Chapter 3

Four Pillars of IoT

3.1 The Horizontal, Verticals, and Four Pillars

Applications of the Internet of Things (IoT) have spread across an enormously large number of industry sectors, and some technologies have been used for decades as described in the previous chapter. The development of the vertical applications in these sectors is unbalanced. It is very important to sort out those vertical applications and identify common underpinning technologies that can be used across the board, so that interconnecting, interrelating, and synergized grand integration and new creative, disruptive applications can be achieved.

One of the common characteristics of the Internet of Things is that objects in a IoT world have to be instrumented (step 3 in Figure 3.1), interconnected (steps 2 and 1), before anything can be intelligently processed and used anywhere, anytime, anyway, and anyhow (steps 1 and 2), which are the 5A and 3I [180] characteristics.

Another common feature that IoT brought to information and communications technology (ICT) systems is a fundamental change in the way information is generated, from

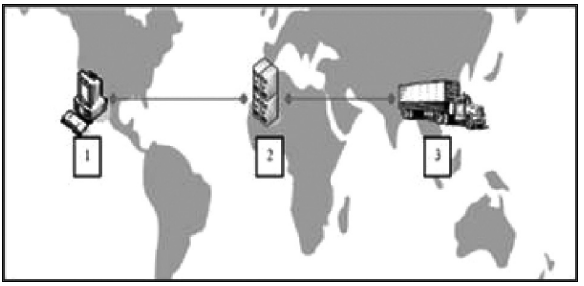

Figure 3.1 3I and 5A.

mostly manual input to massively machine-generated without human intervention.

To achieve such 5A (anything, anywhere, anytime, anyway, anyhow) and 3I (instrumented, interconnected, and intelligent) capabilities, some common, horizontal, general-purpose technologies, standards, and platforms, especially middleware platforms based on common data representations just like the three-tiered application server middleware, HTML language, and HTTP protocol in the Internet/web arena, have to be established to support various vertical applications cost effectively, and new applications can be added to the platform unlimitedly.

Most of the vertical applications of IoT utilize common technologies from the networking level and middleware platform to the application level, such as standard wired and wireless networks, DBMS, security framework, web-based three-tiered middleware, multitenant PaaS (platform as a service), SOA (service-oriented architecture) interfaces, and so on. Those common technologies can be consolidated into a general-purpose, scalable framework and platform to better serve the vertical applications as demonstrated in [202].

Service-management platforms (SMPs) are the key to entry into the machine-to-machine (M2M) market. They allow for the essential connectivity management, intelligent rate-plan management, and customer self-service capability that are today's fundamental prerequisites for providing a successful, managed M2M service. Consequently, with its acquisition of

Telenor Connexion's M2M SMP technology and the staff related to the platform's development, Ericsson has taken a decisive step into the market. Ericsson has built a horizontal platform for the 50 billion M2M market's vertical telematics, medical, utilities, and government applications [203].

Telenor Objects was formed in July 2009 by researchers and developers in Telenor Norway and Telenor R&I. The two entities had individually been working on piloting managed M2M services since 2007, with an RFID (radio-frequency identification) focus in Telenor Norway, and a focus on trace-and-track initiatives in Telenor R&I. Telenor Objects [104] aims to provide a layered and horizontal architecture for connecting devices and applications. The company's platform, dubbed Shepherd, adheres to ETSI's standardization initiative on connected objects and provides a device library as well as a set of enablers to device and application providers. In addition, Shepherd includes a range of operational management services.

As a driver for connecting devices to the Internet of Things, Telenor Objects is a founding member of coosproject.org (Connected Objects Operating System), a general-purpose, modular, pluggable, and distributable open source middleware platform in Java, designed for connecting service and device objects that communicate via messages and enabling monitoring and management. (The targeting devices totaled 2.675 trillion according to Telenor Objects and Harbor Research's Intelligent Device Hierarchy at http://www.harborresearch.com/_literature_32606/News.htm.) The initiative is among several newly established steps by Telenor into the open source and open innovation sphere.

The key benefits of horizontal standard-based platforms will be faster and less costly application development and more highly functional, robust, and secure applications. Similar to the market benefit of third-party apps (e.g., Apple's application store) running on smartphone platforms, M2M applications developed on horizontal [183] platforms will be able to make easier use of underlying technologies and

services. Application developers will not have to pull together the entire value chain or have expertise in esoteric skill sets. This will dramatically increase the rate of innovation in the industry in addition to creating more cross-linkages between various M2M applications.

In an issue of the M2M (now *Connected World*) magazine's cover story in 2007 [50], editorial director Peggy Smedley introduced a graphic that encapsulates the ever-expanding M2M landscape. The graphic covers the "six pillars" of M2M technology, representing market segments that involve networking physical assets and integrating machine data into business systems. The six pillars of M2M are as follows:

1. Remote monitoring is a generic term most often representing supervisory control, data acquisition, and automation of industrial assets.
2. RFID is a data-collection technology that uses electronic tags for storing data.
3. A sensor network monitors physical or environmental conditions, with sensor nodes acting cooperatively to form/maintain the network.
4. The term *smart service* refers to the process of networking equipment and monitoring it at a customer's site so that it can be maintained and serviced more effectively.
5. Telematics is the integration of telecommunications and informatics, but most often it refers to tracking, navigation, and entertainment applications in vehicles.
6. Telemetry [185] is usually associated with industrial-, medical-, and wildlife-tracking applications that transmit small amounts of wireless data.

However, there is plenty of overlap among the pillars in this graphic. Pick any application of M2M and chances are it fits into more than one of the six pillars. Take fleet management as an example. It is certainly remote monitoring. It can be considered a smart service depending on who's doing the

monitoring. It may have elements of telematics. It fits the technical definition of telemetry. And, there may even be RFID tags or a sensor network onboard.

In this book, a four-pillar graphic is introduced for the broader IoT universe. The four pillars of IoT are M2M, RFID, WSNs (wireless sensor networks), and SCADA (supervisory control and data acquisition):

- M2M uses devices (such as an in-vehicle gadget) to capture events (such as an engine disorder), via a network (mostly cellular wireless networks, sometimes wired or hybrid) connection to a central server (software program), that translates the captured events into meaningful information (alert failure to be fixed).
- RFID uses radio waves to transfer data from an electronic tag attached to an object to a central system through a reader for the purpose of identifying and tracking the object.
- A WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, pressure, motion, or pollutants, and to cooperatively pass their data through the network, mostly short-range wireless mesh networks, sometimes wired or hybrid, to a main location. (Methley et al. [62] reports on the overlaps or coverage differences when WSN was compared with M2M and RFID; SCADA or smart system was not mentioned in the report.)
- SCADA is an autonomous system based on closed-loop control theory or a smart system or a CPS that connects, monitors, and controls equipment via the network (mostly wired short-range networks, a.k.a., field buses, sometimes wireless or hybrid) in a facility such as a plant or a building.

The term *SCADA* was picked as one of the pillars of IoT over the terms *smart system* and *CPS.* CPS [28] is more of an academic term, and EPoSS defines *smart system* as "miniaturized devices that incorporate functions of sensing, actuation, and

control" [22]. Both of these can be considered parts of the extended scope of SCADA or ICS (industrial control system) under the IoT umbrella.

Smart systems evolved from microsystems. They combine technologies and components from microsystems (miniaturized electric, mechanical, optical, and fluid devices) with knowledge, technology, and functionality from disciplines like biology, chemistry, nano sciences, and cognitive sciences.

However, Harbor Research [32] defines smart systems as a new generation of systems architecture (hardware, software, network technologies, and managed services) that provides real-time awareness based on inputs from machines, people, video streams, maps, news feeds, sensors, and more that integrate people, processes, and knowledge to enable collective awareness and decision making. Based on this definition, a smart system is close to an industrial automation system, a facility management system, or a building management system.

Harbor Research's definition is close to what a SCADA system covers. Due to the difference of the definitions of Harbor and EPoSS, SCADA is chosen as one of the four pillars.

There is much less overlap between these four pillars compared with those of the six-pillar categorizations of M2M. The clear categories of the four pillars and the distinct networking technologies are shown in Table 3.1 and Figure 3.2.

Table 3.1 Four Pillars of IoT and Their Relevance to Networks

Four Pillars and Networks	*Short-Range Wireless*	*Long-Range Wireless*	*Short-Range Wired*	*Long-Range Wired*
RFID	Yes	Some	No	Some
WSN	Yes	Some	No	Some
M2M	Some	Yes	No	Some
SCADA	Some	Some	Yes	Yes

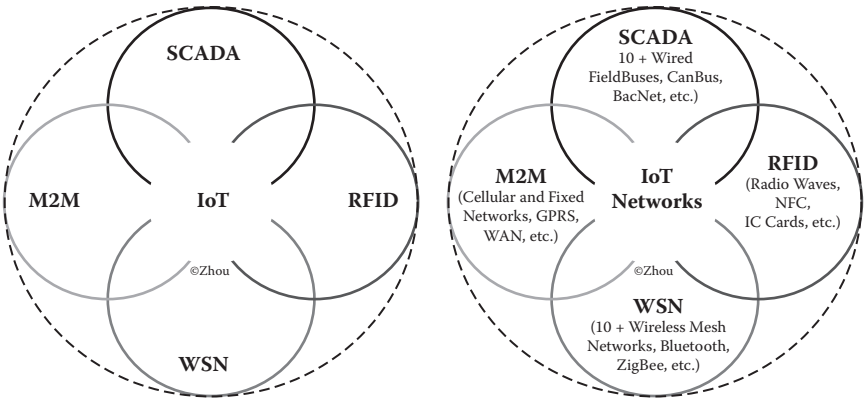

Figure 3.2 The four pillars of IoT paradigms and related networks.

The Strategy Analytics research firm also categorized the IoT networks as wired (stationary) and wireless (mobile), and compared their market value and ease of integration as early as 2004 [204].

IoT is the glue that fastens the four pillars through a common set of best practices, networking methodology, and middleware platform. This enables the user to connect all of their physical assets with a common infrastructure and a consistent methodology for gathering machine data and figuring out what it means. Take away the glue, and end users are left with multiple application platforms and network accounts. The true power of the Internet of Things occurs when it is working behind the scenes (just like Mark Weiser said about ubiquitous computing) and sharing a common platform, which can't happen if companies have to manage multiple, independent systems.

3.2 M2M: The Internet of Devices

Although the rest of the world may not agree, in the United States, *machine-to-machine* is a more popular term than the *Internet of Things*, thanks perhaps to *M2M Magazine*'s efforts since 2004. Two of the six pillars, remote monitoring

and smart service, are features or functions of an IoT system rather than pillars. Conceptually, the terms M2M, RFID, and WSN are similar, but when the underlying communication network is taken into consideration, they are quite different segments.

In this book, the term M2M is restricted to refer to device connectivity technologies, products, and services relevant to the cellular wireless networks operated by telco companies. In fact, most of the M2M market research reports assume M2M modules are simply just cellular modules. Table 3.2 showcases the major applications. However, there is overlap between M2M and the consumer electronics applications. The consumer electronics offerings include the following (as opposite to the traditional M2M offerings shown in Table 3.2):

- Personal navigation devices
- eReaders
- Digital picture frames
- People-tracking devices
- Pet-tracking devices
- Home security monitors
- Personal medical devices

ABI Research forecasts that the M2M market is expected to reach more than 85 million connections globally by 2012, and more than 200 million by 2014, with a total market valuation of approximately $57 billion, with utilities (automatic meter reading, telemetry) and automotive (telematics) the clear winners. In fact, it has been assumed that M2M comprises telematics and telemetry [42]. However, Analysys Mason predicts telemetry (utilities, etc.) will outperform telematics in the long run [205].

iSuppli's research depicts the worldwide cellular M2M module market by vertical applications in millions of dollars and the market shares of major vendors [206]. Juniper Research

Table 3.2 Application Areas for Cellular M2M

Industry	*Example Application*	*Benefits*
Medical	Wireless medical device	Remote patient monitoring
Security	Home alarm and surveillance	Real-time remote security and surveillance
Utility	Smart metering	Energy, water, and gas conservation
Manufacturing	Industrial automation	Productivity and cost savings
Automotive	Tracking vehicles	Security against theft
Transport	Traffic systems	Traffic control for efficiency
Advertising and public messaging	Billboard	Remote management of advertising displays
Kiosk	Vending	Remote machine management for efficiency and cost savings
Telematics	Fleet management	Efficiency and cost savings
Payment systems	Mobile transaction terminals	Mobile vending and efficiency
Industrial automation	Over-the-air diagnosis and upgrades	Remote device management for time savings and reduced costs

estimates there will be approximately 412 million M2M mobile connected devices in the marketplace by 2014 [207].

The number of cellular M2M devices surpassed the number of mobile phones for the first time in Europe in 2010, just a few months later than the time predicted by e-Principles in 2003.

According to Beecham Research in August 2011, Cisco recently announced dedicated routers for the M2M market, stating that it believes M2M will become an important mass market. This is just the latest announcement of a series of recent initiatives in the M2M market, both in the United States and in Europe.

In April 2011, Ericsson announced the acquisition of longtime M2M platform provider Telenor Connexion, while in July TeliaSonera announced that it had signed a cooperation agreement with France Telecom-Orange and Deutsche Telekom to increase the quality of service and interoperability for M2M services. In May 2011, T-Mobile USA announced that it had cast off its M2M operational business to longtime service partner Raco Wireless, although in July T-Mobile USA struck a partnership with asset protection provider IContain and Asset Protection Products LLC to help reduce operating costs of $7 billion in the US rent-to-own (RTO) sector.

Those and other initiatives signal that the M2M market is deemed ready to truly become a mass market, and players from hardware providers to M2M specialists passing through telco operators and sytem integrators [208] are trying to position themselves to reap the benefits.

While the executive-level comments and business unit launches from AT&T and Verizon signal a highly promising vision for the future, the reality of the M2M market is different and less optimistic as seen by other analysts such as Berg Insights. A comparison of analyst projections for the M2M market points to a market of about 100 million unit shipments for 2012 [38]. Strategy Analytics identifies five key barriers to scaling the global M2M market [275]:

1. Lack of a low-cost local access media that can be implemented on a global basis
2. The fragmented nature of both the technology vendors and the solutions they provide

3. Lack of any single killer application that can consolidate the market and drive demand forward
4. The increased costs associated with development and integration because of the complex nature of M2M solutions
5. Management's inability to express the benefits of M2M in anything other than cost savings, rather than exploiting and encouraging the service enablement capacity of mobile M2M

Figure 3.3 shows the typical architecture of an M2M system from BiTX. The integration middleware at the server side is the brain of the entire system.

Cellular networks were designed for circuit-switched voice. While they do a perfectly adequate job for regular, packet-switched data such as email and web browsing, they do not have the requisite functionality for M2M applications. For example, the normal OSS (operation support system) and BSS (business support system) are not designed for low-cost, mass handling of huge amounts of similar subscriptions. That led to the development of service enablement middleware platforms by specialized service providers (Table 3.3).

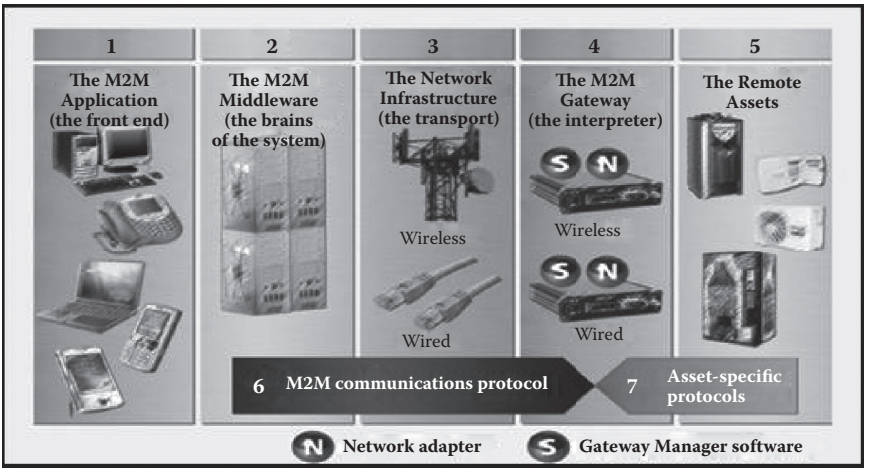

Figure 3.3 BiTX M2M architecture based on middleware.

Table 3.3 M2M Service Enablement Middleware

Vertical Applications Applications to connect to and communicate with objects tailored for specific verticals. Must be done in partnership with industry.
Service Enablement Middleware (APIs over Internet) Reduce complexities with regard to fragmented connectivity, device standards, application information protocols, etc., and device management. Build on and extend connectivity.
Connectivity (ADSL, SMS, USSD, GSM, GPRS, UMTS, HSPA, WiFi, Satellite, Zigbee, RFID, Bluetooth, etc.) Connectivity tailored for object communication with regards to business model, service level, SIM provisioning, billing, etc.

Service enablement is a middleware layer that facilitates the creation of applications. You can think of it as an operating system that the software developers write to this layer via application programming interface (APIs). A significant percentage of the functionality of the middleware comes from the charging, mediation, service management, and network management solutions that are being deployed in next-generation networks. These components have functionality that is similar and in some ways superior to that of regular M2M middleware platforms.

Table 3.4 shows the value chain of M2M business, which can be separated into two parts: the first relating to devices and the second to application development and service delivery. The broad intersection between these two parts represents the means by which devices are procured and integrated into M2M solutions and services. Both MNOs (mobile network operators), with some operators taking a more active role than others, and MVNOs (mobile virtual network operators, as shown in the table), subject to having their devices certified on a host operator's network, are trying to be M2M service providers.

The M2M device market share of chipset vendors including TI, Infineon, ST-Ericsson, Qualcomm, and others, and module

Table 3.4 Operator's Participation in Value Chain

Type of Entity / *Activity in Value Chain*	*Mobile Network Operator*	*Mobile Network Enabler*	*Mobile Virtual Network Enabler*	*Mobile Virtual Network Operator*	*Branded Reseller*	*Service Provider*
Mobile License	X	X				
Mobile Infrastructure	X	X				
Direct Customer Relationship	X			X	X	X
Network Routing	X	X	X	X		
Roaming Agreements	X	X	X	X		
Customer Services Delivery	X	X	X	X		X
Billing	X	X	X	X		X
Mobile Handset Management	X	X	X	X		X

vendors including Enfora, Infone, Kyocera, Murata, Mobicom, Novatel, Panasonic, Semco, Siemens, Sierra Cellular, Simcom, Telit, Wavecom, and others, can be found in [209].

As MNOs become more directly involved with M2M application service providers (ASPs), some MNOs such as Sprint, AT&T, Verizon Wireless, China Mobile, China Telecom, China Unicom, Orange, Rogers Communications, Telenor, Telefonica, NTT DOCOMO, and others are actively deploying M2M-based services. Many are deploying key network elements, specifically mobile packet gateways (e.g., Gateway GPRS Support Node [GGSN], Packet Data Serving Node [PDSN], Home Location Register [HLR], etc.), specifically for their M2M operations, separate from their general mobile data infrastructure. Key benefits of doing this are that it simplifies internal business operations and optimizes use of the network.

Likewise, MVNOs active in the M2M market are also increasingly deploying mobile packet gateways and similar equipment to interconnect with their MNO partners' radio infrastructure. (ABI Research classifies MVNOs who have deployed HLRs and mobile packet gateways as "MMOs" [52]; i.e., M2M Mobile Operators, Aeris Communications, Jasper Wireless, Numerex, Kore Telematics, Wyless, Qualcomm nPhase, Wireless Maingate, etc., are examples of MMOs.) The benefits to the MVNO for doing this include the ability to create new service offerings independently of their MNO partners and to enable quicker provisioning and diagnostic capabilities to their ASP customers.

MMOs and ASPs are called M2M partners of MNOs. They could use only the connectivity services of an MNO or other services such as rating and charging. Amazon eReaders, M2M DataSmart, FleetMatics, TeloGis, and others are examples of ASPs. Jasper Wireless is an example that uses less services of MNOs in some applications, because it's also an MMO.

As more and more MNOs start to enter into the M2M market directly, such as Telenor Objects, etc., some ASPs and MMOs are forced to become mobile virtual network enablers

(MVNEs), that is, MNO or MVNO enablers for M2M. For example, Jasper Wireless is an MVNE of some of AT&T's M2M businesses.

There is virtually no MVNO in existence in China because there is no regulation allowing such a business or service; the Big Three state-owned telcos, China Mobile, China Unicom, and China Telecom, dominate the market. Based on the flagship product ^{ez}M2M Middleware Platform for IoT applications, built at THTF Co., Ltd. (the second largest system integrator of China) led by the author, THTF has successful established a joint venture with China Mobile to construct the M2M Platform for China Mobile's M2M/IoT base in ChongQing serving nationwide users for all vertical applications.

3.3 RFID: The Internet of Objects

The term *Internet of Things* was first used by Kevin Ashton, co-founder and executive director of the Auto-ID Center, when he was doing RFID-related research at Massachusetts Institute of Technology in 1999. The Auto-ID lab is a research federation in the field of networked RFID and emerging sensing technologies, consisting of seven research universities located on four different continents chosen by the former Auto-ID Center to design the architecture for the Internet of Things together with EPCglobal. The technology they have developed is at the heart of a proposal sponsored by EPCglobal and supported by GS1, GS1 US, Walmart, Hewlett-Packard, and others to use RFID and the electronic product code (EPC) in the identification of items in the supply chain for companies.

An RFID tag is a simplified, low-cost, disposable contactless smartcard. RFID tags include a chip that stores a static number (ID) and attributes of the tagged object and an antenna that enables the chip to transmit the store number to a reader. When the tag comes within the range of the appropriate RF reader, the tag is powered by the reader's RF

Figure 3.4 RFID system components. (From Erick C. Jones and Christopher A. Chung, *RFID in Logistics: A Practical Introduction,* Boca Raton, FL: CRC Press, 2008.)

field and transmits its ID and attributes to the reader. The contactless smartcard provides similar capabilities but stores more data.

An RFID system involves hardware known as readers and tags, as well as RFID software or RFID middleware (Figure 3.4). RFID tags can be active, passive, or semipassive. Passive RFID does not use a battery, while an active has an on-board battery that always broadcasts its signal. A semipassive RFID has a small battery on board that is activated when in the presence of a RFID reader.

The RFID technology is different from the other three technologies of IoT in the sense that it tags on an "unintelligent" object such as a pallet or an animal (an early experiment with RFID implants was conducted by British professor of cybernetics Kevin Warwick, who implanted a chip in his arm in 1998) to make it an instrumented [180] intelligent object for monitoring and tracking, while the other three (M2M, WSN, and Smart Systems) simply connect "intelligent" electronic devices.

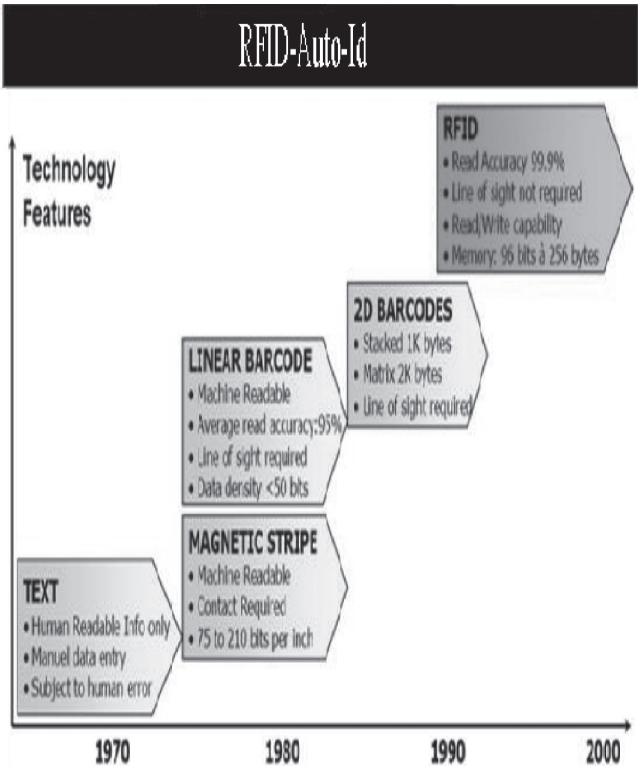

Figure 3.5 Evolution of identifications.

Mario Cardullo's passive radio transponder device in 1973 was the first true ancestor of modern RFID. For object or article identifications, text and then barcodes were widely used before RFID tags come into being (Figure 3.5).

UPC (universal product code) of UCC (Uniform Code Council, later called GS1 US) was widely used in the United States and Canada for tracking trade items in stores (Figure 3.6). EAN (European article number), developed after UPC, was used in Europe. EAN International is now called GS1. All the numbers encoded in UPC and EAN (as well as EAN/UCC-13, EAN/UCC-14, EAN-8, etc.) bar codes are known as global trade item numbers (GTIN). GS1, GS1 US, and Auto-ID labs joined forces to form EPCglobal in 2003 (which means the United States and Europe share the EPC standard; however, UID

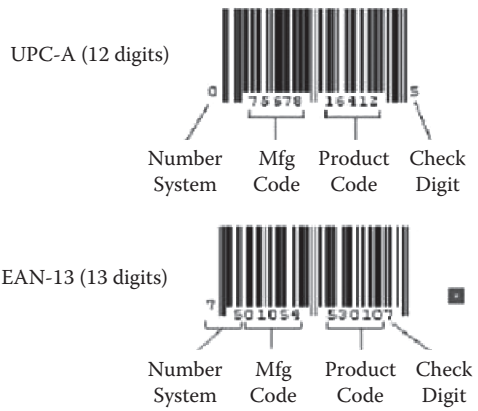

Figure 3.6 Bar code formats. (From James B. Ayers and Mary Ann Odegaard, *Retail Supply Chain Management*, New York: Auerbach Publications, 2008.)

[ubiquitous ID] is used in Japan). EPCglobal is an organization set up to achieve worldwide adoption and standardization of EPC technology. The main focus of the group currently is to create both a worldwide standard for RFID and the use of the Internet to share data via the EPCglobal Network™.

The automotive industry has been using the technology in manufacturing for decades. Pharmaceutical companies are already adopting the technology to combat counterfeiting. The Department of Homeland Security has been looking to leverage RFID along with other sensor networks to secure supply chains and ensure port and border security. Many major businesses already use RFID for better asset visibility and management. But the RFID technology and applications became widely used after the industry mandates started in 2004. Walmart and the U.S. Department of Defense (DOD) along with some other major retailers required their suppliers to begin RFID tagging pallets and cases shipped into their distribution centers in 2005 (http://www.controlelectric.com/RFID/Wal-Mart_DOD_Mandates.html). The mandates impacted some 200,000 suppliers globally. That year was also when the ITU published the Internet of Things report. Many companies

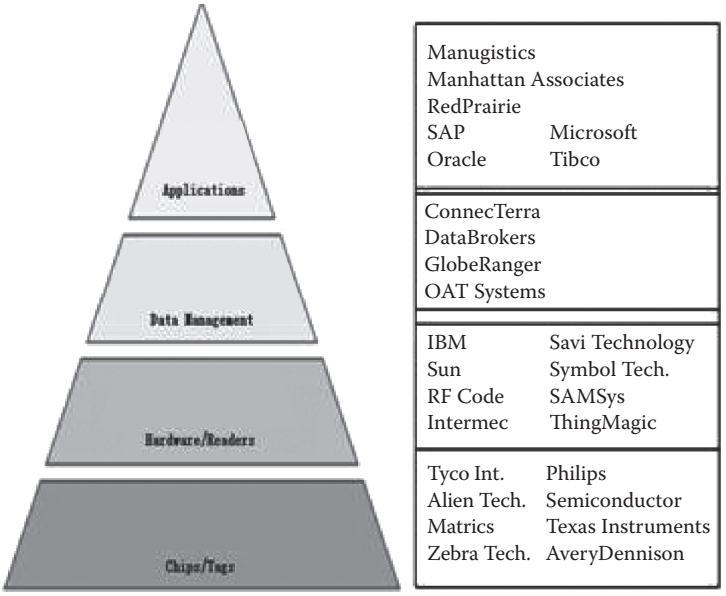

Figure 3.7 RFID value chain and vendors.

worldwide have since started to aggressively invest and build RFID technologies and products. Figure 3.7 shows a list of RFID vendors and solutions introduced in 2004.

The International Organization for Standardization asserts jurisdiction over the air interface for RFID through standards-in-development ISO 18000-1 through 18000-7. These are represented in the United States by American National Standards Institute and the Federal Communications Commission. The frequencies available are shown in Table 3.5.

The Auto-ID concept is that the data will be stored on the Internet or the EPCglobal network, and the EPC stored in the tag is used as an index to locate the data. This introduces several standards as shown in the EPCglobal architecture framework [51], which is a collection of interrelated standards for hardware, software, and data interfaces, together with core services that are operated by EPCglobal and its delegates.

All the software specifications from the Auto-ID Center are written in and for Java. Java-based middleware plays

Table 3.5 RFID Frequency Ranges

RFID	*Key Applications*	*Standard*
125 kHz (LF)	Inexpensive passive RFID tags for identifying animals	ISO 18000-2
13.56 MHz (HF)	Inexpensive passive RFID tags for identifying objects; library book identification, clothes identification, etc.	ISO 14443
400 MHz (UHF)	For remote control for vehicle center locking systems	ISO 18000-7
868 MHz, 915 MHz, and 922 MHz (UHF)	For active and passive RFID for logistics in Europe, the United States, and Australia, respectively	Auto-ID Class 0 Auto-ID Class 1 ISO 18000-6
2.45 GHz (MW)	An ISM band used for active and passive RFID tags; e.g., with temperature sensors or GPS localization	ISO 18000-4
5.8 GHz (MW)	Used for long-reading range passive and active RFID tags for vehicle identification, highway toll collection	ISO 18000-5

an important and pivotal role in the implementation of the EPCglobal architecture framework, especially the application level events (ALE) and EPC information services (EPCIS). That's why middleware and software giants such as IBM, Oracle, Microsoft, and SAP all have large investments in RFID and developed complete RFID solution stacks.

The ONS (object naming service) is an authoritative directory service just like the DNS (domain name service) for the Internet that routes requests for information about EPCs between a requesting party and the product manufacturer, via a variety of existing or new network- or Internet-based information resources. That's why EPCglobal has worked with VeriSign to provide such a service in addition to VeriSign's

DNS. VeriSign has operated the authoritative root directory for the EPCglobal Network since 2005. Although companies have successfully implemented internal RFID solutions that have captured efficiencies within the enterprise, the greatest promise of the EPCglobal Network is the ability to extend the benefits across trading-partner boundaries via the Internet to realize the IoT vision. It is not hard to imagine that RFID can be used in almost all industry segments and the benefits it will bring.

There are many estimates of the RFID market size. IDTechEx predicts that the total market of RFID will be around US$27 billion worldwide in 2018. The market size of China will be around US$1.7 billion in 2014 per iSuppli reports [210]. The RFID market was more than US$3 billion in 2008 in China when the issuing of RFID-based national ID cards for each citizen reached its peak.

In a contactless smart card, using NFC (near field communication) technologies, the chip communicates with the card reader through an induction technology similar to that of RFID. These cards require close proximity to an antenna to complete a transaction. They are often used when transactions must be processed quickly or hands-free, such as on mass transit systems, where a smart card (ticket) can be used without even removing it from a wallet. Figure 3.8 shows the RFID-based ticket and the ^{ez}M2M middleware-based application system the author's team built for the Beijing Olympic Games in 2008.

Mobile payment or mobile wallet is an alternative payment method that has been well adopted in many parts of Europe and Asia. Juniper Research forecasts that the combined market for all types of mobile payments is expected to reach more than $600 billion globally by 2013. RFID/NFC technologies have been used for mobile payments in China by its big three telco companies as well as China UnionPay, whose UnionPay cards can be used in 104 countries and regions around the world.

Figure 3.8 Example of RFID application.

3.4 WSN: The Internet of Transducers

As defined in the first section, WSN is more for sensing and information-collecting purposes. Other networks include BSN (body sensor network [56]), VSN (visual or video sensor network [54,55]), vehicular sensor networks (V2V, V2I), underwater (acoustic) sensor networks (UW-ASN), urban/social/participatory sensor networks, interplanetary sensor networks, fieldbus networks (categorized as SCADA systems, the good oldies in the buildings and plants are getting wireless/mobile capabilities and scaling up), and others.

BSN is a term used to describe the application of wearable computing devices to enable wireless communication between several miniaturized body-sensor units and a single body central unit worn on the human body to transmit vital signs and motion readings to medical practitioners or caregivers (Figure 3.9). Applications of BSN are expected to appear primarily in the healthcare domain, especially for continuous monitoring and logging of vital parameters for patients suffering from chronic maladies such as diabetes, asthma, and heart attacks.

Visual sensor networks are based on several diverse research fields, including image/vision processing, communication and networking, and distributed and embedded system

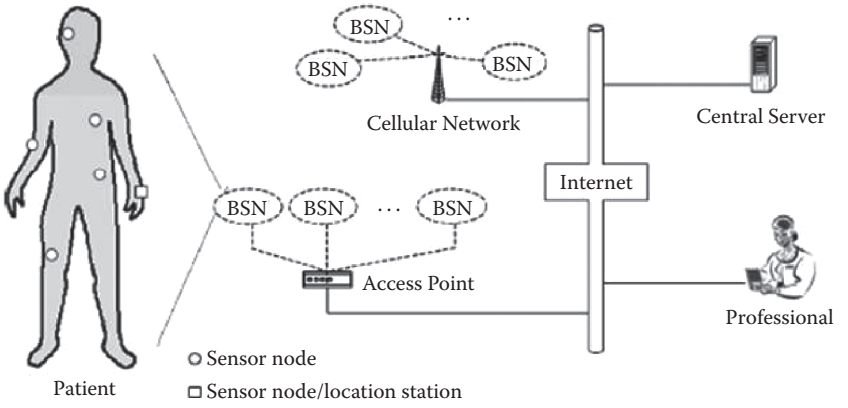

Figure 3.9 Body sensor networks. (From Hui Chen and Yang Xiao (eds.), *Mobile Telemedicine: A Computing and Networking Perspective*, New York: Auerbach Publications, 2008.)

processing. Applications include surveillance, environmental monitoring, smart homes, virtual reality, and others.

With the development of WSN, recent technological advances have led to the emergence of distributed wireless sensor and actuator networks (WSANs) that are capable of observing the physical world, processing the data, making decisions based on the observations, and performing appropriate actions. These networks can be an integral part of systems such as battlefield surveillance and microclimate control in buildings; nuclear, biological and chemical attack detection; home automation; and environmental monitoring.

The extended scope of WSN is the USN, or ubiquitous sensor network, a network of intelligent sensors that could one day become ubiquitous [53]. This USN is also a unified "invisible," "pervasive," or "ambient intelligent" Internet of Things.

The development of WSNs was motivated by military applications such as battlefield surveillance. The WSN is built of nodes—from a few to several hundred or even thousands—each node connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio

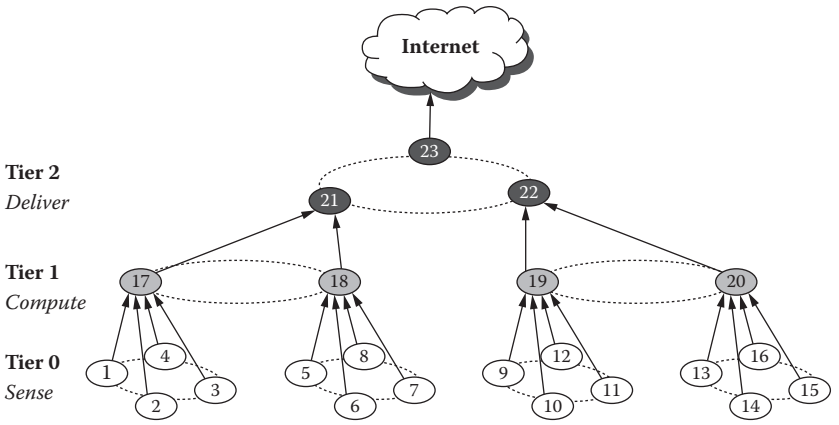

Figure 3.10 Sensor network architecture. (From Mark Yarvis and Wei Ye, "Tiered Architectures in Sensor Networks," in Mohammad Ilyas and Imad Mahgoub (eds.), *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, Boca Raton, FL: CRC Press, 2004.)

transceiver with an antenna, a microcontroller, an electronic circuit for interfacing with the sensors, and an energy source, usually a battery or an embedded form of energy harvesting.

The architecture of a typical sensor network is shown in Figure 3.10. The topology of the WSNs can vary from a simple star network to an advanced multihop mesh network with a gateway sensor (sink) node connected (e.g., via a cellular M2M module) with a remote central server.

- Sensor node: sense target events, gather sensor readings, manipulate information, send them to gateway via radio link
- Base station/sink: communicate with sensor nodes and user/operator
- Operator/user: task manager, send query

Routing is required for reliable data transmission in a WSN mesh network. Routing protocols are distributed and reactive: nodes in the system start looking for a route only when they have application data to transmit. Ad hoc on-demand distance

vector (AODV) and dynamic source routing (DSR) are frequently used routing algorithms.

The U.S. DOD, which operates the largest and most complex supply chain in the world, awarded in January 2009 a contract for $429 million in DASH7 infrastructure. This represents a major development in terms of global adoption of an ultra-low-power WSN technology based on a single global standard [72].

WSN is currently an active research area with limited mission-critical uses. IT giants such as IBM and Microsoft have invested in WSN research for a long time with little commercial success. Currently there is no common WSN platform. Some designs such as Berkeley Motes and their clones have broader user and developer communities. However, many research labs and commercial companies prefer to develop and produce their own devices. Since there is no true killer application for WSNs that would drive the costs down, it is often more convenient and even less expensive to build your own WSN devices than to buy commercially available ones.

Some of the existing WSN platforms are summarized in Table 3.6. Most of the device designs are still in the research stage.

According to IDTechEx, the price per WSN node was about $30 in 2011. In the future (10 years), a functionally equivalent "smart dust" sensor node is expected to be available for use with cost per node less than $1.

Energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. WSNs are meant to be deployed in large numbers in various environments, including remote and hostile regions, with ad hoc communications as key. For this reason, algorithms and protocols need to address the following issues:

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

Table 3.6 RFID Platforms

Accsense, Inc. (http://www.accsense.com/)
Ambient Systems mesh networks (Netherlands) (http://www.ambient-systems.net/ambient/technology-features.htm)
Atlas (Pervasa/University of Florida) (http://www.pervasa.com/)
BEAN Project (http://www.dcc.ufmg.br/~mmvieira/publications/bean.pdf#search=%22BEAN%20brazilian%20sensor%20node%22)
Berkeley Motes/Piconodes
BTnode (ETH Zurich) (http://www.btnode.ethz.ch)
Cortex Project
COTS Dust (Dust Networks) (http://www.dustnetworks.com/
EYES Project (http://www.eyes.eu.org)
Fleck (CSIRO Australia) (http://www.btnode.ethz.ch/Projects/Fleck)
Glacsweb from University of Southampton (http://www.glacsweb.org)
G-Node from SOWNet Technologies (http://sownet.nl/index.php/en/products/gnode)
Global Sensor Networks (http://gsn.sourceforge.net/)
Hoarder Board—Open Hardware Design (MIT Media Lab) (http://vadim.oversigma.com/Hoarder/Hoarder.htm)
iSense hardware platform from Coalesenses GmbH, Germany (http://www.coalesenses.com)
Kmote (TinyOS Mall) (http://www.tinyosmall.co.kr/)
MeshScape (Millennial Net, Inc.) (http://millennialnet.com/Technology.aspx)
Mica Mote (Crossbow) (http://www.xbow.com/Products/productsdetails.aspx?sid=62)
MicroStrain, Inc. (http://www.microstrain.com/)
Newtrax Technologies, Inc. (http://www.newtraxtech.com/)
openPICUS—Open Hardware (http://openpicus.blogspot.com/)

Table 3.6 (continued) RFID Platforms

Particles (Particle Computer) spun out of TecO, Univ. of Karlsruhe) (http://www.particle-computer.de
PicoCrickets (Montreal, Canada) (http://www.picocricket.com)
Redwire Econotag (http://www.redwirellc.com/store/node/1)
ScatterWeb ESB nodes (http://www.inf.fu-berlin.de/inst/ag-tech/scatterweb_net/)
SensiNet Smart Sensors (Sensicast Systems) (http://www.sensicast.com)
Sensor Internet Project (http://sip.deri.ie)
Sensor Webs (SensorWare Systems) spun out of the NASA/JPL Sensor Webs Project (http://www.sensorwaresystems.com/)
Shockfish TinyNodes
Smart Dust (Dust Networks) spun out of UC Berkeley (http://www.dustnetworks.com/)
TIP Mote (Maxfor) (http://www.maxfor.co.kr/)
Tmote (Moteiv) spun out of UC Berkeley (http://www.moteiv.com/)
Tyndall Motes (http://www.tyndall.ie/mai/Wireless%20Sensor%20Networks.htm)
UCLA iBadge
Waspmote (Libelium) (http://www.libelium.com/waspmote)
WINS (Rockwell Wireless Integrated Network Sensors)
WINS (UCLA)
WSN430 (INSA de Lyon/INRIA) (http://www.senslab.info/)
XYZ node (http://www.eng.yale.edu/enalab/XYZ/)

WSNs have found more and more applications in a variety of pervasive computing environments. However, how to support the development, maintenance, deployment and execution of applications over WSNs remains a nontrivial and challenging task, mainly because of the gap between the

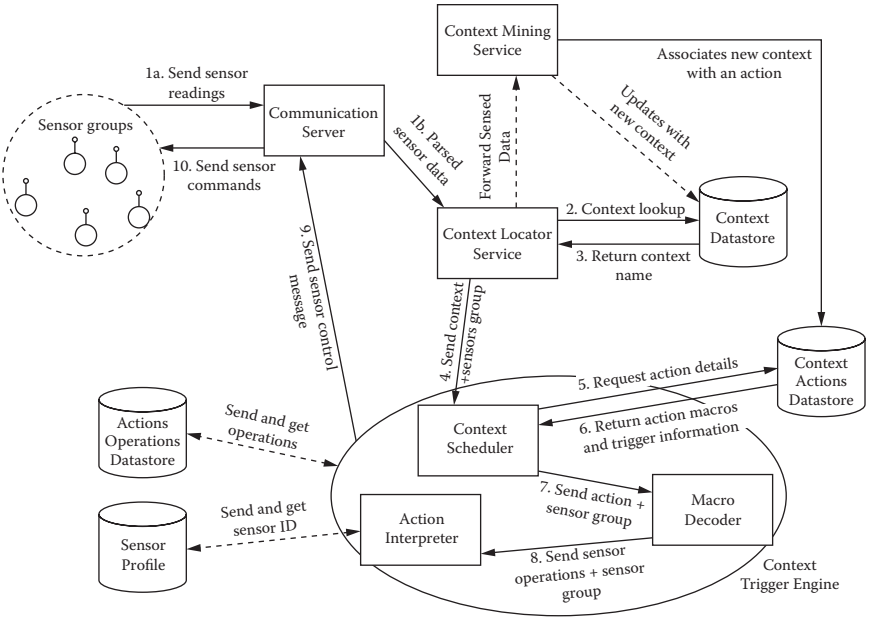

Figure 3.11 Context-aware system based on WSN. (From Seng Loke, *Context-Aware Pervasive Systems: Architectures for a New Breed of Applications*, New York: Auerbach Publications, 2007.)

high-level requirements from pervasive computing applications and the underlying operation of WSNs. Middleware for WSN, the middle-level primitives between the software and the hardware, can help bridge the gap and remove impediments. Middleware can help build context-aware IoT systems as shown in Figure 3.11.

Mobile sensor networks (MSNs) are WSNs in which nodes can move under their own control or under the control of the environment. Mobile networked systems combine the most advanced concepts in perception, communication, and control to create computational systems capable of interacting in meaningful ways with the physical environment, thus extending the individual capabilities of each network component and network user to encompass a much wider area and range of data. A key difference between a mobile WSN and

a static WSN is how information is distributed over the network. Under static nodes, a new task or data can be flooded across the network in a very predictable way. Under mobility this kind of flooding is more complex, depending on the mobility model of the nodes in the system. The proliferation of commodity smartphones that can provide location estimates using a variety of sensors—GPS, WiFi real-time locating systems (RTLS), or cellular triangulation—opens up the attractive possibility of using position samples from drivers' phones to monitor traffic delays at a fine spatiotemporal granularity. MSN systems such as vTrack [58] of the MIT CarTel group have been built to monitor traffic delays and change routes.

According to IDTechEx research in the new report "Wireless Sensor Networks 2011–2021" [211], the WSN market is expected to grow rapidly from $0.45 billion in 2011 to $2 billion in 2021. These figures refer to WSN defined as wireless mesh networks, that is, self-healing and self-organizing. WSNs will eventually enable the automatic monitoring of forest fires, avalanches, hurricanes, failure of country-wide utility equipment, traffic, hospitals, and much more over wide areas, something previously impossible. More humble killer applications already exist such as automating meter readings in buildings, and manufacture and process control automation.

The United States dominates (72 percent, according to IDTechEx, of all countries worldwide) the development and use of WSN partly because of the heavier funding available. The U.S. WSN industry sits astride the computer industry thanks to companies such as Microsoft and IBM, and WSN is regarded as a next wave of computing, so U.S. industry is particularly interested in participating. Add to that the fact that the U.S. military, deeply interested in WSN, spends more than all other military forces combined, and creating and funding start-ups is particularly easy in the United States, and you can see why the United States is ahead at present.

3.5 SCADA: The Internet of Controllers

For more than a decade, many in the building industry have been envisioning a day when building automation systems (BAS) would become fully integrated with communication and human interface practices and standards widely employed for information technology systems. Not long ago, building automation graphical interfaces (shown in Figure 3.12; the part on the right is the human–machine interface the author's team built for the super-energy-efficiency building at QingHua University) employed almost no web-browser techniques and technologies; now, web approaches are the basis of many such packages. How close we are to a complete convergence of BAS and IT is difficult to tell, but it is not too much of a stretch to say that when the convergence is complete, there may be nothing to distinguish one from the other [59].

SCADA (supervisory, control and data acquisition) systems, as the core technology of the controls–IT convergence, will evolve and take the center stage. By their very nature, SCADA, low-data-rate (LDR), and M2M/IoT [129] services are closely related and largely overlapped in technologies and deployment approaches, as per GII Research [60]. Also, WSN is considered a new computing paradigm that emerged from the fusion of the SCADA systems and ad hoc networks technologies [61]. The advent of the Internet of Things will no doubt speed up the controls–IT convergence and make control systems and IT systems inseparable and indistinguishable from each other.

SCADA was generally referring to industrial control systems (ICSs): computer systems that monitor and control industrial, infrastructure, or facility-based processes, as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.

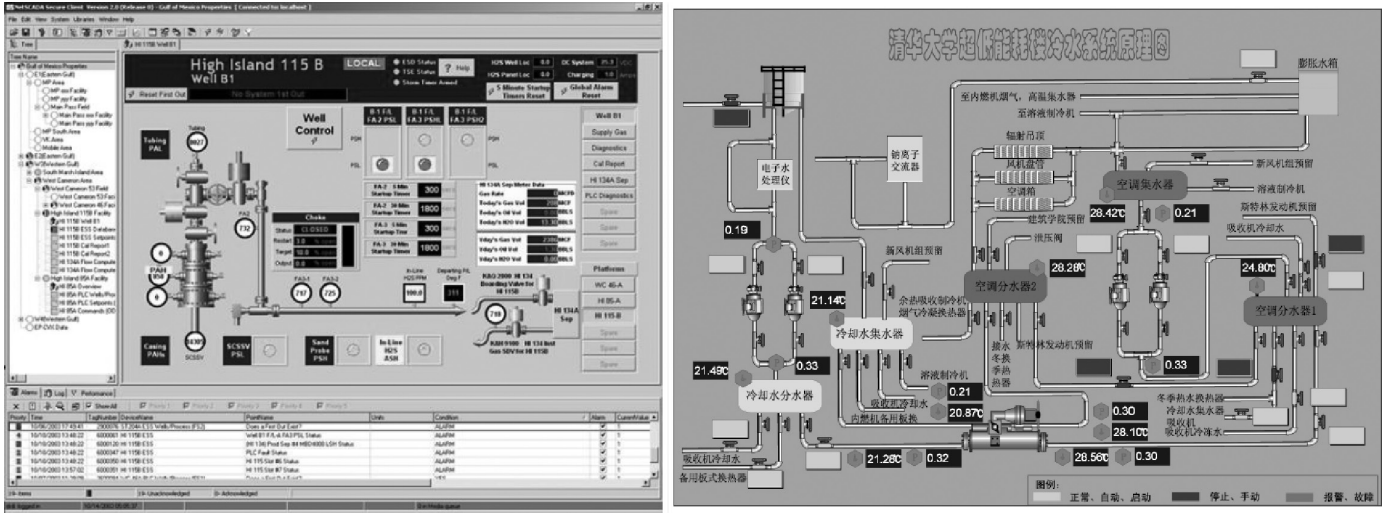

Figure 3.12 Examples of SCADA graphics and animations.

- Infrastructure processes may be public or private and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large transportation systems.
- Facility processes occur in both public and private facilities, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption using PLCs (programmable logic controllers) and DCSs (distributed control systems) via the OPC (OLE for process control) middleware.

An existing SCADA system usually consists of the following subsystems (Figure 3.13):

- A human–machine interface (HMI), which is the apparatus that presents process data to a human operator, and through this, the human operator monitors and controls the process.
- Remote terminal units (RTUs) connect to sensors in the process, convert sensor signals to digital data, and send digital data to the supervisory system.
- PLCs are used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- DCSs; as communication infrastructures with higher capacity become available, the difference between SCADA and DCS will fade. SCADA is combining the traditional DCS and SCADA.
- As mentioned before, M2M (telemetry), WSN, smart systems, CPS, and others all have overlaps of scope with SCADA, but the extended scope of SCADA is bigger under the IoT umbrella.

A SCADA system could be a layer between the top-layer business systems such as ERP, WMS (warehouse management

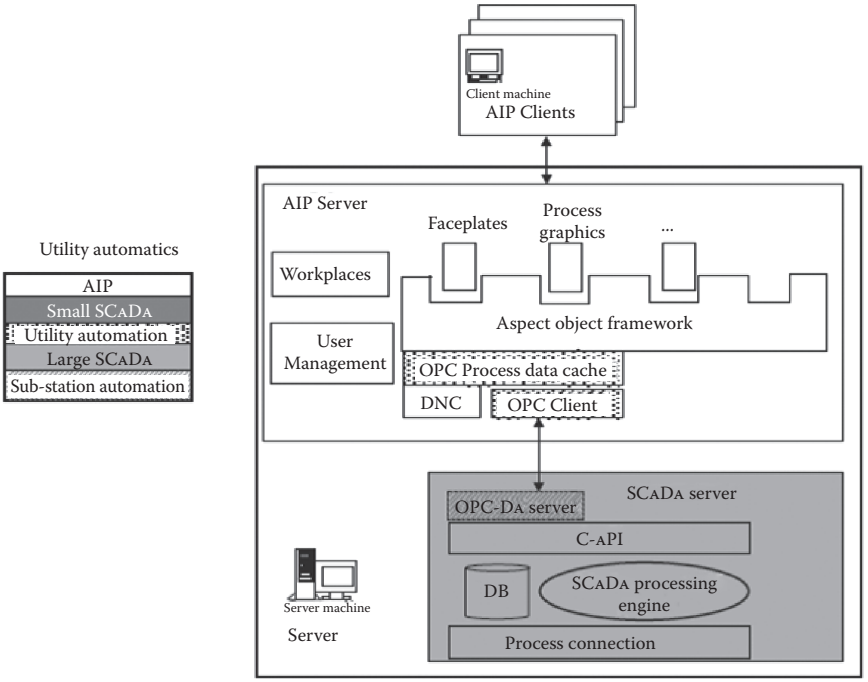

Figure 3.13 Components of a SCADA system. (From Yauheni Veryha and Peter Bort, "Industrial IT-Based Network Management," in Richard Zurawski (ed.), *The Industrial Information Technology Handbook*, Boca Raton, FL: CRC Press, 2005.)

system), SCM, CRM, EAM (enterprise asset management), PIMS (plant information management system), EMI (enterprise manufacturing intelligence), LIMS (laboratory information management system), and other applications and the lower layer DCS, PLC, RTU, MES (manufacturing execution system), SIS (supervisory information system in plant level), and other systems as exemplified in Figure 3.14.

A traditional SCADA system is a client/server system. New technological developments have turned C/S SCADA systems into middleware-backed, web-based, three-tiered open systems with SOA capabilities.

Figure 3.15 showcases a typical SCADA middleware or platform architecture. Examples of such platforms include

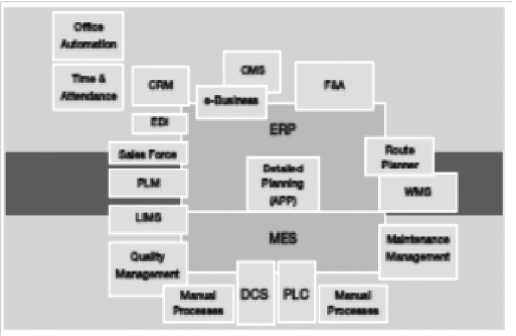

Figure 3.14 SCADA sits in the center.

Figure 3.15 Middleware-based SCADA systems.

(Invensys) Wonderware's ArchestrA™, (Honeywell) Tridium's Niagara Framework™ (a Java EE–based platform), THTF's ezM2M Middleware for IoT, various implementations of the OPC UA framework standard, and the list goes on.

SCADA systems allow the automation of complex industrial processes where human control is impractical. However, with all the raw data and real-time updates pouring in, it can be difficult to decipher what is going on and how to respond. All the on-screen numbers, flashing lights, and blaring alarms still leave you in the dark. The solution is an integrated controls–IT convergence system [59,183].

IP video technology has become one of the hottest trends in the automation industry today, especially since automation and surveillance systems have both migrated to IP-based applications. Moreover, the integration of IP surveillance software with automation systems is gaining popularity and momentum, and integrating real-time visual surveillance systems [100] with SCADA systems via IP video technology is now both a viable and an affordable solution for system integrators.

Many industries are using SCADA as a core technology to link the geographically separated facilities and support new business processes in response to changing industry dynamics.

As examples, the worldwide oil and gas industry SCADA market was $850 million in 2007 and is forecast to be over $1.3 billion in 2012; the worldwide market for electric power SCADA was $1.629 trillion in 2008 and is forecast to be over $2.125 trillion in 2013; and the worldwide water and wastewater industry SCADA market was $212 million in 2006 and is forecast to be over $275 million in 2011, all according to ARC Advisory Group studies.

In 2010, Chinese government and industry leaders stated that a "unified strong and smart grid" [166] system is going to be built across the country by 2020. SCADA sales will increase as part of this initiative and overall IoT development.

Supported by intelligent field devices, expanded communications networks, and improved compatibility with IT, especially the Internet and web technologies, SCADA can now provide a wealth of information and knowledge as a means to modify business processes and enable the creation of new SCADA-based IoT applications.

3.6 Summary

Many IoT technologies and applications are not new. IoT is an aggregation, convergence, and evolution of existing ICT technologies and applications. What should be included in the IoT paradigm has long been and still is an issue of many disagreements.

In this chapter, a solution to this disagreement is introduced. The four-pillar classification of the Internet of Things was proposed based on analysis of common IoT characteristics and previous categorization efforts. The technologies, applications, and market potentials of each pillar were described in detail.

In the next chapter, we will talk about the three DCM layers of IoT value chain, the role of each, and what is included in each layer.