example of a smart flowmeter for a water utility application; similar concepts apply to natural gas or electric power.

FIGURE 3.2 Example of an instrumented flowmeter.

The advanced metering infrastructure (AMI) is the electric information service infrastructure that is put in place between the end-user (or end device) and the power utility. AMI is a system for implementing the SG, and it is the principal means for realizing DR. According to press time market forecasts, shipments of smart meter units were expected to continue to grow at a 15% annual rate, with a total of about half-a-billion meters shipped by 2015.

Proponents expect that the use of smart appliances and energy management systems will allow consumers to manage and reduce their energy bills and overall consumption. The combination of the AMI meter and an appropriate home area network (HAN) enables consumers to become aware of electricity consumption costs on a near real-time basis; to be able to monitor their energy usage; and to manage their usage based on their financial metrics. To assist consumers in managing their energy use, manufacturers are designing products that contain built-in communication systems that communicate with the HAN (and the AMI meter). Having knowledge of the cost of electricity and of the consumer preferences, these smart devices are able to manage appliances to either defer operation or adjust the operating condition to reduce peak energy demand. Thus, this intelligent management has the potential to reduce the consumer's energy bills and also reduce the peak demand for the utility. Peak reduction can save utilities money by helping them avoid the construction of new peaking power plants[1] that exist only to handle peak loads; peak load may occur only a few hours per day, or, in some cases, for only a few hours per year. Utilities can

[1] Peaking power plants are power plants that operate only when there is a high peak demand for electric power.

also avoid (or defer) the cost of upgrading their infrastructure to meet these infrequent peak loads (6).

The AMI environment is fairly complex. The underlying technology that enables these benefits to the consumer and the utility company is the availability of an AMI and HAN communication system. To be effective and easily deployed, the HAN communication network should preferably be based on a network technology that (i) utilizes open standards, (ii) is low cost, (iii) consumes a minimum amount of energy, and (iv) does not require extensive new infrastructure. Metering devices are typically monitored and controlled by a centralized entity outside or inside the network operator system. Due to the need for centralized control, the centralized entity will inform or poll the metering device when it needs measurement information rather than the metering device autonomously sending measurements. Depending on the nature of the metering application, low latency responses are sometimes required (metering for high pressure pipelines, for example). To accomplish this, the centralized entity will need to inform the metering device when it needs a measurement. Typically, due to the limitation of IPv4 address space, the metering terminal is behind a network address translator (NAT) where it is not assigned a routable IPv4 address (3). This predicament is one of the reasons why it is desirable to utilize IPv6 for IoT devices/things.

AMI can utilize a number of methods and communication standards to connect the end device to the applications of the utility company. To communicate between physical service layers, some combinations and/or refinements of existing communication protocols are required. See Figure 3.3, loosely modeled after reference (37). While a number of power line carrier (PLC)-based communication approaches are technically feasible, at the current time none of these technologies and protocols have reached the level of technical maturity and cost competitiveness to enable one

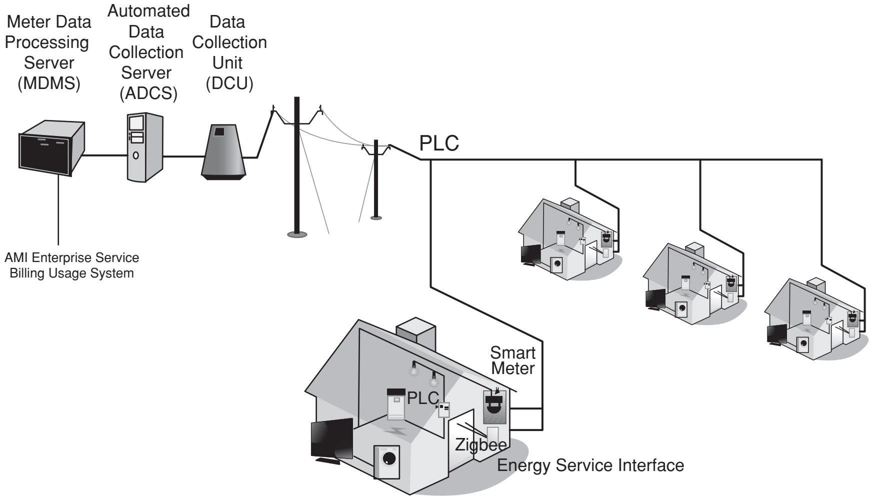
Meter Data Processing Server (MDMS)
Automated Data Collection Server (ADCS)
Data Collection Unit (DCU)
PLC
AMI Enterprise Service Billing Usage System
Smart Meter
PLC
Zigbee
Energy Service Interface

FIGURE 3.3 Advanced Metering Infrastructure.

to institutionalize a viable solution. However, there is work underway by several industry and/or standards organizations to develop standards for devices supporting these applications; for example, the European Commission (EC) has given support to the following initiatives:

- EC's M/411 Smart Metering Mandate: EC mandate issued in March 2009 by the Directorate-General for Transport and Energy (DG TREN) and sent to the three ESOs (European Standards Organizations)—CEN, CENELEC, and ETSI. The objective is to build standards for European smart meters, allowing interoperability and consumer actual consumption awareness.
- EC's M/490 SG Mandate: EC mandate issued in March 2011 by DG TREN and sent to the three ESOs—CEN, CENELEC, and ETSI. The objective is to build standards for European SGs.

3.3 e-HEALTH/BODY AREA NETWORKS

e-Health applications include health and fitness. Advocates envisage an environment where mobile health monitoring systems interoperate seamlessly and cohesively to reduce the lag time between the onset of medical symptoms in an individual and the diagnosis of the underlying condition. These applications make use of one or more biosensors placed on, or in, the human body, enabling the collection of a specified set of body's parameters to be transmitted and then monitored remotely. These sensors free patients from the set of wires that would otherwise tie the patients to a specific site at home or to a hospital bed; the on-body sensors are generally light and the links are wireless in nature, allowing the patient to enjoy a high degree of mobility (7). Sensors may consist of several wearable body sensor units, each containing a biosensor, a radio, an antenna, and some on-board control and computation. When multiple sensors are used by a patient, they are typically homed to a central unit also on the body. These on-body sensor systems—the sensors and the connectivity—are called wireless body area networks (WBANs), or alternatively, medical body area networks (MBANs), or alternatively medical body area network system (MBANS), although in the latter case the term does not necessarily mean a wireless system (8). Figure 3.4 provides a pictorial view of a WBAN.

MBAN technology consists of small, low powered sensors on the body that capture clinical information, such as temperature and respiratory function. Sensors are used for monitoring and trending for disease detection, progression, remission, and fitness. As patients recover, MBANs allow them to move about the healthcare facility, while still being monitored for any health issues that might develop. MBANs consist of two paired devices—one that is worn on the body (sensor) and another that is located either on the body or in close proximity to it (hub) (9). Some of these devices are disposable and are similar to a band-aid in size and shape; the disposable sensors include a low power radio transmitter. Sensors typically register patient's temperature, pulse, blood glucose level, blood pressure (BP), and respiratory health; the benefits

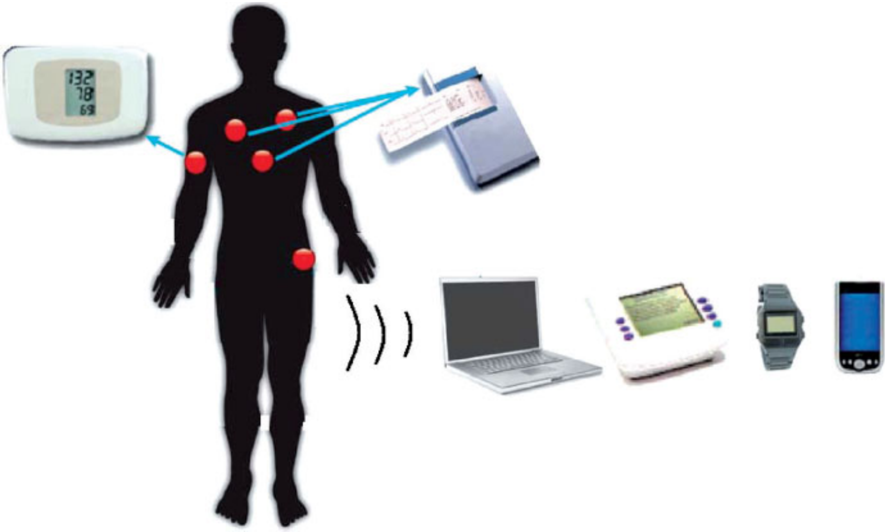

FIGURE 3.4 Wireless body area network/Medical body area network.

include increased mobility, better care, and lower costs. Examples of healthcare-related sensors include, but are not limited to:

- Glucose meter: A device that measures the approximate concentration of glucose in the blood; it is used by chronic disease (e.g., diabetes) management applications.
- Pulse oximeter: A device that indirectly measures the amount of oxygen in a patient's blood (oxygen saturation (SpO_2)).
- Electrocardiograph (ECG): A device that records and measures the electrical activity of the heart over time.
- Social alarm devices: Devices that allow individuals to raise an alarm and communicate with a caretaker when an emergency situation occurs; the caretaker may be a monitoring center, a medical care team, or a family member; these include devices fall detector and panic pendant/wrist transmitters.

The development activities related to WBANs/MBANs/MBANSs pertain to the formalization and standardization of wireless on-body monitoring technology entailing low power radio system used for the transmission of non-voice data to and from medical devices, especially in terms of frequency bands and communications at the higher layers (PHY, MAC, IP). A WBANs/MBANs consists of one or more on-body wireless sensors to simultaneously collect multiple vital sign parameters and/or medical actuator devices that can communicate with a monitoring device placed on/around (up to 10 m from) the human body. Today, existing technologies allow for *wired* solutions for monitoring patient vital signs as well as controlling actuators such as ventilators and infusion pumps. On-body sensors—measuring vital signs of a patient—and actuators are typically wired up to a bedside patient monitor. This bundle-of-wires situation limits the mobility of patients and reduces their comfort, adversely affecting their recovery times. Workflow delays are also introduced due to caregivers moving tethered patients. In Europe, the first wireless patient monitoring solutions operating in the generic short-range device (SRD) band from 2400 MHz to 2483.5 MHz have recently been introduced by vendors to overcome the disadvantages of wired solutions. However, the increasingly intensive use of this band by other applications (such as WiFi®, Bluetooth®, and ISM equipment) will tend to prevent such systems from offering the required reliability as their use increases within healthcare facilities (8). Hence the need for a standardized dedicated approach for MBANs, preferably with a worldwide and/or multiregion standard. There is movement to that effect in the United States (see below) and in Europe (with ETSI TR 101 557 as discussed in Chapter 6).

WBANs/MBANs are considered to be an assistive technology (AT). AT can be defined as "any device or system that allows an individual to perform a task that they would otherwise be unable to do, or increases the ease and safety with which the task can be performed" (according to the United Kingdom Royal Commission on Long-term Care). Another definition is "any product or service designed to enable independence for disabled or older people" (according to the European Union SOPRANO Review State-of-the-Art and Market Analysis Deliverable D1.1.2 published in 2007) (10). Table 3.2 depicts some of the benefits of (and/or motivations for) MBAN technology (9).

Standards drive economy-of-scale benefits for components; standards also simplify the control and monitoring of patients in hospitals, in care facilities, and in homes. e-Health and m-health rely on groups of connected devices, including devices communicating with classic smartphones using near field communication (NFC) technology, or with other nodes using low power, short-range radio communication technology such as Bluetooth low energy (BLE), or ZigBee (10), Kingsley (39).

- ZigBee aims at enabling the deployment of reliable, cost-effective, low power, wireless monitoring and control products based on an open IEEE standard; it was designed with simplicity in mind and is efficient in the use of power, allowing monitoring devices to operate on commonly available batteries for years.
- BLE is a low power version of Bluetooth capable of reporting data from a sensor for up to a year from a small button battery; although the BLE data rate and radio range is lower than that of classic Bluetooth, also an IEEE standard, the low power and long battery life make it suitable for short-range monitoring applications in medicine.
- NFC is a form of contactless communication between devices such as smartphones or tablets and readers. Contactless communication allows a user to wave the smartphone over an NFC-compatible device to send information without requiring the devices to touch or to use a cable.

TABLE 3.2 Benefits of (and/or Motivations for) MBAN Technology

Benefit	Description
Transforming Patient Care, Saving Lives	• Almost 50% of all patients in US hospitals are not monitored. MBANs provide a cost-effective way to monitor patients in a healthcare institution, so clinicians *can provide real-time and accurate data*, allowing them to intervene and save lives • MBANs allow for ubiquitous and reliable monitoring and give healthcare providers the chance to identify life-threatening problems or events before they occur. According to a study by the Institute for Healthcare Improvement, a monitored hospital patient has a 48% chance of surviving a cardiac arrest—this number plummets as low as 6% without monitoring • Portions of MBAN spectrum can also be used outside the hospital and in patients' homes. Monitoring a patient at home saves money by reducing readmission rates • MBAN-equipped devices allow patients *greater independence and mobility*, both in the hospital and in the home, implying a higher level of comfort and care
Driving Down Costs	• With MBAN technology, physicians can intervene before a patient's condition seriously deteriorates—resulting in less time spent in the intensive care unit—and can reduce costly follow-up visits. One healthcare company estimates it could save *$1.5 million per month* if unplanned (emergency) transfers could be prevented by early detection and treatment • Disposable wireless sensors can also help decrease hospital-acquired infections. The industry estimates that disposable sensors could help to *save an estimated $2000 to $12,000 per patient*—more than $11 billion nationwide • As one example, remote monitoring of patients with congestive heart failure would create an annual savings of *over $10 billion a year*
Spurring Innovation in Mobile Health	• The m-health industry consists of mobile applications, cloud-based data management, wireless medical devices, and other solutions to increase patient engagement and improve the delivery of healthcare services • Almost 17 million people are accessing health data on their mobile phones in the United States, a 125% increase since 2010 • m-health is expected to be *a $2 to 6 billion industry* by 2015 • About 88% of doctors support patients monitoring their health at home, especially weight, blood sugar, and vital signs • Early detection allows earlier treatment and better outcomes. For example, after an initial hospitalization for heart failure, 60% of patients are readmitted at least once within 6–9 months. Industry estimates indicate that remote monitoring could *generate net savings of $197 billion* over 25 years from just four chronic conditions

These wireless technologies are discussed in more detail in Chapter 6.

In mid-2012, the US Federal Communications Commission (FCC) announced it was planning to allocate spectrum bandwidth in the United States for use of body sensors to monitor wirelessly a variety of patient's vital signs using MBANSs. The FCC was planning to adopt new rules to permit more intensive use of spectrum for wireless medical devices, making the United States the first country in the world to dedicate spectrum for MBANs in hospitals, clinics, and doctors' offices (9). Using the newly allocated spectrum bandwidth, the sensors on a patient's body wirelessly form a network to a designated control node that aggregates the results and transmits that data to centralized computer systems. The FCC's MBAN proposal is a multi-industry effort to foster innovation in this spectrum band (2360–2400 MHz) by allowing distinct but compatible users to share. This proposed use of spectrum provides wireless health manufacturers with *increased spectrum capacity and reliability*, giving them the certainty they need to streamline their product development, which for many years operated on a variety of frequencies. The proposed new spectrum allocation can:

- Provide more reliable service and increased capacity for the use of MBANs in hospital waiting rooms, elevator lobbies, preparatory areas, and other high density settings.
- Greatly improve the quality of patient care with more effective monitoring, catching patients before critical stages, improving patient outcomes, and ultimately saving lives.
- Decrease expenses while increasing competition and innovation, easing entry for companies that are developing new wireless medical devices.

Healthcare monitoring applications include chronic disease monitoring, personal wellness monitoring, and personal fitness. Chronic diseases include diabetes, asthma, heart diseases, and sleep disorders. Chronic diseases typically require some kind of health monitoring, especially in advanced stages of the disease progression. Chronic disease monitoring encompasses the following, as described in Reference 10 (on which the next few paragraphs are based):

- *Episodic patient monitoring*; this is utilized in noncritical patients to track specific indicators and identify the progress of the disease or recovery. In this use case, the patient's vital signs (e.g., heart rate, temperature) and disease-specific indicators (e.g., BP, blood glucose level, EKG) are monitored to determine anomalies and identify trends. The monitoring is done periodically, and all the information collected by the medical sensors is time-stamped and then securely forwarded to a gateway that functions as a patient monitoring system. Additionally, the gateway forwards the aggregated information in a secure way to a database server. Medical personnel and family caregivers can access the information stored in the database server to monitor the progress of the disease.
- *Continuous patient monitoring*; this is associated with acute conditions that require constant or frequent measurement of health status. In this case, the

vital signs (e.g., heart rate, temperature, pulse oximeter) are monitored on a constant basis to allow continuous measurement of patients' health status at rest or during mild exercise for purpose of treatment adjustment, recovery, or diagnosis. The vital signs measurements waveforms (e.g., pulse pleth wave or heart rate) are securely streamed to an on-body data collection unit for data fusion and/or sequential storage. The data is securely forwarded from the data collection unit to an off-body gateway (e.g., PC/laptop, PDA or mobile phone) for storage and data analysis; alternatively, the data can be sent directly to a mobile terminal. The patient or the care provider remotely activates the on-body sensors via the off-body unit; the measurement data from the body sensors is securely transmitted continuously to the on-body unit, where it is temporarily stored. Subsequently, the recorded measurement data is securely sent to the off-body unit via batch transmission for persistent storage and further analysis by the healthcare provider. Optionally, an off-body unit can also be used for secure waveform viewing during the measurement. The healthcare professional uses the captured data to provide the appropriate diagnosis or to adjust the treatment level.

- *Patient alarm monitoring*: this entails the triggering of alarms based on preset conditions that are specific to the patient and the disease. In this use case, the patient's vital signs (e.g., heart rate, temperature) and disease-specific indicators (e.g., BP, EKG, EEG) are monitored on a continuous basis. The data collected by the sensors is time-stamped and securely forwarded to a gateway that acts as a patient monitoring system. The gateway securely forwards the aggregated information to a database server. Additionally, at predetermined settings, alarms are issued and responses/actions could be triggered automatically. For example, if during the monitoring of a diabetic patient the blood glucose level falls below a certain threshold, an alert can be sent to the patient, physician(s), and/or medical personnel. Increasing the sampling rate of a given monitor can also be triggered once an alarm has been asserted. The alarm can be issued either by the medical device or by the gateway.

Personal wellness monitoring concerns a person's activity and safety (especially for the elderly). Applications include but are not limited to smoke alarms, panic buttons, motion sensors, home sensors (e.g., bed, door, window, shower), and other monitors for assisted living facilities. The information collected by these devices is securely transmitted to a central location for decision-making, analysis, trending, and storage. Personal wellness monitoring includes the following:

- *Senior activity monitoring scenario* focuses on monitoring an elderly person's daily activity. Besides a wearable medical sensors/devices that monitor the vital signs (e.g., heartbeat, body temperature), this application involves monitoring other nonmedical sensors such as environmental sensors. If an elderly person has to follow a certain daily schedule, for example, taking a weight measurement in the morning, obtaining glucose level readings at 11 AM and at 5 PM, and so on, the caregiver can monitor the daily activity status of the person. If certain routine activities are not completed, the person can be sent a reminder.

- *Safety monitoring scenario* deals with monitoring the safety of the home environment. The home environment is monitored for safety hazards including toxic gases, water, and fire. Additionally, the vital signs (e.g., heartbeat, temperature) of the persons in the home are also monitored.

Personal fitness monitoring includes (i) monitoring and tracking fitness level and (ii) personalized fitness schedule scenario:

- The *monitoring and tracking fitness level* use case focuses on tracking the fitness level or progress made by an individual. A number of parameters that the individual wishes to monitor are recorded as that individual performs his/her workout routine (e.g., while running on a treadmill, the individual monitors his/her heart rate, temperature, and blood oxygen level). This information, obtained from medical sensors that are worn by the individual, is securely streamed to a gateway or a collection data unit and displayed on the treadmill's console in real time, along with other performance information provided by the treadmill. Additionally, the gateway sends the information to a database server for recordkeeping.
- The *personalized fitness schedule* use case focuses on personalization of the fitness schedule of an individual. The schedule to be followed by that individual can be entered by a trainer or the individual. For example, training for a marathon could include running on a treadmill according to a schedule designed by his/her trainer. For each training day, the trainer schedules the distance, the pace, and the maximum heart rate at which the individual is to train. The trainer would also like to monitor the individual's respiration pattern. While the distance and the pace are provided by the treadmill, the heart rate and the respiration are monitored by wireless medical devices worn by the individual.

Some press time demonstrations of MBAN technology included the following:

- *Fetal telemetry*: A small, lightweight, and noninvasive way to continuously monitor a baby's health, while allowing the mother to move freely.
- *LifeLine home care pendants*: A device that collects health information for the elderly or those with chronic diseases—allowing them to live independently with the security and peace of mind that they are being monitored.
- *Predictive and early warning systems*: Provides continuous monitoring to help prevent sudden and acute deterioration of a patient's condition.
- A greatly abbreviated press time list of specific illustrative *examples* in this arena includes the following.[2]

[2] Companies named in this text are simply illustrative examples of entities that may offer technologies and services under discussion at point in the text; named companies are generally not the only suppliers that

Sierra Wireless has developed Positive ID secure modules to provide support for diabetics through monitoring levels of glucose in the blood. Cinterion/Gemalto has developed Aerotel, a system capable of modulating in real time the flow of air sent to people suffering from sleep apnea; the company has also developed M2M modules to remotely monitor problems of cardiac arrhythmia in real time. The first applications of NFC technology appeared recently in the United States with the launch by the company iMPack of a system "tracking" the quality of sleep, allowing a clock to transmit data collected during the night to the Nokia C7 NFC smartphone. It uses an embedded application to generate an initial result, which can then be transmitted to a physician (11).

Press time research issues for WBANs include but are not limited to the following:

- Antenna design for in- and on-body networks
- Channel modeling radio propagation issues for WBAN
- Electromagnetic radiation and human tissues
- Interference management and mitigation
- Coexistence of WBAN with other wireless technologies
- Protocols and algorithms for the PHY, MAC, and network layer
- End-to-end quality of service (QoS) provision for WBAN
- Energy-efficient and low power consumption protocols
- Power management for WBAN
- Integration of WBAN with heterogeneous networks
- (Lightweight) security, authentication, and cryptography solutions for WBAN
- Standardization activities

3.4 CITY AUTOMATION

Some applications in this domain include but are not limited to the following:

- Traffic flow management system in combination with dynamic traffic light control
- Street light control
- Passenger information system for public transportation
- Passive surveillance (see Section 3.9)

Generic city sensors include environmental sensors and activity sensors. Environmental sensors include:

– thermal
– hygrometric

may provide such services, and mention of a company and/or service does not imply that such entities or capabilities are recommended herewith, or considered in any way better than others.

- anemometric
- sound
- gas
- particles
- light, other EM spectrum
- seismic

Activity sensors include:

- pavement/roadway pressure
- vehicle and pedestrian detection
- parking space occupancy

ETSI TR 102 897: "*Machine-to-Machine Communications (M2M); Use Cases of M2M Applications for City Automation*" provides the following description of these applications (12):

Use Case 1: Traffic Flow Management System in Combination with Dynamic Traffic Light Control. The flow of road traffic within cities depends on a number of factors such as the number of vehicles on the road, the time and the day, the current or expected weather, current traffic issues and accidents, as well as road construction work. Traffic flow sensors provide key traffic flow information to a central traffic flow management system; the traffic flow management system can develop a real-time traffic optimization strategy and, thus, endeavor to control the traffic flow. The traffic control can be achieved by dynamic information displays informing the driver about traffic jams and congested roads; traffic signs can direct the traffic to utilize less used roads. The traffic flow management system can also interact with controllable traffic lights to extend or to reduce the green light period to increase the vehicle throughput on heavy used roads; dynamically changeable traffic signs can lead to an environment where the vehicular traffic is managed more efficiently, thus enabling cities to reduce fuel consumption, air pollution, congestions, and the time spent on the road.

Use Case 2: Street Light Control. Street lights are not required to shine at the same intensity to accomplish the intended safety goal. The intensity may depend on conditions such as moonlight or weather. Adjusting the intensity helps to reduce the energy consumption and the expenditures incurred by a municipality. The street light controller of each street light segment is connected (often wirelessly) with the central street light managing and control system. Based on local information measured by local sensors, the control system can dim the corresponding street lights of a segment remotely or is able to switch street lights on and off.

Use Case 3: Passenger Information System for Public Transportation. Public transportation vehicles, such as busses, subways, and commuter trains, operate on a schedule that may be impacted by external variables and, thus, have a degree of variability compared with a baseline formal schedule. Passengers need to know when their next connection is available; this information also allows passengers to select alternative connections in the case of longer delays. In this application, the current locations of the various public transport vehicles are provided to the central system that is able to match the current location with the forecasted location at each time or at specific checkpoints. Based on the time difference, the system is able to calculate the current delay and the expected arrival time at the upcoming stops. The vehicle location can be captured via checkpoints on the regular track or via GPS/general packet radio service (GPRS) tracking devices that provide the position information in regular intervals. Two approaches are possible:

- With a checkpoint-based approach, the line number (of the bus or the street car) is captured at each station where the vehicle stops regularly, or at defined checkpoint in between. Because of the fact that the sensor at a specific station is able to provide the data to the central system, the expected delay can be calculated by comparing the information of the scheduled arrival time and the actual arrival time. This change can be added to the arrival time displayed at each following station. Each vehicle must be equipped with a transponder (variously based on infrared, radio frequency identification (RFID), short-range communication, or optical recognition). In addition, each station has to be equipped with one or more checkpoint systems that are able to readout or to receive the line number information of the vehicle. In case of larger stations with several platforms, multiple systems are needed.
- With a GPS/GPRS-based approach, each vehicle has to be equipped with a GPS/GPRS tracking device that provide, besides the current position, the information that can be directly or indirectly matched to the serviced line number. Based on the “regular” position/time pattern, the system is able to calculate the actual time difference and provide the expected time on the passenger display.

A combination of checkpoint- and GPS/GPRS-based solution can be used to integrate railed vehicles (such as subways and street cars) and road vehicles (such as busses).

3.5 AUTOMOTIVE APPLICATIONS

IoT/M2M automotive and transportation applications focus on safety, security, connected navigation, and other vehicle services such as, but not limited to, insurance or road pricing, emergency assistance, fleet management, electric car charging management, and traffic optimization. These applications typically entail IoT/M2M communication modules that are embedded into the car or the transportation equipment. Some of the technical challenges relate to mobility management and environmental hardware considerations. A brief description of applications follows from Reference 13 (on which the next few paragraphs are based).

- *bCall (breakdown call):* A bCall sends the current vehicle position to a roadside assistance organization and initiates a voice call. The bCall trigger is usually a switch that is manually pushed by the user in order to activate the service. An “enhanced” bCall service allows current vehicle diagnostic information to be transmitted in addition to the vehicle position.

- *Stolen vehicle tracking (SVT):* A basic application for automotive M2M communications is tracking of mobile assets—either for purposes of managing a fleet of vehicles or to determine the location of stolen property. The goal of a SVT system is to facilitate the recovery of a vehicle in case of theft. The SVT service provider periodically requests location data from the Telematics Control Unit (TCU) in the vehicle and interacts with the police. The TCU may also be capable of sending out automatic theft alerts based on vehicle intrusion or illegal movement. The TCU may also be linked to the Engine Management System (EMS) to enable immobilization or speed degradation by remote command. Vehicles contain embedded M2M devices that can interface with location-determination technology and can communicate via a mobile cellular network to an entity (server) in the M2M core. The M2M devices will communicate directly with the telecommunication network; the M2M devices will interface with location-determination technology such as standalone GPS, or network-based mechanisms such as assisted GPS, Cell-ID, and so on. For theft-tracking applications, the M2M device is typically embedded in an inaccessible or inconspicuous place so that it may not be easily disabled by a thief. The tracking server is an entity located in the M2M core and owned or operated by the asset owner or service provider to receive, process, and render location and velocity information provided by the deployed assets. The tracking server may trigger a particular M2M device to provide a location/velocity update, or the M2M devices may be configured to autonomously provide updates on a schedule or upon an event-based trigger.
- *Remote diagnostics*: Remote diagnostic services can broadly be grouped into the following categories:
  - Maintenance minder—when the vehicle reaches a certain mileage (e.g., 90% of the manufacturer’s recommended service interval since the previous service), the TCU sends a message to the owner or the owner’s named dealership, advising the owner (or the dealership) that the vehicle is due for service.
  - Health check—Either on a periodic basis or triggered by a request from the owner, the TCU compiles the vehicle’s general status using inbuilt diagnostic reporting functions and transmits a diagnostic report to the owner, the owner’s preferred dealership, or to the vehicle manufacturer.
  - Fault triggered—When a fault (a diagnostic trouble code [DTC]) is detected with one of the vehicle systems, this triggers the TCU to send the DTC code and any related information to the owner’s preferred dealer, or to the vehicle manufacturer.
  - Enhanced bCall—When a manual breakdown call is initiated by the owner, the TCU sends both position data and DTC status information to the roadside assistance service or to the vehicle manufacturer.

- *Fleet management:* The fleet owner wishes to track the vehicles—that is, to know, over time, the location and velocity of each vehicle—in order to plan and optimize business operations. A fleet management application assumes that a fleet of vehicles have been deployed with M2M devices installed that are able to:
    - Interface with sensors on the vehicle that measure velocity
    - Interface with devices that can detect position
    - Establish a link with a mobile telecommunication network using appropriate network access credentials, such as a USIM (universal subscriber identity module)

A server in the fleet owner's employ receives, aggregates, and processes the tracking data from the fleet and provides this information to the fleet owner. Devices could be configured to autonomously establish communication with the server via a cellular network either at regular intervals, at prescheduled times, or based on some event such as crossing a geographic threshold. Alternatively, the M2M devices could be commanded by the M2M server to report their location/velocity data. See Figure 3.5 for an illustrative example.

- *Vehicle-to-infrastructure communications.* A European Intelligent Transport Systems Directive[3] seeks the implementation of eSafety applications in vehicles. Some vehicle manufacturers have begun to deploy vehicle-to-vehicle communication, for example, in the context of wireless access in vehicular environments (WAVE). On the other hand, vehicle to roadside applications are less well-developed; in this case, vehicles have embedded M2M devices that can interface with location-determination technology and can communicate via a mobile telecommunication network to an entity (server). This application assumes that vehicles have been deployed with M2M devices installed that are able to:
    - Interface with sensors on the vehicle that measure velocity, external impacts
    - Interface with devices that can detect position
    - Establish a link with a mobile telecommunication network using appropriate network access credentials, such as a USIM
    - Upload or download traffic and safety information to a traffic information server

Devices could be configured to establish communication with the server via the cellular network based on some event triggered by a vehicle sensor such as external impact, motor failure, and so on. For example, the traffic information server pushes roadside or emergency information out to vehicles based on location (cell location or actual location). Or, vehicle information is pushed to the traffic information server

[3] A directive is a legislative act of the European Union requiring member states to achieve a stated result but without mandating the means of achieving that result.

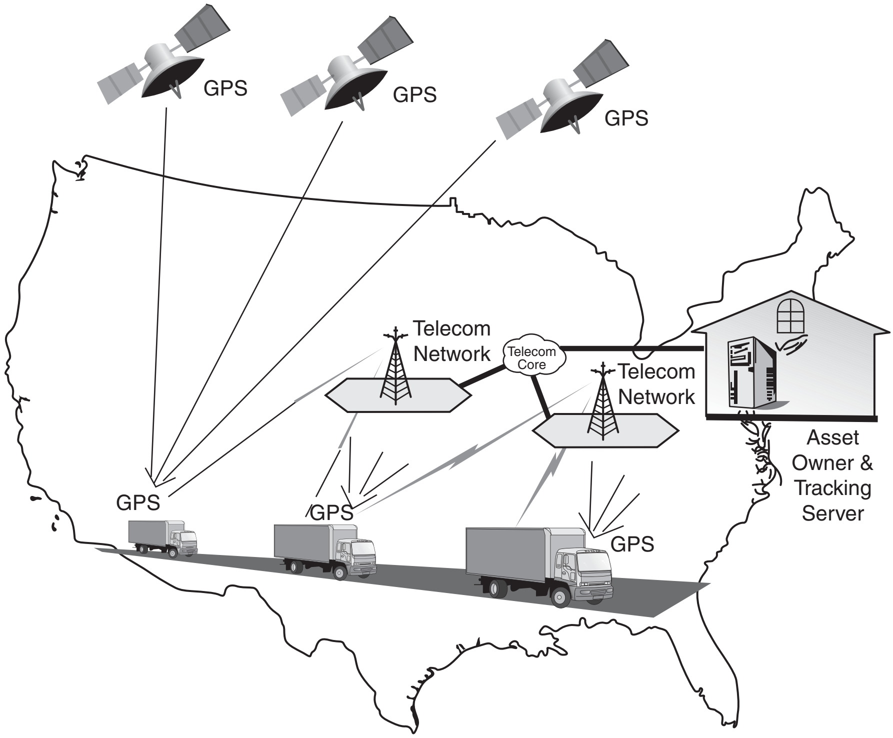

FIGURE 3.5 Vehicular asset tracking.

based on external sensor information, internal sensor information, or subscription basis. See Figure 3.6.

- *Insurance services:* Pay-as-you-drive (PAYD) schemes offer insurers the opportunity to reduce costs based on actual risk and provide more competitive products to the end-user based on getting feedback from the vehicle as to when, where, how, or how far the vehicle is being driven (or a combination of these factors).

3.6 HOME AUTOMATION

Home automation has received a lot of attention of late in the IoT/M2M context. Basic applications of the automated home include remote media control, heating control, lighting control (including low power landscape lighting control), and appliance control. Sensed homes, as examples of smart space, are seen as “next-step/next-generation” applications. Smart meters and energy efficiency (making use of the potential of SG), discussed above, also fit this category. Telehealth (e.g., assisted living and in-home m-health services) also can be captured under this set of applications; security and emergency services also can be included here.

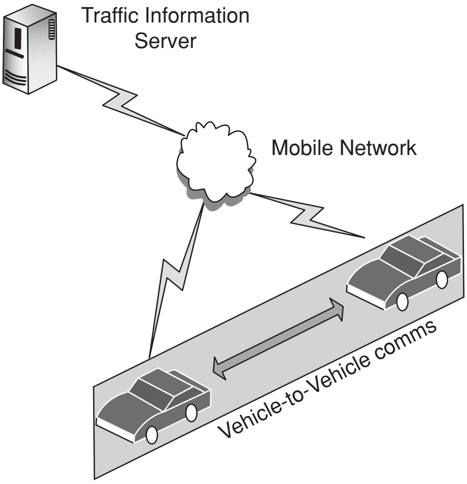

FIGURE 3.6 Vehicle-to-infrastructure communications.

M2M communications is expected to play a major role in residences, where instrumentation of elements supporting daily living (e.g., appliances), comfort, health, security, and energy efficiency can improve the quality of life and the quality of experience. Home control applications include but are not limited to:

- Lighting control
- Thermostat/HVAC
- White goods/
- Appliance control
- In-home displays

Home security applications include but are not limited to:

- Door access phone
- Window locks
- Motion detector
- Smoke/fire alert
- Baby monitors
- Medical pendant

See Figure 3.7 for an illustrative example.

Energy efficiency at home is a key application of interest because of the possibility of monetary saving for the consumer. Occupancy sensors can be used to establish whether there is somebody in a room or not and when the room becomes unoccupied the lights are automatically switched off; other types of sensors can be used to control

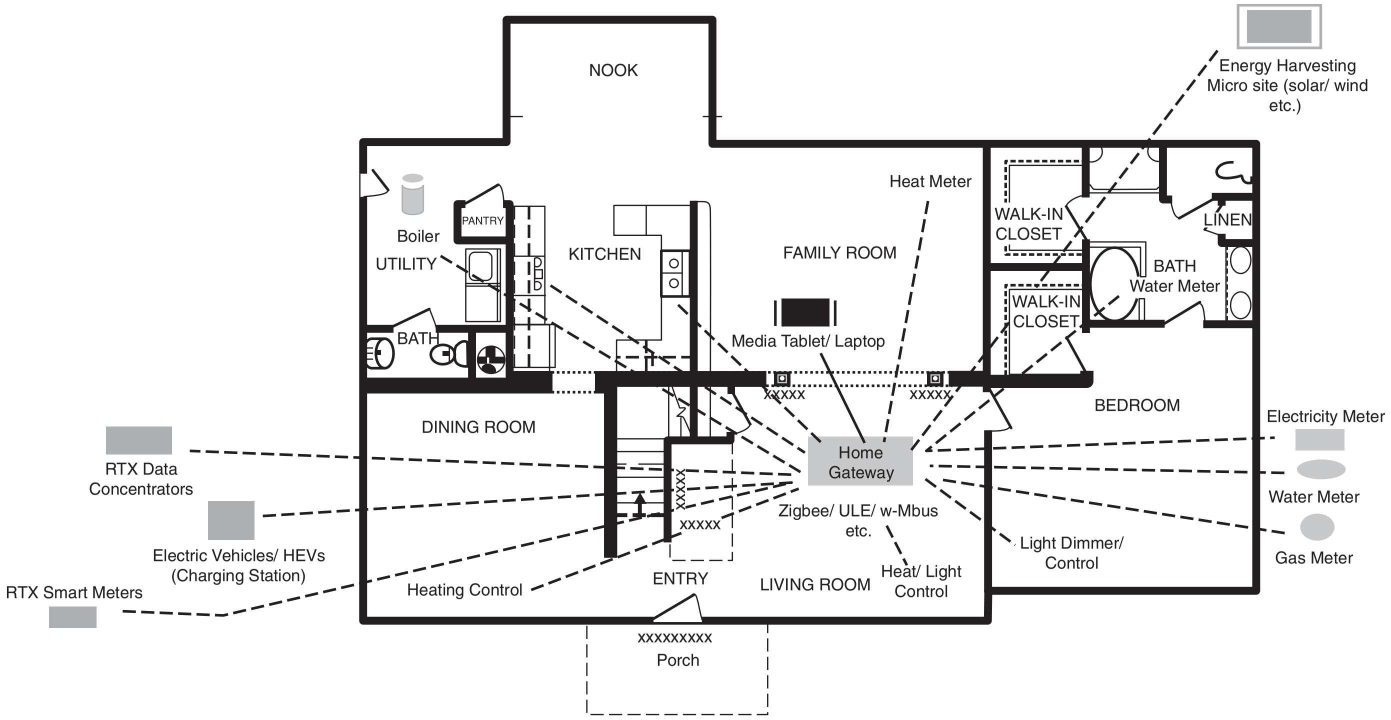

FIGURE 3.7 Home automation example.

the energy consumption from different equipments (e.g., temperature, TVs, and so on). The sensors and actuators can be autonomous (as in the case of light sensors), or can be connected to an M2M gateway control node (wirelessly or using wires, e.g., via PLC). By integrating the data from a plethora of sensors (e.g., outside temperature, multizone heating status), the gateway can dispatch the appropriate commands to the relevant actuators (e.g., to switch off the heater in a room or zone, or in the entire house). The M2M system allows reducing energy consumption by automatically adapting the use of the house equipment to various short-term situations (people moving in and out of rooms, people going to work and retuning later) or long-term situations (people taking vacations or long weekends or managing a second/vacation home) (5).

3.7 SMART CARDS

Smart cards (SCs) in general, and M2M-based systems in particular, enable wired and wireless communication for a large set of commercial and industrial applications. SCs are now routinely accepted as credentials for controlling secure physical access. The purpose of an SC is to safeguard user identities and secret keys and to perform requisite cryptographic computations (an SC is a tamper-resistant device). SC technology includes contact and contactless systems. A terminal is the entity with which the SC can establish a secure channel. Examples include generic card acceptance devices (CADs), a CAD on a mobile handset, a Set-top box, a laptop/PC/tablet. See Figure 3.8.

Applications include utility monitoring, vending machines, security systems, industrial machines, automotive, traffic management, speed cameras, and medical equipment. A more inclusive list of SC applications is as follows:

- Biometrics
- Cybersecurity
- Enterprise ID
- Government ID
    - ePassport
    - FIPS 201
    - Real ID
    - Passport Card/WHTI
- Healthcare
- Identity
- Logical access
- Market research
- Mobile telecommunications
- Network security

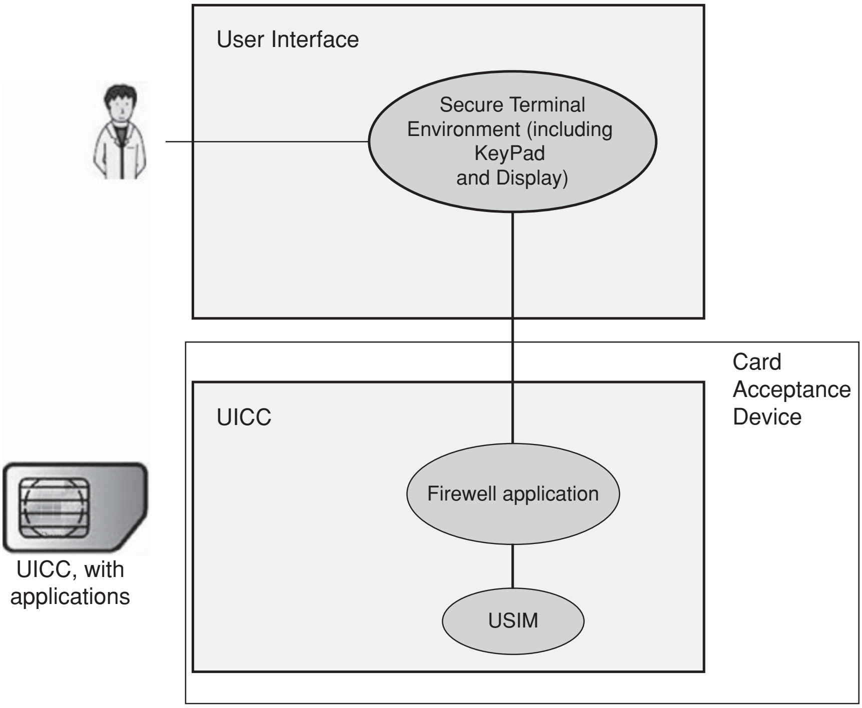

FIGURE 3.8 UICC environment, including user interfaces.

- Payments
  - POS
  - Contactless payments
  - EMV payments
  - Mobile payments/NFC
  - Transportation payments
- Physical access
- Privacy
- RF/RFID tags
- Security
  - ePassport security
  - Contactless payments security
  - Transit fare payment system security
- Transportation (toll tags, speed-of-vehicle readers)

These applications require advanced, durable USIM cards. SCs are resource-limited devices because they are designed to be economic and portable (small and light).

In recent years, memory size on SCs has increased from KBs up to MBs; this trend is expected to continue in the future allowing operators to offer enhanced new services.

Applications such as electronic payment, electronic ticketing, and transit can be combined with physical access to provide a multiapplication and multitechnology ID credential; the issuer can also record and update appropriate privileges from a single central location. Contactless SCs can authenticate a person's identity, determine the appropriate level of access, and admit the cardholder to a facility, all from data stored on the card; SCs can also include additional authentication factors (such as biometric templates) and other card technologies (such as an SC chip) (14). Another application example is POS use. Currently, most POS terminals are connected using a wired connection; as a consequence, the terminals are placed at a fixed position within the establishment in question, and the person needing to perform a transaction is required to go to the location of the POS terminal—this may be inconvenience or restrict commerce (in some fashion). In some cases (e.g., remotely located POS terminals, parking meters, garage checkout booths, and so on), a wired connection is difficult and costly to be installed. An option, therefore, is to connect POS terminals via a secure wireless connection. As M2M communication modules are installed into wireless POS terminals, street parking, and ticketing machines, and so on to provide communication for credit or debit card online transactions, new commercial applications become a reality (5).

Contactless cards use NFC to communicate and receive power over short distances; since these devices do not need physical contact with a reader, they simplify operation and increases transaction speeds. For transponders to work they require power, although the levels are very small. Passive devices operate without an internal battery source, deriving the power to operate from the field generated by the reader; this implies that passive devices offer an unlimited operational lifetime but have shorter read ranges and require a higher-powered reader (15). There are three basic contactless technologies considered for physical access control applications: 125 kHz, ISO/IEC 14443, and ISO/IEC 15693 technologies.

- 125 kHz read-only technology is used by many of today's RFID access control systems and is based on de facto industry standards rather than international standards. 125 kHz technology allows for a secure, uniquely coded number to be transmitted and processed by a back-end system. The back-end system then determines the rights and privileges associated with that card.
- Contactless SC technology based on ISO/IEC 14443 and ISO/IEC 15693 standards are intelligent, read/write devices capable of storing different kinds of data and operating at different ranges. Contactless SCs operate at 13.56 MHz and are further divided into proximity (ISO 14443) and vicinity (ISO 15693) devices with nominal operating ranges of up to 10 cm and 1 m, respectively. ISO 14443 specifies A and B operation modes that use different communication and card selection procedures. The ISO 14443A standard is used with most contactless cards and is compatible with the lower layers of popular commercial products. The standard specifies the operating frequency, modulation and coding schemes

> (ISO 14443-2), anti-collision routines (ISO 14443-3), and communication protocols (ISO 14443-4). It uses amplitude shift keying (ASK) modulation with modified miller coding (106 Kbps) in reader to card communication (15).

NFC setups allow a device (known as a *reader*, *interrogator*, or *active device*) to create a radio frequency current that enables communication with another NFC-compatible device or a small NFC tag holding the information the reader wants. Passive devices, such as the NFC tag in smart posters, store information and communicate with the reader, but do not actively read other devices. Peer-to-peer communication through two active devices is also a possibility with NFC, allowing both devices to send and receive information. NFC maintains interoperability between different wireless communication methods such as Bluetooth and other NFC standards including FeliCa—popular in Japan—through the NFC Forum. Founded in 2004 by Sony, Nokia, and Philips, the NFC Forum enforces standards that manufacturers must meet when designing NFC-compatible devices. This ensures that NFC is secure and remains easy to use with different versions of the technology. Compatibility is the key to the growth of NFC as a popular payment and data communication method. It must be able to communicate with other wireless technologies and be able to interact with different types of NFC transmissions. For example, by integrating credit cards, subway tickets, and paper coupons all into one device, a customer can board a train, pay for groceries, redeem coupons or store loyalty points, and even exchange contact information all with the wave of a smartphone. NFC technology is popular in parts of Europe and Asia and is also being deployed in the United States. As an illustrative example, Google launched Google Wallet that supports MasterCard PayPass, PayPal offers money transfers between smartphones, and other companies are expected to follow suit. The expectation is that as the technology is deployed, more NFC-compatible smartphones will be available, and more stores will offer NFC card readers for customer convenience (16). This topic is revisited later in the text.

SC use depends on the environment in which they are deployed. For example, in banking, user information includes identity, account information, and possibly information on recent transactions made and secret keys used in security functions; the operations allowed encompass card holder authentication, automatic transaction registration, and transaction nonrepudiation. In mobile communications, user information includes identity, personal information such as address book, operator-related information, and again secret keys used in security functions. Functions executed include user authentication, voice encryption, as well as data access to user's private information. There are no peripherals that allow user direct access, such as a keyboard or a screen: SC access must go through a terminal, and, unless the communication is secure end-to-end, this may constitute a security weakness. System security is determined at the weakest link and, unless strengthened, attackers may target the terminal or the data exchange with the terminal, to get round the robustness of the tamper-resistant device (17). For example, a UICC (Universal Integrated Circuit Card) is the SC used in mobile terminals in GSM and UMTS networks. A UICC typically contains several applications, and the same SC provides access to both GSM and UMTS networks. The UICC also provides storage (e.g., for a directory). In a GSM network, the UICC contains a subscriber identification module (SIM) application; in a UMTS network it is the USIM application. It is a new-generation SIM included in cell phones or laptops using high speed 3G cellular networks. The UICC SC typically has a CPU, ROM, RAM, EEPROM, and I/O circuits.

Occupational use of health cards still lags behind that of credit cards and mobile phone SIM/USIM cards, but they are finding applications in countries where the health system is subject to extensive major fraud and where the costs of conventional treatment of medical data are becoming difficult to manage. The Health Information Technology for Economic and Clinical Health (HITECH) Act, signed in the United States in February 2009, encourages stakeholders in the health ecosystem to work toward the creation of a network (protected health infrastructure) for the collection and exchange of standardized medical data (electronic health record) using "certified technology" capable of simultaneously ensuring the availability, sharing, security, accuracy, and confidentiality of such data. Although not explicitly named, smart security technologies are at the forefront of this trend: any candidate technology must be able to handle the rights of all stakeholders (patients, doctors, nurses, specialists, pharmacists, and so on), keys and certificates, means of encryption, and strong authentication (in some cases, biometric). The American Medical Association (AMA) has stressed the benefits offered by the use of an SC that stores personal medical information (allergies, blood type, current treatment, and so on), especially in emergency situations. The Secure ID Coalition, which also campaigns in the United States for the generalization of personal health cards, observed recently that SCs could be employed to reduce fraud in health spending of around $370 billion over a period of just 10 years. Several health SCs have already emerged in the United States as of press time. For example, LifeNexus[4] launched a health card that also serves as a personal credit card. A bracelet containing a contactless chip (MasterCard PayPass) has also been issued; the bracelet contains a unique number (VITAnumber[5]), providing access in emergencies to the bearer's personal medical data. Germany was preparing to launch a new generation of health cards (eGK Generation 1plus) designed in conjunction with insurance companies for online use. In France, the new CPS3 card for health professionals entered circulation earlier this year; this contactless card is now in line with the European IAS ECC standard (signature, identification, and authentication) (11).

Other examples of SC/UICC applications include the following as described in Reference 17 (some of these applications require a high speed dedicated channel between UICC and terminal):

- The UICC is a control point for device management (DM). DM aims to provide the protocols and mechanisms to achieve remote management of devices. DM includes: (a) setting initial configuration information in devices; (b) subsequent installation and updates of persistent information in devices (firmware update);

[4] See previous footnote.

[5] VITA Products Incorporated's VITAnumber is a unique numerical identifier printed on a VITAband that is individually assigned to each user. The VITAnumber links the user to his/her Emergency Response Profile (ERP). Unlike other ID bracelets, which print all the personal information on the band, the VITAnumber anonymizes the personal information until it is needed.

(c) retrieval of management information from devices; and (d) processing events and alarms generated by devices. In this application, the SC inserted in the device is expected to: (i) support dynamic provisioning of the device with up-to-date information and (ii) handle a part of the security during the update of device firmware (service access controlled by the operator, authentication of the origin, and so on). To achieve this, the SC must store DM objects accessible by the device through the SC to device interface and also manageable by a remote server (through the device).

- Digital rights management (DRM) and distributed applications. DRM is used to secure media content owned by a service provider; the end-user has a limited set of rights to use the content. Usually, media content is supposed to be rendered on any type of compatible terminal (e.g., CD audio on any CD player) so that the user can transport his/her content wherever he/she wants. Adding security should not change this user experience. When the user is a mobile network operator (MNO) subscriber, the rights are bound to a device, not to a user. This implies that when the user needs to change the player (i.e., the handset), the rights have to be downloaded onto the new device and the certificates are to be recalculated with the new terminal ID. This scheme works well as long as a network connection is available and/or the terminal belongs to the same user domain.
- Multimedia file management. As the UICC will be able to store and encrypt/decrypt multimedia files (such as multimedia message service [MMS], pictures, MP3 files, video clips), customer's usability and quality user experience cannot be compromised by a too long wait for the data download/upload. For example, it could be of interest to associate an image, a sound, and eventually a short video with the information relative to each contact in order to display all the images and video when accessing the phonebook.
- Man–machine interface (MMI) on UICC. Large-sized SCs offer the possibility to store card issuer's MMI in the UICC. During initialization process, the terminal can detect the type of UICC (which operator, which service providers, which features) and upload the whole MMI that the card issuer has defined for its purposes and its services.
- Real-time multimedia data encryption/decryption. UICC can be used to directly encrypt/decrypt data stream (such as protected voice communications or streamed video and music). For example, the user should be able to receive multimedia files encrypted using rights stored inside the UICC. Both the content and its decryption key should be stored in the UICC and also the decryption process could be executed inside the card. The decrypted content could be offered via a streaming protocol in order to increase the level of security. In addition, the user could also store personal contents in the UICC and send them after having protected them through encryption features of the UICC.
- Storage of terminal applications on the UICC. UICC could be used to store and distribute applications that could be uploaded by the terminal during the initialization phase or later. The uploading from the UICC to the terminal (or vice versa) of the applications should happen dynamically according to

user rights purchased from the operator. This enables efficient management of operator-related applications on the terminal and easy deployment of innovative services on the field.

- Direct and indirect UICC connection to a PC. As it is now possible for some devices, it should be possible either to insert a UICC directly into a PC laptop or to connect the handset to PC laptop in order to download/retrieve some personal data (MMS, pictures, movies, applications, and so on) to/from the card in a very quick time but also to easily execute cryptographic operations for accessing a secure environment (e.g., PKI for e-commerce). The user should consider the UICC as his/her trusted storage device, ensuring acceptable performances for the targeted use.
- Web server on SC. UICC can be considered similar to a web server, to which an Internet connection can be established with a usual Internet browser. Such a solution removes the needs of deployment of middleware to interface the functionality of the UICC as standard browsers and protocols would be used to access UICC contents and applications. Contents will be both stored and dynamically generated on the SC and then transferred to the terminal: the aim is to reuse standard graphic features of handsets to allow mobile operators to offer attractive and secure services. An effective communication interface between the terminal and the UICC will enhance the web server performances; TCP/IP-based communication allows internal pages (in the UICC) to be served locally and remotely using standard protocols and methods.
- Antivirus on UICC. The usage of the UICC as a storage device or the downloading on it of new applications and services leads to the need of antivirus running on the UICC itself, as is the case in a PC environment. The UICC could be able to perform auto-scan, to update virus signature or manage user rights.
- High priced ticketing scenario. Tickets can be purchased and stored securely on the UICC. In view of the (medium to) high value of the tickets, the UICC-based implementation must provide adequate protection mechanisms (e.g., to make it useless to steal someone's phone to enter an event). The UICC-based ticket may need the system to authenticate itself before each ticket can be viewed, used, or deleted. The ability to view and legitimately and securely transfer tickets is potentially an added benefit for tickets stored in a UICC (as compared with a "classical" contactless card). For this type of application, UICC-based ticketing offers the issuers of these tickets a cheaper way of implementing a contactless ticketing system. For the user, UICC-based ticketing should offer a more convenient and secure way to carry ticket and more flexible purchase experience.
- Payment application. Here the UICC contains the application and data required for contactless payment application. The terminal containing the UICC in this scenario has two possibilities: (i) it can act like a contactless payment application to pay at a contactless-enabled POS; (ii) it can act as a proxy for a payment account in which a third party performs a debit transaction, passing the payment to the merchant.

- Loyalty application. Here the UICC contains the application and data required for loyalty application. The terminal containing the UICC can act like a contactless loyalty application at a contactless-enabled POS.
- Healthcare application. Here the UICC contains the application and data required for a healthcare application. The terminal containing this UICC is used to store medical and health insurance data. These essential data would be available whatever the powering mode of the UICC. The use of the contactless interface may occur in places where strict security or safety rules apply (e.g., regulations requiring a terminal to be switched off in a hospital).

The SC Alliance is an advocate for a multitude of applications of SC technology; it is a not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for SC technology—the Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, healthcare, retail and entertainment industries, as well as a number of government agencies.

3.8 TRACKING (FOLLOWING AND MONITORING MOBILE OBJECTS)

Track and trace applications are typical of automotive environments as well as of goods movement in production environments, distribution, and retail; in the latter case RFID tags are often utilized. Automotive applications are focused on (i) physical security for people such as emergency situations, (ii) asset tracking for theft or law enforcement applications, and (iii) fleet management to achieve increased operational efficiency. Other facets of these services include remote diagnostics, navigation systems, PAYD (insurance, in-car services), and so on. See Table 3.3, loosely based on references (5, 13). In these applications, the M2M modules will have to function in an extended temperature and humidity range; in addition, the connection with the M2M communication module will have to withstand the vibration produced by the engine of a car, truck, or construction machinery, as well as by the movement of the vehicle on the road. Tracking devices are often placed in harsh environments; this means that may experience strong vibrations or shocks. The space is often very limited, implying that the size of the M2M communication module needs to be kept to a minimum.

Tracking (such as vehicles of any kind, containers, people, pets, and so on) is a common application implemented in conjunction with GPS; it can also be implemented using cellular technology. GPS is based on a cluster of satellites that continually send out signals. The satellites orbit the earth approximately every 12 h; the height of the orbits is about 20,183 km in the MEO (medium earth orbit). See Figure 3.9. GPS receivers can determine their position based on the time delay between transmission and reception of the signals transmitted by the satellites. The satellites are arranged on six planes, each of them containing at least four slots where satellites can be arranged equidistantly. Typically more than 24 GPS satellites orbit the earth (Russia and Europe are also planning to deploy their own GPS systems). In theory,

TABLE 3.3 Track and Trace Application Examples

Example	Description
Emergency call	The in-vehicle emergency call system can automatically or manually send location and driver information to an emergency center. The in-vehicle M2M communication module supports the transfer of emergency call data between the vehicle and the emergency service center. The on-board M2M communication module is connected to sensors that can identify an accident event and in such case set up a connection to an emergency center forwarding information about the location, an indication about the level of the accident, and possibly other additional information. A key requirement for this application is that the M2M module and its sensors/interfaces are able to survive and operate after a shock caused by an accident
Fleet management	For this application, a vehicle has a built-in M2M communication module (typically owned by the service provider not the driver) that collects information, such as location, timings, traffic jams, maintenance data, and travel location environmental conditions at any point along the way. This information is transmitted by the module via a mobile network to a server application where it is used to track the vehicle and deliveries. Using real-time information (such as traffic conditions), a logistics application can optimize the delivery plan and route; the updated delivery plan is then sent to the vehicle's driver. Using maintenance-related information, maintenance can be planned or remote emergency maintenance can be performed. In addition, environmental sensors can be used to retrieve information on the storage environment and condition of product being transported
Theft tracking	In this application, the use of M2M capabilities allows the recovery of a stolen vehicle. The M2M module supports secure communication over the network to a third-party entity. The M2M module needs to be protected against theft and misuse; another factor in this environment is the often limited space available to conceal or secure the system from theft and misuse, implying that the size of M2M modules should be kept small
Person/animal protection/ tracking	In this application, humans (e.g., workers, healthcare, elderly, or children) and/or animals are equipped with portable and/or wearable devices incorporating an M2M communication module that transmits information (automatically or on demand) to a server application used to monitor the status and positioning of the subject. Cellular and/or GPS-based triangularization functions are used. These services may be implemented via applications residing inside the M2M module/ UICC
Object protection/ tracking	The purpose of this application is to track and trace. In this application, objects (e.g., containers, construction equipment, and so on) are equipped with portable devices containing an M2M communication module, and optionally a GPS function, which forward location/status information either automatically or on demand to a server application; the server can monitor the status and location of those objects

FIGURE 3.9 GPS satellites.

three satellites emitting signals are sufficient to determine the precise position and height; in practice additional satellites are utilized. GPS allows one to establish the receiver's position as well as the receiver's speed and direction (this is done by measuring the Doppler effect or the numerical differentiation of a location according to time). Figure 3.10 shows a basic service arrangement: the DEP is comprised of a GPS sensor and a cellular modem; the GPS sensor transfers the position data to the cell modem and the modem transmits the position data to the DIP via a cellular network. The positioning data is then manipulated, displayed (e.g., using a map or GIS—geographic information system), and/or stored as needed.

3.9 OVER-THE-AIR-PASSIVE SURVEILLANCE/RING OF STEEL

Integrated open-air surveillance (IOS) technologies such as high resolution digital video surveillance (DVS), license plate recognition technology, facial recognition systems, traffic light cameras, gunshot detection systems (GDSs), aerial surveillance with drones (UAVs—unmanned aerial vehicles), and other related technologies are increasingly being put to use to support public safety mandates at a reduced surveillance/interdiction costs for those jurisdictions that deploy the infrastructure, while at the same time generating revenues for service providers and system integrators. *Open air* refers to the fact that the surveillance is done in the public domain; this type of surveillance can be done, for example, with (i) high resolution (even low light level) digital video cameras (which can be wired and/or wireless); (ii) license plate/face recognition technology; (iii) GDSs; and (iv) other related technologies or sensors. *Integrated* refers to the internetworking of multiple geographically dispersed

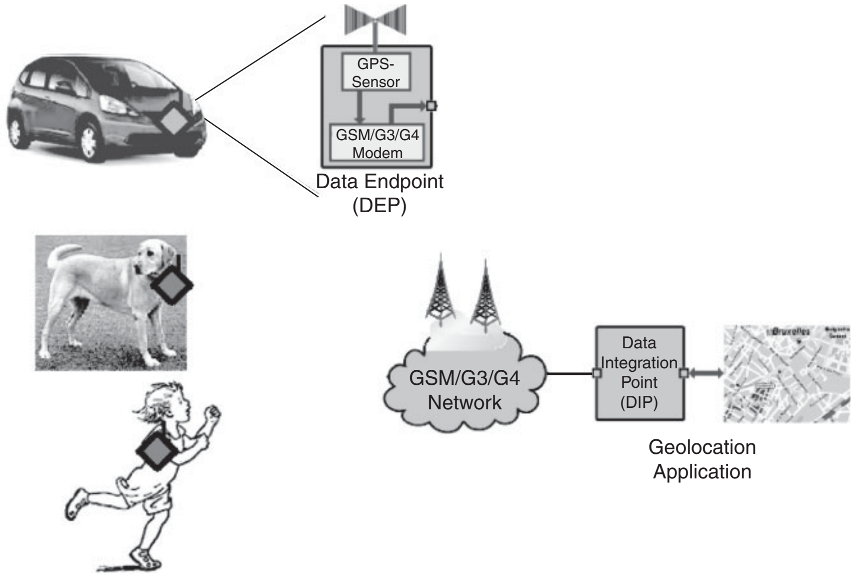

FIGURE 3.10 Geolocation/tracking application.

systems and multiple technologies with database systems that may archive a variety of pertinent background data or metadata. IOS technologies make use of both of these capabilities. Many of these applications can be seen as IoT applications, where the "things" are the sensors, the cameras, and other related instrumentation.

IOS enables the collection, aggregation, and analysis of factors in physical public view. This is not identical to the term *mass surveillance.* Mass surveillance is used to describe the pervasive surveillance of an entire (or large fraction of the) population.[6,7]

[6] *Mass surveillance* could be done, say, with wiretapping of voice and data communications, metadata collection, or with other means. We are not covering this topic because different technologies are in play compared with those used for integrated open-air surveillance: We only make passing mention of this by noting that recent surveys in about 50 countries suggest that there has been an increase in recent years in surveillance. For example, there are already mass surveillance (and open-air surveillance) in Taiwan, Thailand, the United States, Singapore, the United Kingdom, China, Malaysia and Russia, and others. In 2006, the European Union passed and adopted the Data Retention Directive (Directive 2006/24/EC), which requires telecommunication companies to retain metadata on telecommunications (e.g., who called whom, when, how often, etc.) and to keep the collected data at the disposal of governmental agencies for up to two years. Under this directive, access to the information is not required to be limited to investigation of serious crimes nor is a warrant required for access.

[7] The directive requires member states to ensure that communication providers must retain necessary data as specified in the directive

- to trace and identify the source of a communication;
- to trace and identify the destination of a communication;
- to identify the date, time, and duration of a communication;
- to identify the type of communication;

We focus in this section only on open-air surveillance and not other areas (e.g., wiretapping of voice and data communications). Open-air surveillance may be done either with or without the consent of those under surveillance; it may or may not serve their interests. The focus of this section, however, is on legitimate law enforcement applications. There are legitimate legal law enforcement uses of the technology, but also there are other uses of the technology. Considerations and issues related to possible surveillance abuse and privacy concerns are not addressed herewith, although these should not be ignored outright.[8]

As a backdrop, note that during the 1990s, the City of London, England, deployed for a security and surveillance an electronic cordon surrounding the city. The popular name of the system was and remains *Ring of Steel*. In 2005, the Ring of Steel was widened to include more businesses in the City. In 2007, New York City announced plans to install an array of cameras and roadblocks designed to detect, track, and deter terrorists; this effort is known as the *Lower Manhattan Security Initiative*, which is similar to the “Ring of Steel.” The Lower Manhattan Security Initiative aims at hardening a number of physical “high value target” areas. The New York Police Department also deployed a system to track every car, truck, or other vehicle entering Manhattan and screen it for radiation or other terror threats; this proposal is called *Operation Sentinel* and is being developed alongside the Security Initiative to tighten security throughout lower Manhattan. As of early 2013 Lower Manhattan reportedly had 3,000 publicly deployed monitoring video cameras. These cameras are integrated via a system known as Domain Awareness System, that provides data mining using artificial intelligence techniques. In the recent past, many other cities in the United States have made similar announcements. In recent years, the federal budget sought to increase the amount of money spent on surveillance technology and programs; the money is being used by state and local governments to create networks of surveillance cameras to watch over the public in the streets, shopping centers, at airports, and elsewhere (18–20). At the private level, many universities are now using camera surveillance systems, including the University of Nevada at Reno, the University of Texas at Austin, and the University of Pennsylvania (18).

Figure 3.11 depicts a generalized scenario of dispersed equipment such as video cameras, triangularization devices, and wireless sensors connected over a (multitechnology) network to a control/operations center. Connectivity services may include traditional telephone company facilities, including T1 lines, fiberoptic links, metro

- to identify the communication device;
- to identify the location of mobile communication equipment.

The data is required to be available to competent national authorities in specific cases, “for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.”

[8] There are advocates that are (strongly) opposed to the idea of surveillance. The reader may wish to consult the Electronic Privacy Information Center, Spotlight on Surveillance, http://epic.org/, and/or Privacy International, http://www.privacyinternational.org, for such advocacy.

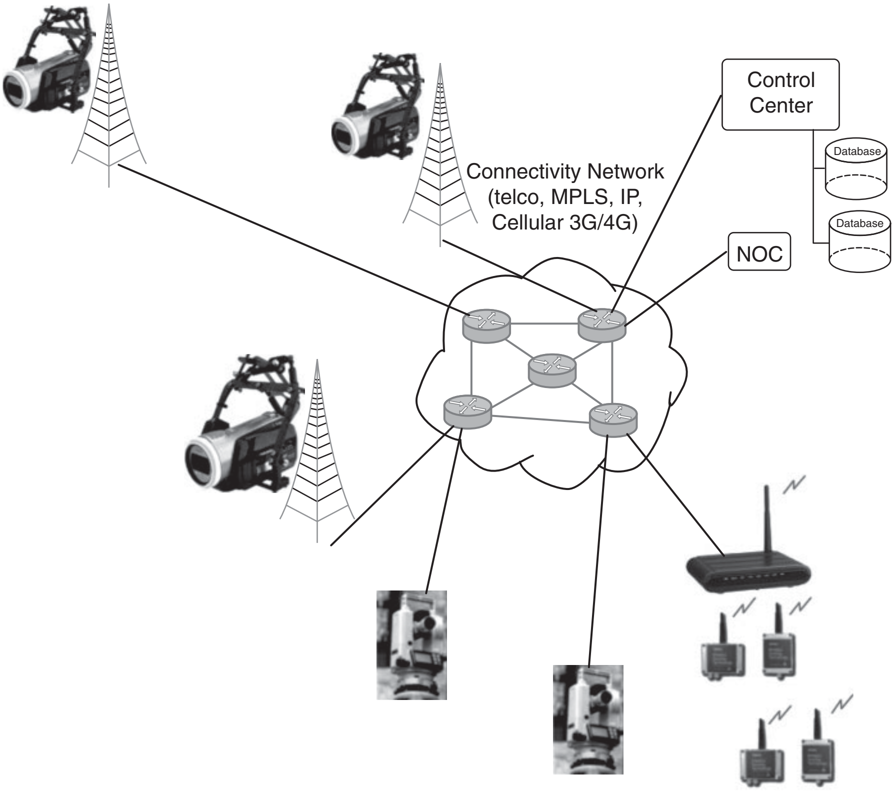

FIGURE 3.11 Generalized scenario of dispersed IOS equipment.

Ethernet services, MultiProtocol label switching, Internet services, and wireless links, including cellular 3G/4G, WiMax, WiFi links, point-to-point microwave, and other wireless technologies.

IOS' baseline objective is to create and maintain (through a combination of technologies and analysis tools) a "crime-free zone" within an urban or suburban environment by securing a perimeter both physically and electronically. At this time, cameras are found in stores, streets, parks, and intersections where police seek to ticket drivers for running red lights; cameras installed at intersections monitor every vehicle coming into the city—the cameras capture all license plate numbers.

The recent Law Enforcement success in using video imaging to identify suspects the Boston Marathon bombing will give further impetus to sustained additional deployment of IOS-based technologies in general, and video monitoring in particular, in major U.S. cities and abroad. While the data fusion and data mining will require large computational (and human) capabilities, the utility of having these data is self-evident. Face recognition technology will become widespread in the future.

Deployments of IOS-like services have seen quantifiable success in high crime areas. IOS proponents and law enforcement personnel often feel that the benefits "outweigh concern over privacy." Basic open-air surveillance is increasingly being undertaken by metropolitan (law enforcement) jurisdictions and by homeland security agencies: IOS systems are now being deployed in various forms in the United States and abroad. Cities such as Baltimore, Chicago, and New Orleans have installed camera surveillance networks with financing from the federal government; during the 2010s, many additional agencies and municipalities have deployed these IOS capabilities.

IOS functionality, however, can go beyond routine law enforcement and can provide sensor-based capabilities for toxic chemicals, explosives, and biological agents; applications include anti-terrorist detection, for example, with a chemical sensing overlay. Furthermore, with every telephone call, swipe of a card, and click of a mouse that an individual may make, information is being recorded, compiled, and stored, and this data is generally available for mining by authorities; while the latter is not exactly "open air," it is still affords a somewhat "passive" form of monitoring.

IOS approaches can be taxonomized as follows:

- Public space open-air surveillance: Methods of collecting (any type of) information about individuals when they are in any public environment (whether indoors or outdoors). Examples are people in a crowd, people in the street, cars with toll tags, and so on.
- Private space open-air surveillance: Methods of collecting (any type of) information about individuals when they are in a private environment, typically indoors. Examples are people in a doctor's office, people at work, and so on.
- Hybrid public/private space open-air surveillance: Methods of collecting (any type of) information about individuals that crosses both boundaries. Examples include using cell phones to track movements.

At the macro level, three drivers have been offered for IOS services:

- Detection/prevention of crimes
- Anti-terrorism
- Increased municipal revenue collection via remote monitoring of infractions

Recent events in Boston, Massachusetts, will further fuel sales growth in the $3.2 billion video U.S. surveillance industry, as assessed in 2013; the U.S. market was projected to grow to $4.1 billion by 2016.

Looking at the first driver, for example, some US cities have a high rate of violent crime, with 2332.6 violent crimes per 100,000 population, compared with a national average of 454.5 (2008 statistics) (21). Some claim that studies have found that surveillance systems have limited effect on crime, and that it is more effective to place more officers on the streets and improve lighting in high crime areas (18); law enforcement entities tend to take the view that services such as the IOS services described here can be very helpful. San Francisco has given license plate readers to police as well as to parking control officers, allowing them to track cars parked for too long in one spot; some cities use the cameras to assess anti-congestion tolls on motorists, while casino bosses get an alert when a high roller—or a cheater—arrives at the establishment (22).

At this juncture, the apparent goal of metropolitan (law enforcement) jurisdictions and homeland security agencies is to have a capability to support quick turnkey installations for IOS services. The deployment can be motivated and "sold" to the appropriate governmental funding agency on the idea that recurring revenue stream generated by IOS enablement (parking tickets (38), expired registration, suspended license, bail jumpers) will pay for itself in a matter of months. Most importantly, criminal activity detection coupled with rapid interdiction can result in the reduction, migration, and cessation of the same. IOS systems are being positioned by advocates for Homeland Security grant money similar to the approach used for Public Safety Interoperable Communications (PSIC) grants for state, municipal, and local jurisdictions.

As noted, the basic model for IOS is based on the concept of *Ring of Steel*. During the 1990s, the City of London, England, deployed for a security and surveillance cordon surrounding the city to deter identifiable threats; the popular name of the system was and remains *Ring of Steel*. Under this arrangement, roads entering the city are narrowed and have small chicanes to force drivers to slow down and be recorded by interconnected video cameras. A chicane is an obstacle on a racecourse or a series of tight serpentine curves in a roadway (opposite directions in an otherwise straight stretch—usually an S-shape curve), used on city streets to slow down traffic. These roads typically have a concrete median with a sentry box where police can stand guard and monitor traffic.[9] Since February 2003, the London congestion charging zone contains the *Ring of Steel* and also records all traffic on closed-circuit TV (CCTV). These measures were introduced following an IRA bombing campaign in the city; during the 1990s, the sentry posts were guarded by armed police continuously. Following the September 11, 2001, terrorist attacks, and other terrorist threats, security has been stepped up again. In 2005, the *Ring of Steel* was widened to include more businesses in the City. London had 200,000 cameras in 2005, and more than 4.3 million cameras have been deployed throughout the country. (Britain now has a fifth of the cameras in use around the world—and around 8000 speed cameras.) It is estimated that there is one camera for every 14 citizens and the typical Briton is seen by 300 cameras per day—some say the average Briton is being recorded 3,254 times a week inclusively using a variety of means (the average person living in Britain has that many pieces of personal information stored about him or her—details about shopping habits, mobile phone use, emails, locations during the day, journeys and Internet searches—most of which is kept in databases for years and in some cases indefinitely) (23).

Video surveillance is only one of several technologies and techniques used for IOS. Much of the technology needed to implement IOS is off-the-shelf; however

[9] Notwithstanding the term "Ring of Steel," the roadblocks and chicanes are actually created with concrete blocks that are wedged together.

the integration is novel. Sensor technologies can be upgraded as new and/or affordable developments emerge (e.g., EM detection of IEDs, microwave bombardment using ultra wide band (UWB) methods at stationary and moving structures, etc.). The potential enhancements to visual detection are numerous (including night vision/IR sensors, gait analysis, etc.). Constituent technologies that can be deployed in integrated open-air surveillance consist of:

- **High resolution (low light level) DVS (wired & wireless).** Cameras can be indoor/outdoor, PTZ (pan, tilt, zoom) and configured in covert or exposed modes depending upon deterrent philosophy, field conditions, and field of view considerations.
    - Outdoor cameras will be physically hardened, vandal–proof and pole, wall and surface mountable.
    - Transport media (copper, fiber, wireless) and camera power (wired, solar, battery) will depend upon physical constraints. Dozens to hundreds of cameras will be deployed in a scalable architecture.
    - Recording can be selective or under all conditions at all times for a given view.
    - These cameras can be remotely controlled by police to PTZ and rotate; have day and night vision capabilities, and wireless technologies. The cost can be as high as $60,000 per unit for some complex systems.
- **Image processing systems (at the command center)** to analyze the video streams in real time, alert law-enforcement personnel, and detect aberrant behavior (individuals walking erratically, lying prone), imagery of interest (e.g., crowd gathering, individuals running, etc.) as well as simple motion detection and if possible facial recognition of "persons of interest."
- **License plate recognition** of both parked and moving vehicles (within the field of view) at speeds up to 60 MPH moving past certain checkpoints. This can be augmented with UPC handheld scanners of registration stickers by roving patrols.
- **GDSs** using acoustic triangulation technology (pioneered with great success in Iraq to ferret out night snipers). GDS will be integrated with DVS so that after detecting gunfire, DVS will "train" on specific areas viewing in zoom for low light conditions and initiating event recording.
- **Moveable barrier technology** to inhibit selectively the movement of people and vehicle and/or people at designated checkpoints.
- **Real-time position reporting system** for vehicles, personnel, assets (VPA) using a combination of GPS, radio triangulation, and other automated vehicle locator (AVL) technologies (sign post transponders/checkpoints); personnel can be equipped with either or both active transponders/vehicles also. The tracking can start with inexpensive techniques (available from cell phone or other portable radio systems) and evolve to military-style resolution (+/−1 m).

- **Computer-aided dispatch** will direct VPA to events, targets based on predefined and/or user-defined threat categories/priorities. This can be augmented of course with AI techniques working off a predefined knowledge base.
- **GIS** will be overlaid and integrated with photogrammetry and remote sensing (PRS), as appropriate to identify building structures, natural resources, and known hazardous materials.
- **Interoperability** may be needed between different systems to extend coverage and surveillance area as well as among types of personnel (local police, state authorities, law enforcement, Office of Domestic Preparedness (ODP), and intelligence types) as well as in some cases the Feds (FEMA, FBI, DEA, ATF, etc.).
- **Traditional covert alarms** alerting personnel to events of interest.
- **Wireless sensors** for detection of toxic chemicals, explosives, and biological agents, along with sensor networking systems to support a city-wide distributed environment.

The surveillance ring provided by IOS can be tightened or loosened dynamically by enabling different regional cameras and/or “illuminating” areas of interest. Table 3.4 (based partially on Reference 23) provides a perspective on data collection, including “over-the-air” information.

Table 3.5 lists a number of recent examples to illustrate some of the approaches, issues, and perspectives; this appendix is only illustrative of some announcements in the past few years; of late, there has been an acceleration in the deployment of IOS systems across the United States, also including the use of domestic drones.

3.10 CONTROL APPLICATION EXAMPLES

Some other possible examples are discussed below, as described in Reference 5.

Controlling vending machines. Vending machines can be found in a variety of locations, for example inside office or public buildings, outdoors in public places, and gas stations. The re-stocking and maintenance of vending machines is typically done manually by staffers that visit the vending machines at regular intervals to check the re-stock levels, re-stock the machines, and perform any requisite maintenance functions. The introduction of M2M technology automates vending machine management: by having access to a (mobile) telecommunication network, the built-in M2M communication module provides information to the operator about the current status of the vending machine (e.g., current fill-levels, maintenance status, possible damages, malfunctions, and so on); as a consequence, the vending machines need only to be visited when absolutely required.

Controlling production machines. Various industrial processes make use of dispersed production devices (including but not limited to construction machines, manufacturing machines, food production machines, and so on). These machines may be exposed to harsh environments driving repair and maintenance requirements. This

TABLE 3.4 A Perspective on Data Collection

Mobile phones	Every day the average person makes three mobile phone calls and sends at least two text messages. Each time the network provider logs information about who was called as well as the caller's location and direction of travel, worked out by triangulation from phone towers. Customers can also have their locations tracked even when they are not using their phones, as the devices send out unique identifying signals at regular intervals. All of this information can be accessed by police and other public authorities investigating crimes
The Internet	Internet service providers (ISPs) compile information about their customers when they go online, including name, address, the unique identification number for the connection, known as an IP address, any browser used, and location. They also keep details of emails, such as whom they were sent to, together with the date and time they were sent. In 2008, an average of 50 websites are visited and 32 emails sent per person in Britain every day; very likely these numbers are higher today (23). Privacy campaigners have expressed concern that the country's three biggest ISPs—BT, Virgin Media, and TalkTalk—now provide this data to a digital advertising company called Phorm so that it can analyze web surfing habits. ISPs are already voluntarily providing information they hold about their customers if requested by law-enforcement agencies and public authorities. A total of 520,000 requests were made in the United Kingdom by public officials for telephone and Internet details last year, an increase from around 350,000 the previous year. Internet search engines also compile data about their users, including the IP address and what was searched for. Google receives around 68 searches from the average person each day and stores this data for 18 months. Companies such as Google and ISPs are building up huge databases of data about Internet users. These companies may be compelled, through a legal action, to hand over this information to third parties or the Government, or the companies may lose the data and it can then be misused
Loyalty cards	Store "loyalty" cards also retain large amounts of information about individuals who have signed up to use them. They link a person's personal details to the outlets used, the transaction times, and how much is spent. In the case of Nectar cards, which are used by more than 10 million people in Britain once a week, information from dozens of shops is compiled, giving a detailed picture of a cardholder's shopping habits
Banks	Banks can also be required to hand over personal account information to the authorities if requested as part of an investigation. They also provide personal data to credit reference agencies, debt collectors, and fraud prevention organizations. Debit and credit card transactions can give information about where and on what people are spending their money

(*continued*)

TABLE 3.4 (*Continued*)

CCTV	The biggest source of surveillance in Britain is through the network of CCTV (closed-circuit television) cameras. On average, an individual will appear on 300 CCTV cameras during a day and those tapes are kept by many organizations for indefinite lengths of time. On the London Underground network, Transport for London (TfL) keeps footage for a minimum of 14 days. TfL operates more than 8500 CCTV cameras in its underground stations, 1550 cameras on tube trains, and up to 60,000 cameras on buses. Britain now has more CCTV cameras in public spaces than any other country in the world. A study in 2002 estimated that there were around 4.2 million cameras, but that number is likely to now be far higher
Number plate recognition	The latest development in CCTV is the increased use of automatic number plate recognition systems, which read number plates and search databases for signs that a vehicle has been used in crime. A national automatic number plate recognition system is maintained by the Association of Chief Police Officers along motorways and main roads. Every number plate picked up by the system is stored in a database with date, time, and location for two years
Public transport and car toll cards	Travel passes such as the Oyster Card used in London and the Key card, in Oxford, can also reveal remarkable amounts of information about an individual. When they are registered to a person's name, they record journey history, dates, times, and fares. The same can be said about EasyPass (toll) cards for cars
The workplace	Employers are increasingly using radio-tagged security passes for employees, providing them with information about when staff enter and leave the office
On the street	Car-mounted video-camera passby to record pictures of the street for Google's StreetView website
Airports	Miami International Airport is one of a dozen airports in the United States that have begun pilot-testing whole-body imaging machines, which reveal weapons and explosives concealed under layers of clothing. It allows authorities to detect threat objects that are not metallic and that cannot be detected by metal detectors, and items that are sometimes missed even in a physical pat-down, in a nonintrusive manner using millimeter wave technology to create an image. This technology is being discontinued in some locations due to privacy concerns (24).

maintenance is typically done by dedicated personnel who have to visit the production machines at regular intervals to repair, perform maintenance, and identify damages or malfunction. M2M technologies improve the efficiency and optimization of the operation by allowing access to a mobile telecommunication network to forward information about the current status of the production machine (e.g., the current maintenance status, possible damages which may lead to malfunctions, and so on; additionally it is possible to transmit updates of updated software or perform remote maintenance).

TABLE 3.5 Recent Examples of IOS Systems; for Illustrative Purposes

New York City, New York	The New York Police Department is working on a plan to track every car, truck, or other vehicle entering Manhattan and screen it for radiation or other terror threats; the proposal, called *Operation Sentinel*, is being developed alongside a separate $90 million security initiative to tighten security throughout lower Manhattan in New York City. Police officials say *Operation Sentinel* would rely on license plate readers, radiation detectors, and closed-circuit cameras installed at the 16 bridges and four tunnels serving Manhattan, including the Brooklyn and George Washington bridges and the Lincoln Tunnel. About a million vehicles drive into Manhattan every day. The vehicle data—license plate numbers, radiological readings, and photos—would be automatically analyzed by computers programmed with information about suspicious vehicles. Vehicle data deemed innocent would be purged from police records after 30 days. The plan calls for 116 fixed and mobile license plate readers and 3000 closed-circuit cameras monitored by officers assigned to a command center on Broadway (this goal was reportedly achieved as of early 2013). The plan was modeled in part after the *Ring of Steel* surveillance measures in London's financial district. There is no estimate yet for the cost of *Operation Sentinel* since it was only in the planning phase at press time. The proposal has raised red flags for civil rights advocates, as one might expect (25)
Washington D.C.	For public health and safety reasons D.C. officials were planning in 2008 to give police access to more than 5260 CCTV cameras citywide that monitor traffic, schools, and public housing; this makes D.C. one of the largest surveillance networks in the country. The Video Interoperability for Public Safety (VIPS) program aims at consolidating more than 5200 cameras operated by D.C. agencies—including D.C. Public Schools and the D.C. Housing Authority—into one network managed by the city's Homeland Security and Emergency Management Agency. The program will allow agencies to share camera video feeds and provide the city with a network that is actively monitored and that will operate 24 × 365 days a year. The initiative was expected to enhance the District's counter-surveillance and public safety capabilities by increasing the number of cameras available for authorities to monitor. For example, 225 surveillance cameras in high crime neighborhoods will become available to police, and other agencies also will have access to 1388 outside cameras and 3874 cameras inside buildings throughout the city. Nearly 3500 of the cameras are operated by D.C. Public Schools. The city's transportation department operates 131 of the devices, which are normally trained on streets but can swivel (26). The Police Chief testified in 2008 that the department's cameras have resulted in a 19% reduction in violent crime within 250 feet of the devices, and a 4% violent crime reduction within 1000 feet. The District expected to spend an estimated $900,000 in recent years to operate and staff the consolidated monitoring network

(*continued*)

TABLE 3.5 (*Continued*)

	In the recent past, D.C. officials have placed cameras on light poles, police cars, and government buildings. But now, they are planning to put them on street-sweepers in the latest example of increasing surveillance of city residents. Officials will equip the District's street-sweeping machines with cameras that can scan license plates and photograph vehicles illegally parked in a street-sweeping zone. The cameras will cost approximately $40,000 each and will be placed initially on two street-sweepers. The city also operates 74 surveillance cameras affixed to light poles and buildings in neighborhoods as part of an effort to deter crime. Officials say that if 20% of motorists violate regulations against parking in blocks marked for street sweeping in a given month, the city will collect over $200,000 in additional monthly revenue
Boston	As of mid-2013 the Boston Financial District had about 250 public and private cameras and dvs to terrorist events that number is expected to increase over time.
Medina, Washington	In Medina, a new sign bears this warning: "You Are Entering a 24 Hour Video Surveillance Area." Cameras have recently been installed at intersections to monitor every vehicle coming into the city. Under the "automatic license plate recognition" project, once a car enters Medina, a camera captures its license plate number. Within seconds, the number is run through a database. If a hit comes up for a felony—say, the vehicle was reported stolen or is being driven by a homicide suspect—the information is transmitted instantaneously to police, who can "leap into action." All captured information is stored for 60 days—even if nothing negative turns up, he said. That allows police to mine data if a crime occurs later. The Police Chief has stated that "These cameras provide us with intelligence; they gets us in front of criminals." Medina had discussed the idea for years as a way to discourage crime (in 2008 there were 11 burglaries). Spokesmen for the American Civil Liberties Union of Washington argue that such a system raises the issue of privacy violations but Medina City Council members state that crime prevention "outweighs concern over privacy" (27)
Hunts Point, Washington	Hunts Point has been using a video-camera setup to record a continuous loop of car traffic in and out of town since 2006. There are eight cameras in all; pairs of cameras point in four directions. No residents have ever complained about it. The town has used it for evidence in a couple of traffic accident cases (27)
Michigan and New York Borders	The US Border Patrol is erecting 16 more video surveillance towers in Michigan and New York as part of its plans to use technology to help secure parts of the United States' 4000-mile northern border with Canada. The government awarded the $20 million project to Boeing Co., the same company responsible for the so-called virtual fence along the United States–Mexico border that has come under criticism for faulty technology. Eleven of the towers are being installed in Detroit and five in Buffalo, N.Y., to help monitor water traffic between Canada and the United States along Lake St. Clair and the Niagara River. At present, Border Patrol agents are posted along the river to keep an eye on water traffic (28)

TABLE 3.5 (*Continued*)

	Also in Michigan, the City of Flint was looking for sponsors for surveillance cameras that will be mounted around the city to keep a watch out for criminals. In exchange for cash, the city will show the business names next to police logos on the pole-mounted camera boxes that sport a blue police light that flashes 24 h a day. These systems are known as PODDS (portable overt digital surveillance system). The 14 cameras being planned cost around half-a-million dollars (29)
Illinois, Arizona, Maryland	Chicago is the US city that has made the most aggressive use of surveillance technology, has installed more than 2250 cameras in its “Homeland Security Grid,” which DHS helped finance, and began linking the devices into a single network over a 900-mile fiber-optic grid (26). The cameras are linked to an operations center constantly monitored by police officers. Additionally, the State of Illinois has reportedly considered installing speed cameras in each direction of every interstate in the 20 State Police districts across the state to raise $50 million a year in revenue. Currently, camera-equipped vans nab speeders in construction zones, but state law does not allow speed cameras on interstates. As of 2013 Chicago authorities had access to our 10,000 public and private video surveillance cameras. Also, Cicero, Ill., was planning to install several surveillance cameras with a grant from Homeland Security In Arizona, 100 speed cameras were planned to be deployed on highways at a cost of about $20 million. The state was planning to raise $90 million a year by imposing $165 fines on vehicles going 10 mph over the speed limit Baltimore has used federal grants to finance its camera system and a “Watch Center.” The cameras are connected to the state’s existing highway monitoring cameras, and the plan is for five counties in Maryland—Anne Arundel, Baltimore, Carroll, Hartford, and Howard—to connect with the city’s surveillance system
Florida	A surveillance video program is being implemented in Orlando called Innovative Response to Improve Safety (IRIS) aimed at detecting crimes or other incidents and send alerts to law enforcement. High-tech cameras similar to those used in London will be installed in busy sections of Orlando to help curb crime. The IRIS cams are also known as “intelligent cameras.” The first 18 of 60 motion-detecting cameras installed around Orlando will cost about $1.3 million. Orlando is one of the first US cities in the nation to get the high-tech cameras that provide real-time data enabling the police to send officers as soon as they see some activity and we send officers to that activity in a “hot zone”—the legacy technology that is in stores employs offline recording (typically for evidence for future use, for future follow-up, and future investigative purposes); these systems do all that, but also allow real-time video collection (30) As of 2013 Orlando police had 138 cameras scattered throughout the city with more on the way. Police stated that in 2012 the cameras were used in nearly 800 criminal investigations, leading to more than 100 arrests.

(*continued*)

TABLE 3.5 (*Continued*)

	The Miami Police Department could soon be the first in the United States to use cutting-edge, spy-in-the-sky technology to beef up their fight against crime. A small pilotless drone manufactured by Honeywell International, capable of hovering and "staring" using electro-optic or infrared sensors, is expected to make its debut soon in the skies over the Florida Everglades. If use of the drone wins Federal Aviation Administration approval after tests, the Miami-Dade Police Department will start flying the 14-pound (6.3 kg) drone over urban areas with an eye toward full-fledged employment in crime fighting. It is intended to be used in tactical situations as an extra set of eyes. The wingless Honeywell aircraft fits into a backpack and is capable of vertical takeoff and landing. Government agencies acknowledge the development of a dragonfly-sized unmanned aerial vehicle (UAV) known as the "Insectohopter" for laser-guided spy operations as long ago as the 1970s. There is reportedly strong interest from law-enforcement agencies in getting UAVs up and running and smaller aircrafts are possibly having a "huge economic impact" over the next 10 years (31). (Reportedly there are around 100 different designs of flying drones currently in use by the US Government.)
Other localities	Tiburon, a town that juts into San Francisco Bay, is planning to use cameras to record the license plate number of every vehicle that crosses city limits. Some residents describe the plan as a commonsense way to thwart thieves, most of whom come from out of town. The readers, which use character recognition software, can compare plates to databases of cars that have been stolen or linked to crimes, then immediately notify police of matches. The project has an expected price tag of $100,000. Once the street cameras are installed, hunting a burglary suspect could be easier: officials will look for a plate that came and went and detectives could then check to see if any of the cars has been linked with crimes in the past. Information on which cars enter and leave town will be erased within 60 days and police officers will be granted access to the information only during an investigation. License plate readers have exploded in popularity in recent years, but Tiburon would be one of the first to mount them at fixed locations—and perhaps the very first to record exhaustively *every* car coming or going. California Highway Patrol (CHP) officials have put the readers on 18 cruisers and at four fixed locations. CHP officers have seen an increase in recoveries of stolen cars since the devices were installed, starting in August 2005. Through December 2008, CHP had used the devices to recover 1739 cars and arrest 675 people (22) In New Orleans, digital camera images are sent to a main server archive for monitoring, and the Internet-based archive can be accessed from any location, including police vehicles. Paramus, N.J., is launching a pilot camera surveillance system at shopping malls that will be partially financed by federal grants. A federal grant was expected to help Newport, R.I. pay for the installation of surveillance cameras. St. Bernard Parish, La., has used federal funds for surveillance cameras

TABLE 3.5 (*Continued*)

England	Local newspapers read: “Now snooping on the public has reached new heights with local authorities putting spy planes in the air to snoop on homeowners who are wasting too much energy” (32). Thermal imaging cameras are being used to create color-coded maps that will enable council officers to identify offenders. The aircraft takes images of homes and businesses, with those losing the most heat showing up as red, while better insulated properties appear blue. The City Council has spent £30,000 using a plane carrying a thermal camera to determine which homes are wasting energy. A scheme is already underway in Broadland District Council in Norfolk, which has spent £30,000 hiring a plane with a thermal imaging camera. The exercise has been so successful that other local authorities are planning to follow suit. In England, police could soon use unmanned spyplanes like those used to track enemy troops in Iraq and Afghanistan for surveillance operations on British homes. Plans to introduce the UAVs are outlined in the Home Office’s Science and Innovation Strategy. The Home Office has suggested that the remote-controlled drones could be used to help police gather evidence and track criminals without putting officers at risk. The miniature aircraft could be fitted with cameras and heat-seeking equipment, allowing police to carry out aerial reconnaissance from a control room. They also have the benefit of being quieter than conventional helicopters or spotter planes and are much cheaper to run due to their fuel economy. Home Office’s Science and Innovation Strategy states that “UAVs are likely to become an increasingly useful tool for police in the future, potentially reducing the number of dangerous situations the police may have to enter and also providing evidence for prosecutions and support police operations in real time” (33) In one week, the average person living in Britain has 3254 pieces of personal information stored about him or her, most of which is kept in databases for years and in some cases indefinitely. The data include details about shopping habits, mobile phone use, emails, locations during the day, journeys, and Internet searches. In many cases, this information is kept by companies such as banks and shops, but in certain circumstances they can be asked to hand it over to a range of legal authorities. The U.K. Government has published plans to grant local authorities and other public bodies access to the email and Internet records of millions. Phone companies already retain data about their customers and (in the United Kingdom, for example) give it to 650 public bodies on request

3.11 MYRIAD OTHER APPLICATIONS

Many other examples of IoT applications can be cited and many more will evolve in the future. For example, M2M and SCADA applications are now also being extended to support over satellite links. Satellite service providers perceive M2M communications as an approach the global demand for uninterrupted and seamless data connectivity across a mixture of urban, suburban, exurban, rural, and oceanic environments: satellite-based M2M can facilitate the delivery of small quantities of information to and from anywhere in the world. Applications include civil government, environmental monitoring and climate analysis, police and coast guard, off-shore oil drilling, and mining. Observers are noticing an increased demand for satellite services from several companies associated with finance, energy, and maritime industries. Although at press time, satellite-based services were only a small share of the M2M market which is largely dominated by cellular systems (around 2% in terms of volume and 6% of revenue in 2011), M2M is a growing segment for the satellite industry: forecasts say the global satellite M2M market will reach 2.3 billion EUR by 2016. The region with the highest rate of progress will be the Asia-Pacific with developments in countries such as China, Indonesia, Vietnam, and India (34). Proponents make the case that “M2M market represents an interesting and potentially huge revenue stream for the satellite industry with opportunities in many markets, particularly vertical ones.” (35).

As another application, Bank of America Corp has been testing a technology that allows a customer to pay at a store register by simply scanning an image with a smartphone, such as Apple Inc’s iPhone or Google Inc’s Android devices. This is similar but not identical to the SC concept described earlier in the chapter. Companies such as, but not limited to, Google and eBay Inc’s PayPal are investigating ways to turn phones into digital wallets that house credit and debit cards, coupons and store loyalty program details. The market for global mobile payments was over $170 billion at press time. Initially Bank of America experimented with NFC technology, in which a chip installed in a phone transmits a radio signal when it is waved or tapped at a device at the cash register; newer approaches entail the use of iPhones and phones that implement the Android operating system (iPhone 5 does not embed NFC chips). In the bank’s NFC trials, customers stored their payment information digitally in a secure area on their phone and then paid at a merchant who kept a device to read the signal from the phone (36). In the latest test, customers store their payment cards on a computer server and when they pay, they use an application on their phone that scans a Quick Response code displayed at the register.

REFERENCES

1. Lee GM, Park J, Kong N, Crespi N. The Internet of Things – Concept and Problem Statement. July 2011. Internet Research Task Force, July 11, 2011, draft-lee-iot-problem-statement-02.txt.
2. Scarrone E, Boswarthick D. Overview of ETSI TC M2M Activities, March 2012, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.
3. 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Service Requirements for Machine Type Communications (MTC); Stage 1 (Release 10); Technical Specification 3GPP TS 22.368 V10.1.0 (2010–06).

4. African Utility Week Conference: 22–23 May 2012, Nasrec Expo Centre, Johannesburg. Available at www.african-utility-week.com.
5. Machine-to-Machine communications (M2M); M2M Service Requirements. ETSI TS 102 689 V1.1.1 (2010–08). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.
6. Drake J, Najewicz D, Watts W. Energy Efficiency Comparisons of Wireless Communication Technology Options for Smart Grid Enabled Devices. White Paper, General Electric Company, GE Appliances & Lighting, December 9, 2010.
7. ETSI TR 102 732: Machine to Machine Communications (M2M); Use Cases of M2M Applications for eHealth. (2011–03). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.
8. ETSI TR 101 557 V1.1.1 (2012–02), Electromagnetic Compatibility and Radio Spectrum Matters (ERM); System Reference document (SRdoc); Medical Body Area Network Systems (MBANSs) in the 1785 MHz to 2500 MHz range.
9. Staff. FCC Chairman Unveils Proposal to Spur Innovation in Medical Body Area Networks, to Transform Patient Care, and Lower Health Care Costs. May 17, 2012, Federal Communications Commission, 445 12th Street SW, Washington, DC 20554.
10. ZigBee Wireless Sensor Applications for Health, Wellness and Fitness, March 2009, ZigBee Alliance. Available at www.zigbee.org.
11. Staff. Smart Cards, Mobile Telephony and M2M at the Heart of e-health Services. CARTES & IDentification Conference, Parc des Expositions Paris-Nord Villepinte, November, 2011.
12. ETSI TR 102 897: Machine to Machine Communications (M2M); Use Cases of M2M Applications for City Automation. (2010-01). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.
13. ETSI TR 102 898: Machine to Machine Communications (M2M); Use Cases of Automotive Applications in M2M Capable Networks. (2010-09). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.
14. Smart Card Alliance. Contactless Technology for Secure Physical Access: Technology and Standards Choices. Smart Card Alliance Report, October 2002, Publication Number: ID-02002, Princeton Junction, New Jersey.
15. Hancke G. A Practical Relay Attack on ISO 14443 Proximity Cards. White Paper, July 2008, University of Cambridge, Computer Laboratory JJ Thomson Avenue, Cambridge, CB3 0FD, UK.
16. Promotional Material of NearFieldCommunication.org. Available at www.nearfield communication.org.
17. ETSI TS 102 412: Smart Cards; Smart Card Platform Requirements Stage 1 (Release 8). (2007-07). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.
18. Electronic Privacy Information Center, Spotlight on Surveillance, More Cities Deploy Camera Surveillance Systems with Federal Grant Money, May 2005, Washington, D.C. Available at http://epic.org/.
19. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2006,* at 81-82 (Feb. 7, 2005).Available at http://www.epic.org/privacy/surveillance/spotlight/0505/dhsb06.pdf.
20. Rotenberg M, Laurant C. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*, EPIC and Privacy International 2004 (EPIC 2004).
21. O'Leary-Morgan K, Morgan S, Boba R, editors, *City Crime Rankings 2009—2010*. Washington, DC: CQ Press, A Division of SAGE; November 23, 2009.

22. Bulwa D. *Tiburon May Install License Plate Cameras*. San Francisco Chronicle; July 10, 2009.
23. Gray R. How big brother watches your every move. The Sunday Telegraph, 16 Aug 2008.
24. Cordle IP. Miami Airport Security Cameras see Through Clothing. Miami Herald, July 22, 2008.
25. AP/Crain's New York, NYPD Planning to Track Every Vehicle in Manhattan. August 18, 2008.
26. Washington Times. D.C. Police Set to Monitor 5,000 Cameras. April 9, 2008.
27. Krishnan S. Cameras Keep Track of all Cars Entering Medina. Seattle Times, September 16, 2009.
28. Sullivan E. Surveillance Towers Planned for Detroit, Buffalo, AP, March 31, 2009.
29. Foren J. Flint seeks sponsors for police surveillance cameras. Flint Journal, July 30, 2008.
30. Local6.com. Orlando Surveillance Cams Will Detect Motion, Alert In Real-Time. June 23, 2008.
31. Brown T. Spy-in-the-sky Drone Sets Sights on Miami. Reuters, March 26, 2008.
32. Levy A. Council Uses Spy Plane with Thermal Imaging Camera to Snoop on Homes Wasting Energy. Daily Mail, 24th March 2009.
33. Wardrop M. Remote-controlled Planes Could Spy on British Homes. The Sunday Telegraph, 24 Feb 2009.
34. IDATE. The Satellite M2M Market 2012–2016. Report, IDATE Consulting & Research, April 23, 2012, London, UK.
35. Staff. Satellite M2M: An Emerging Revenue Stream, September/October 2010. Available at www.satellite-evolution.com.
36. Rothacker R. Bank of America Tests Technology to Pay with Phones. Reuters, October 1, 2012.
37. Jung N-J, Yang I-K, Park S-W, Lee S-Y. "A design of AMI protocols for two way communication in K-AMI", Control, Automation and Systems (ICCAS), Conference Proceedings 2011 11th international Conference on, Date of Conference: 26-29 Oct. 2011, S/W Center, KEPCO Res. Inst., Daejeon, South Korea, Page(s): 1011–1016.
38. Washington Times. Street-sweeper Cameras Eye Illegal Parking. April 2, 2008.
39. Kingsley S, "Personal body networks go wireless at 2.4GHZ", ElectronicsWeekly Online Magazine, 16 May 2012, http://www.electronicsweekly.com.