Chapter 4

The DNA of IoT

4.1 DCM: Device, Connect, and Manage

The first issue that the Internet of Things (IoT) ecosystem needs to address is the long and fragmented value chain that characterizes the industry. This results in numerous supplier–buyer interfaces, adding costs and time to the launch of any new product offering.

Just like the blind men and the elephant story and people's understanding of the four pillars or the six pillars mentioned before, the IoT is still different things to different people, even though introduced more than a decade ago. However, there is one thing most people agree with: IoT (or machine-to-machine, M2M; wireless sensor networks, WSN; supervisory control and data acquisition, SCADA; radio-frequency identification, RFID; etc.) systems all have three layers. Figure 4.1 is an example IoT application of an intelligent nuclear power plant IoT system [63] of Datang Telcom in China. More examples of the three-layer architecture of IoT can be found at European Telecommunications Standards Institute (ETSI)'s website [212].

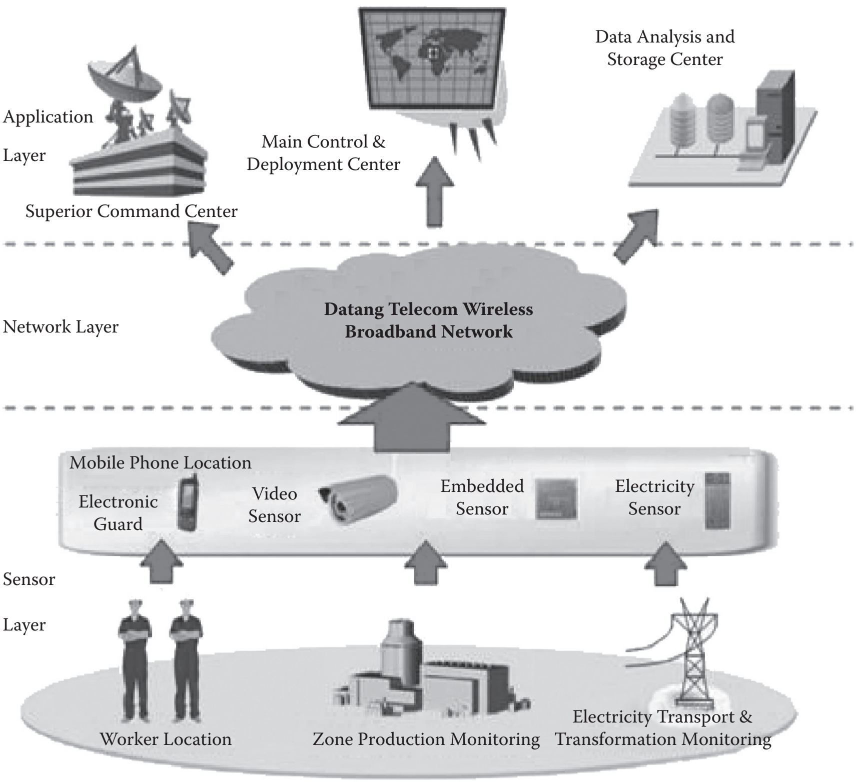

Figure 4.1 Examples of three-layer architecture of IoT.

The author has proposed the concept and acronym DCM (device, connect, and manage [74]) as a corporate stretegy or slogan for TongFang Co. Ltd. The board of the company announced financing of 500 million Chinese renminbi (RMB) (or US$78.5 million) for the development of the IoT/DCM business in 2005. Numerex created a better acronym called DNA™ (devices, networks, and applications) [213] in 2008 (Figure 4.2).

The three-layer DCM classification is more about the IoT value chain than its system architecture at runtime. For system architecture, some (e.g., one of Numerex's and IBM's reports) have divided the IoT system into as many as nine layers, from bottom to top: devices, connectivity, data collection,

M	• Vertical Applications • Server-side Middleware Platform • Data Management	A
C	• Machine Type Communication • Edge Middleware • Pervasive Networks	N
D	• Local/Ad-hoc Sensor Networks • Embedded Middleware • Sensors and Actuators	D

Figure 4.2 DCM (DNA) of IoT.

communication, device management, data rules, administration, applications, and integration.

While large companies such as IBM, Oracle, Microsoft, and others have comprehensive solutions, products, and services that cover almost the entire value chain, startups or smaller players in the IoT sector should focus on providing products or services in no more than two components or areas in the value chain. The following sections discuss the three DCM components.

4.2 Device: Things That Talk

According to the IoT definitions and descriptions in the previous chapters, devices or assets can be categorized as two groups: those that have *inherent intelligence* such as electric meters or heating, ventilation, and air-conditioning (HVAC) controllers, and those that are inert and must be *enabled* to become smart devices (e.g., RFID tagged) such as furniture or animals that can be electronically tracked and monitored—things that "talk."

Just as Paul Saffo [214], a technological forecaster and strategist, described in an interview in 2002:

> This is the Cambrian explosion of communications. We are seeing a radical species divergence

> of different kinds of devices and different types of things that want to talk, from your washing machine having an Internet connection and being able to scream for help if it is broken, to your car having a wireless connection for data telemetry back to the manufacturer. Today, voice communications is way below 1% of the total communications traffic on this planet. That's why people are giving voice away for free. So that means that we're going to see a whole zoo of new kinds of devices that have to talk. It's going to become a world of smartifacts, or intelligent objects. This stuff is so cheap, we're putting chips in everything, anything with a chip inside can be connected into the Internet of Things.

Devices that perform an input function are commonly called sensors because they "sense" a physical change in some characteristic that changes in response to some excitation, for example, heat or force, and convert that into an electrical signal. Devices that perform an output function are generally called actuators and are used to control some external device, for example, movement. Both sensors and actuators are collectively known as transducers because they are used to convert energy of one kind into energy of another kind. For example, a microphone (input device) converts sound waves into electrical signals for the amplifier to amplify, and a loudspeaker (output device) converts the electrical signals back into sound waves.

A *sensor* (also called a detector) is a device that responds to a physical stimulus, measures the physical stimulus quantity, and converts it into a signal, usually electrical, which can be read by an observer or by an instrument.

Based on this definition, a sensor is basically an electrical device. It could be an M2M terminal, an RFID reader, or a SCADA meter. Sensors are particularly useful for making in-situ measurements (things that talk) such as in industrial process control or medical applications. A sensor can be very small and itself can be a trackable device; however, when a train or an aircraft is instrumented with a small sensor, the entire aircraft becomes one trackable device.

The sensor itself, if not connected, is not part of the IoT or WSN value chain. This is like a central processing unit (CPU), which is not part of the web or social networking services, even though they are somwhat related. Some sensors do not generate electrical signals; for example, a mercury-in-glass thermometer converts the measured temperature into expansion and contraction of a liquid, which can be read on a calibrated glass tube. However, it's important to understand the types and shapes of the ubiquitous sensors if you are into IoT, just as an architect should know what concrete and cement are as well as their differences. Figure 4.3 showcases a few sample sensors.

Some of the existing sensors and their types are listed in Table 4.1. The size of the overall sensor market is difficult to estimate. A number of research reports on the market size of

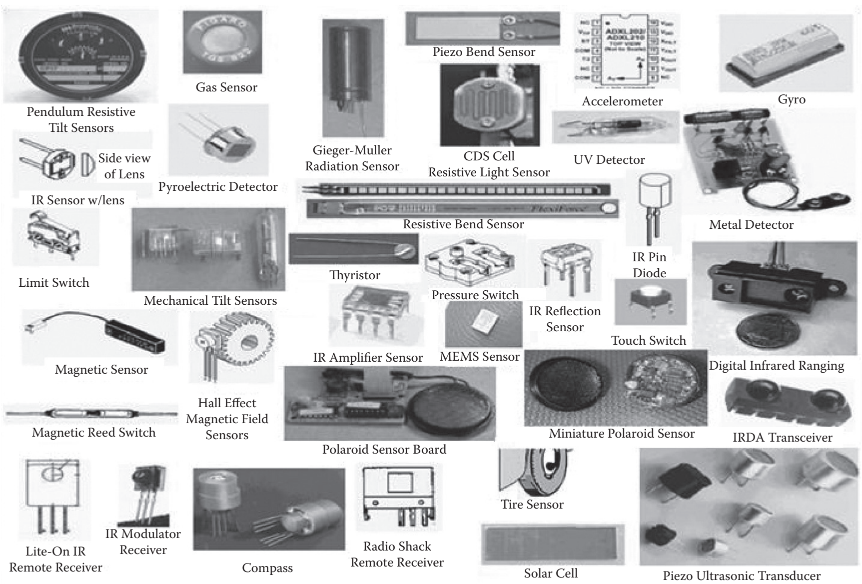

Figure 4.3 Examples of sensors.

Table 4.1 List of Sensors and Types

Sensor Type (Examples)	*Sensors (Examples)*
Acoustic, sound, vibration	Geophone, hydrophone, lace sensor, microphone, seismometer
Automotive, transportation	Air-fuel ratio meter, crank sensor, curb feeler, defect detector, engine coolant temperature (ECT) sensor, all effect sensor, MAP (manifold absolute pressure) sensor, mass flow sensor or mass airflow (MAF) sensor, oxygen sensor, parking sensors, radar gun, speedometer, speed sensor, throttle position sensor, tire-pressure monitoring sensor, transmission fluid temperature sensor, turbine speed sensor (TSS) or input speed sensor (ISS), ariable reluctance sensor, vehicle speed sensor (VSS), water sensor or water-in-fuel sensor, wheel speed sensor
Chemical	Breathalyzer, carbon dioxide sensor, carbon monoxide detector, catalytic bead sensor, chemical field-effect transistor, electrochemical gas sensor, electronic nose, electrolyte–insulator–semiconductor sensor, hydrocarbon dewpoint analyzer, hydrogen sensor, hydrogen sulfide sensor, infrared point sensor, ion-selective electrode, nondispersive infrared sensor, microwave chemistry sensor, nitrogen oxide sensor, olfactometer, optode, oxygen sensor, pellistor, pH glass electrode, potentiometric sensor, redox electrode, smoke detector, zinc oxide nanorod sensor
Electric current, electric potential, magnetic, radio	Ammeter, current sensor, galvanometer, hall effect sensor, hall probe, leaf electroscope, magnetic anomaly detector, magnetometer, metal detector, multimeter, ohmmeter, radio direction finder, telescope, voltmeter, voltage detector, watt-hour meter

Table 4.1 (continued) List of Sensors and Types

Sensor Type (Examples)	*Sensors (Examples)*
Environment, weather, moisture, humidity	Actinometer, bedwetting alarm, dew warning, fish counter, gas detector, hook gauge evaporimeter, hygrometer, leaf sensor, pyranometer, pyrgeometer, psychrometer, rain gauge, rain sensor, seismometers, snow gauge, soil moisture sensor, stream gauge, tide gauge
Flow, fluid velocity	Air flow meter, anemometer, flow sensor, gas meter, mass flow sensor, water meter
Force, density, level	Bhangmeter, hydrometer, force gauge, level sensor, load cell, magnetic level gauge, nuclear density gauge, piezoelectric sensor, strain gauge, torque sensor, viscometer
Ionizing radiation, subatomic particles	Bubble chamber, cloud chamber, geiger counter, neutron detection, particle detector, scintillation counter, scintillator, wire chamber
Navigation instruments	Air speed indicator, altimeter, attitude indicator, depth gauge, fluxgate compass, gyroscope, inertial reference unit, magnetic compass, MHD sensor, ring laser gyroscope, turn coordinator, variometer, vibrating structure gyroscope, yaw rate sensor
Optical, light, imaging, photon	Charge-coupled device, colorimeter, contact image sensor, electro-optical sensor, flame detector, infra-red sensor, kinetic inductance detector, LED as light sensor, Nichols radiometer, fiber-optic sensor, photodetector, photodiode, photomultiplier tubes, phototransistor, photoelectric sensor, photoionization detector, photomultiplier, photoresistor, photoswitch, phototube, scintillometer, Shack–Hartmann, single-photon avalanche diode, superconducting nanowire single-photon detector, transition edge sensor, visible light photon counter, wavefront sensor

continued

Table 4.1 (continued) List of Sensors and Types

Sensor Type (Examples)	*Sensors (Examples)*
Position, angle, displacement, distance, speed, acceleration	Accelerometer, auxanometer, capacitive displacement sensor, free fall sensor, gravimeter, inclinometer, laser rangefinder, linear encoder, linear variable differential transformer (LVDT), liquid capacitive inclinometers, odometer, piezoelectric accelerometer, position sensor, rotary encoder, rotary variable differential transformer, selsyn, sudden motion sensor, tilt sensor, tachometer, ultrasonic thickness gauge
Pressure	Barograph, barometer, boost gauge, bourdon gauge, hot filament ionization gauge, ionization gauge, McLeod gauge, oscillating U-tube, permanent downhole gauge, Pirani gauge, pressure sensor, pressure gauge, tactile sensor, time pressure gauge
Proximity, presence	Alarm sensor, Doppler radar, motion detector, occupancy sensor, proximity sensor, passive infrared sensor, reed switch, stud finder, triangulation sensor, touch switch, wired glove
Sensor technology	Active pixel sensor, biochip, biosensor, capacitance probe, catadioptric sensor, carbon paste electrode, displacement receiver, electromechanical film, electro-optical sensor, Fabry–Pérot interferometer, image sensor, inductive sensor, intelligent sensor, lab-on-a-chip, leaf sensor, machine vision, micro-sensor arrays, photoelasticity, RADAR, ground-penetrating radar, synthetic aperture radar, sensor array, sensor grid, sensor node, soft sensor, SONAR, underwater acoustic positioning system, staring array, transducer, ultrasonic sensor, video sensor, visual sensor network, Wheatstone bridge

Table 4.1 (continued) List of Sensors and Types

Sensor Type (Examples)	*Sensors (Examples)*
Thermal, heat, temperature	Bolometer, bimetallic strip, calorimeter, exhaust gas temperature gauge, gardon gauge, golay cell, heat flux sensor, infrared thermometer, microbolometer, microwave radiometer, net radiometer, quartz thermometer, resistance temperature detector, resistance thermometer, silicon bandgap temperature sensor, temperature gauge, thermistor, thermocouple, thermometer
Other sensors and sensor related techniques	Analog image processing, digital holography, frame grabbers, intensity sensors and their properties, atomic force microscopy, compressive sensing, hyperspectral sensors, millimeter wave scanner, magnetic resonance imaging, diffusion tensor imaging, functional magnetic resonance imaging, optical coherence tomography, positron emission tomography, quantization (signal processing), range imaging, Moire deflectometry, phase unwrapping techniques, time-of-flight camera, structured-light 3-D scanner, omnidirectional camera, catadioptric sensor, single-photon emission computed tomography (SPECT), transcranial magnetic stimulation (TMS)

different sensor sectors are on http://www.sensorsportal.com. For example, the global automotive sensor market, including silicon-based sensors, grew by 9.7 percent in 2006 to $10.1 billion and is forecast by Strategy Analytics to reach $17.1 billion by 2013 as vehicle systems such as powertrain control, safety, and convenience features become more advanced and require more sensors. IC Insights estimates that the wireless sensors and transmitters market will surpass $1.8 billion by 2012. The CMOS image sensor market alone is projected to be $8.3 billion by 2014.

Microelectromechanical systems (MEMS) is the technology of very small mechanical devices driven by electricity. It merges at the nanoscale into nanoelectromechanical systems (NEMS) and nanotechnology. MEMS are also referred to as micromachines in Japan, or microsystems technology in Europe. MEMS can be a sensor or actuator, or a transducer.

Energy harvesting (also known as power harvesting or energy scavenging) is the process by which energy is derived from external sources (e.g., solar power, thermal energy, wind energy, salinity gradients, and kinetic energy), captured, and stored for small wireless autonomous devices, like those used in wearable electronics and WSNs. Energy-harvesting devices or sensors have a very long historical connection to the water wheel, windmills, and waste heat. Before batteries (Volta, 1799) and the dynamo (Faraday, 1831), those energy-harvesting devices were the only ways to get any useful power. The following are options for energy harvesting:

- RF, used for RFID tag energy broadcasting and harvesting
- Solar, a well-known clean energy
- Thermoelectric, used in watches
- Vibrations, used in (kinetic) watches
- Human input, home utility (piezoelectric) switches

Today, there is an accelerated interest in the information and communications technology (ICT) community for powering ubiquitously deployed sensor networks, mobile electronics, electric vehicles, and so on. Many things become possible as this technolgy improves.

4.3 Connect: Via Pervasive Networks

The communications layer is the foundational infrastructure of IoT. There are two major communication technologies: wireless and wired (or wireline). Each category has broadband and narrowband, packet and circuit switched, as well as short-range and long-range communications. The penetration and traffic of U.S. wireless data subscribers in 2013 will reach the same level of broadband wired household usage in 2008 [215]. The mobile Internet is catching up quickly, thanks to the development of the Internet of Things and the flexibility of wireless communications.

Today's communications environment is a complex mix of wired and wireless networks employing circuit-switched (CS) and packet-switched (PS) technology. Developments are taking place in all four sectors and there is competition between different stakeholders, fixed mobile convergence (FMC) being an obvious example. We therefore have a communications environment that is complex [64]. We need a next-generation network (NGN), which has more than the ability to transition between circuit- and packet-switched networks. The general idea behind the NGN is that one network transports all information and services (voice, data, and all sorts of media such as video) by encapsulating these into packets, similar to those used on the Internet. NGNs are commonly built around Internet protocol, and therefore the term all-IP is also sometimes used to describe the transformation toward NGN. For example, the 3GPP long-term evolution (LTE) is a standard for wireless communication of high-speed data. It is based upon GSM/EDGE and UMTS/HSPA network technologies. One of the most important features of LTE is that it will be an all-IP flat network architecture including end-to-end QoS, provisions for low-latency communications.

With the growing abundance of embedded IoT systems comes the increased pressure at the edge of the network: multiple access methods must be accommodated, implying the need for a common underlying converged core IP/MPLS (multi-protocol label switching) network. A high-level graphic view of next-generation all-IP networking is described by Emmerson [64]. The connectivity domain enables broadband access, both wired and wireless. It also includes the transport and aggregation network. This part of the all-IP network supports various access technologies using copper lines, optical fiber, and air as transmission media.

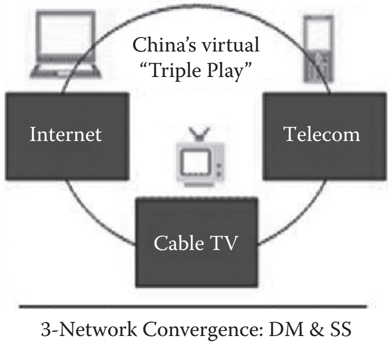

Figure 4.4 Triple network convergence.

The Chinese government has been actively pushing for the convergence of the country's three big networks—the Internet, telecom networks, and TV broadcasting networks—via various measures, most notably through the Triple Network Convergence Plan (Figure 4.4) it laid out early in 2010.

While the Triple Network Convergence Plan reiterates many government policies set out previously, one area that is expected to have significant effects on the market is the government's step to grant permission for TV broadcasting firms and telecom carriers to enter and do business in each other's realms. Local scholars estimate that triple network convergence will induce investment and consumption to 700 billion RMB (about US$103 billion), leading to widespread concern over the policy's effect on the development of related industries and various parties.

The fusion of the three networks is expected to start from business- or policy-level convergence, to application-level convergence, and finally to technological-level convergence, when the all-IP NGN vision is implemented. At that time, many good things will happen; for example, ubiquitous M2M devices can be used as cell phones, so no SIM card will be required for making a phone call.

There is no doubt that if all-IP is a reality, it will give the Internet of Things a huge lift and make the IoT dream come true much easier and faster. As an example, in the building automation industry, all-IP networking will simplify the integration work enormously, without having to deal with various field bus network protocols, OLE for process control (OPC) middleware, and so on.

Internet Protocol version 6 (IPv6) is a version of the Internet protocol that is designed to succeed Internet Protocol version 4 (IPv4). The Internet operates by transferring data in small packets that are independently routed across networks as specified by the Internet protocol. Since 1981, IPv4 has been the publicly used IP, and it is currently the foundation for most Internet communications. The Internet's growth has created a need for more addresses than IPv4 has (32 bits). IPv6 allows for vastly more numerical addresses (128 bits), but switching from IPv4 to IPv6 may be a difficult process [216].

The Internet world is getting ready for the big change from IPv4 to IPv6. After the change, everything, every duct on the planet, could have a fixed IP address, which would have an enormously huge impact on the Internet of Things on all aspects.

However, as a side note, countries such as the United States are not eager to make the change from IPv4 to IPv6 compared with countries such as China and India, because more IPv4 addresses were allocated to the United States and Europe. It's rumored that a university such as Massachusetts Institute of Technology received more IPv4 address allocation than the entire country of China or India. That's why countries such as China have developed other protocols such as IPv9 in an effort to get more IP addresses [65].

When talking about IoT, wireless communications is the topic most of the times, because three (M2M, RFID, and WSN) of the four IoT pillars are based on wireless. However, most of the systems in industrial automation, building automation, and so forth are built using SCADA technology on wired short-range field bus and long-range TCP/IP networks. The development of the Internet of Things, for the time being, should cover both wired and wireless networks, just as Axeda, the device relation management software product and service provider, did in its product and service portfolio before or after the all-IP convergence and IPv6.

4.3.1 Wired Networks

Wired networks for IoT can be categorized as short-range field bus–based access networks, mostly for SCADA applications, and IP-based networks, for M2M and SCADA applications.

The IP-based networks are widely used and their protocol stack is well known, as shown in Figure 4.5, together with telephony SS7 and cable TV DOCSIS (data-over-cable service interface specification) protocols, the triple (Internet, telephony, and cable TV) networks convergence plan candidates. SS7 (Signaling System 7) is a critical component of modern telecommunications systems (PSTN, xDSL, GPRS, etc.). Every call in every network is dependent on SS7. Likewise, every mobile phone user is dependent on SS7 to allow inter-network roaming. SS7, a form of packet switching, is also the "glue" that sticks together circuit-switched (traditional) networks with Internet protocol–based networks.

DOCSIS is an international standard that permits the addition of high-speed data transfer to an existing cable TV

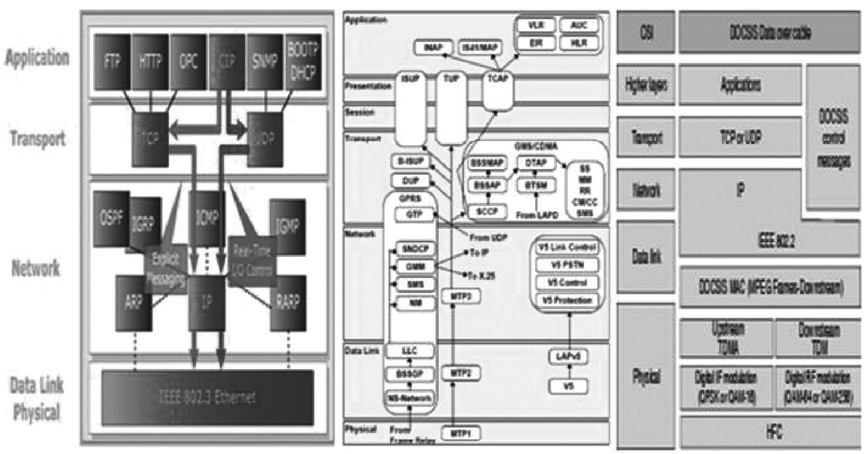

Figure 4.5 Protocol stacks of the "three networks."

system. It is employed by many cable television operators to provide Internet access over their existing HFC (hybrid fiber-coaxial) infrastructure.

A complex automated industrial system, such as a manufacturing assembly line, usually needs an organized hierarchy of controller systems to function. In this hierarchy [217,218], there is usually a SCADA/HMI (Human–Machine Interface) at the top, where an operator can monitor or operate the system. This is typically linked to a middle layer of programmable logic controllers (PLC) via a non-time-critical communications system (e.g., Ethernet). At the bottom of the control chain is the field bus (could run on top of a different power line communications network too) that links the PLCs to the IoT device components that actually do the work, such as sensors, actuators, electric motors, console lights, switches, valves, and contactors.

More details on field bus and its relevance to IoT are described here because this information is currently often neglected in most of the materials about IoT. Field bus is the name of a family of industrial computer network protocols used for real-time distributed control, now standardized as IEC 61158. The IEC 61158 standard includes eight different protocol sets called types:

- Type 1 Foundation field bus H1
- Type 2 ControlNet
- Type 3 PROFIBUS
- Type 4 P-Net
- Type 5 FOUNDATION field bus HSE (high-speed Ethernet)
- Type 6 SwiftNet (a protocol developed for Boeing, since withdrawn)
- Type 7 WorldFIP
- Type 8 Interbus

There is a wide variety of concurring standards. Table 4.2 provides a comprehensive list of wired field bus standards or protocols used with SCADA systems for industrial automation.

Table 4.2 List of Field Bus Standards

Protocol Group	*Protocols/Field Buses*
Automatic meter reading	DLMS/IEC 62056
	ANSI C12.18
	IEC 61107
	Modbus
	M-Bus
	U-SNAP [191]
Automobile/vehicle	Local Interconnect Network (LIN)—a very low cost in-vehicle sub-network
	Controller Area Network (CAN)—an inexpensive low-speed serial bus for interconnecting automotive components
	J1939 and ISO11783—an adaptation of CAN for agricultural and commercial vehicles
	FlexRay—a general purpose high-speed protocol with safety-critical features
	Media Oriented Systems Transport (MOST)—a high-speed multimedia interface
	Keyword Protocol 2000 (KWP2000)—a protocol for automotive diagnostic devices
	Vehicle Area Network (VAN)
	DC-BUS—automotive power-line communication multiplexed network
	IDB-1394
	SMARTwireX
	J1708—RS-485 based SAE specification used in commercial vehicles, agriculture, and heavy equipment
Building, home automation	Wire—from Dallas/Maxim
	BACnet—designed by committee ASHRAE

Table 4.2 (continued) List of Field Bus Standards

Protocol Group	*Protocols/Field Buses*
	S-Bus
	C-Bus
	CC-Link Industrial Networks, supported by Mitsubishi Electric
	DALI
	DSI
	Dynet
	HomePlug—power line home networking
	HomePNA—phone line home networking
	ITU-T G.hn—a way to create a high-speed (up to 1 Gbit/s) LAN using existing home wiring (power lines, phone lines, and coaxial cables)
	Konnex (KNX)—previously AHB/EIB
	LonTalk—protocol for LonWorks by Echelon Corporation
	Modbus RTU or ASCII or TCP
	oBIX—OASIS Standard
	xAP—Open protocol
Industrial control system	MTConnect
	OPC
	OPC UA
	AS-Interface (Actuator Sensor Interface)—an industrial networking solution used in PLC, DCS, and PC-based systems
	SafetyBUS p—a standard for safe field bus communication within factory automation. It meets SIL level SIL 3 according to IEC 61508 and safety category Cat. 4 of EN 954-1

continued

Table 4.2 (continued) List of Field Bus Standards

Protocol Group	*Protocols/Field Buses*
Power system automation	IEC 61850
	IEC 60870-5
	DNP3—Distributed Network Protocol
	Modbus
	Profibus
	IEC 62351—security for IEC 60870, 61850, DNP3, and ICCP protocols
Process automation	DF-1
	FOUNDATION field bus—H1 & HSE
	Profibus—by PROFIBUS International
	PROFINET IO
	CC-Link Industrial Networks, supported by the CLPA
	CIP (Common Industrial Protocol)—can be treated as application layer common to DeviceNet, CompoNet, ControlNet and EtherNet/IP
	Controller Area Network—utilized in many network implementations, including CANopen and DeviceNet
	ControlNet—an implementation of CIP, by Allen-Bradley
	DeviceNet—an implementation of CIP, by Allen-Bradley
	DirectNet—Koyo/Automation Direct proprietary, yet documented PLC interface
	EtherNet/IP—IP stands for Industrial Protocol. An implementation of CIP, by Rockwell Automation

Table 4.2 (continued) List of Field Bus Standards

Protocol Group	*Protocols/Field Buses*
	Ethernet Powerlink—an open protocol managed by the Ethernet POWERLINK Standardization Group (EPSG)
	EtherCAT
	Interbus, Phoenix Contact's protocol for communication over serial links, now part of PROFINET IO
	HART
	Modbus RTU or ASCII or TCP
	Modbus Plus
	Modbus PEMEX
	Ethernet Global Data (EGD)—GE Fanuc PLCs (see also SRTP)
	FINS, Omron's protocol for communication over several networks, including Ethernet
	HostLink Protocol, Omron's protocol for communication over serial links
	MECHATROLINK—open protocol developed by Yaskawa
	MelsecNet, supported by Mitsubishi Electric
	Optomux—Serial (RS-422/485) network protocol originally developed by Opto 22 in 1982
	Honeywell SDS (Smart Distributed System)—originally developed by Honeywell; currently supported by Holjeron
	SERCOS interface—Open Protocol for hard real-time control of motion and I/O
	SERCOS III—Ethernet-based version of SERCOS real-time interface standard

continued

Table 4.2 (continued) List of Field Bus Standards

Protocol Group	*Protocols/Field Buses*
	GE SRTP—GE Fanuc PLCs
	Sinec H1—Siemens
	SynqNet—Danaher
	TTEthernet—TTTech
	PieP—Open Fieldbus Protocol
	BSAP—Bristol Standard Asynchronous Protocol, developed by Bristol Babcock Inc

The graphic (the CIP family of field bus protocols) in [219, first page] compares some of the field buses against the OSI model. In the past, automation field bus protocols have tended to be application specific, making them very efficient at what they do but limiting the roles for which they can be used, and making interoperability between the protocols used in different application areas difficult to achieve. The Common Industrial Protocol (CIP) forms the basis for a family of related technologies and has numerous benefits for both device manufacturers and the users of industrial automation systems. The first of the CIP-based technologies, DeviceNet, emerged in 1994 and is an implementation of CIP over CAN, which provides the data link layer for DeviceNet.

4.3.2 Wireless Networks

Just like the wired networks, wireless networks for IoT can be categorized as follows:

- Short-range (including near field communication [NFC], usually narrowband, and wireless PAN, LAN, and MAN) mesh networks, RFID, WiFi, WiMax, and so on;
- Long-range (via cellular networks, wireless WAN, pseudo-long-range) GSM, CDMA, WCDMA, and other networks, as well as satellite communication.

Short-range wireless mesh networks are the fundamental communication techniques of WSN and RFID. Long-range cellular networks are the foundation networks for M2M.

Radio spectrum refers to the part of the electromagnetic spectrum corresponding to radio frequencies: lower than 300 GHz (or wavelengths longer than about 1 mm). Different parts of the radio spectrum (as shown in http://www.ictregulationtoolkit.org/images/lib/Radio%20Spectrum%20in%20demand.gif) are used for different applications. The so-called sweet spot at ultra-high frequency concentrated most of the widely used frequencies. Radio spectrum are typically government regulated, and in some cases, are sold or licensed to operators of private radio transmission systems, for example, cellular telephone operators or broadcast television stations.

There are as many wireless standards as wired network protocols (Table 4.2). Before 2000, there were about five or six concurring standards, which lasted for a longer time than today's standard. Nowadays, there are more than 15 concurring wireless standards [220] and new ones keep coming, with each and every one's life span shorter than those before. Wireless communications standards can also be categorized as standards for cellular communications networks (such as GSM, CDMA, HSPA, LTE, etc.) and wireless connectivity networks (such as Bluetooth, Wifi, WiMax).

Communications standards are evolving rapidly. With the advent of the Internet of Things, it is expected that new standards will appear with even higher frequency and in larger numbers, due to requirements on wireless network improvements for machine-type communications (MTC) [66,189]. MTC is expected to be one of the major drivers of wireless communications standards in the next decade. The ETSI now has a technical committee exclusively focused on M2M; the Chinese Communications Standards Association is currently exploring the definition of M2M standards for China; and the Geneva-headquartered International Telecommunications Union (ITU) is working on "mobile wireless access systems providing

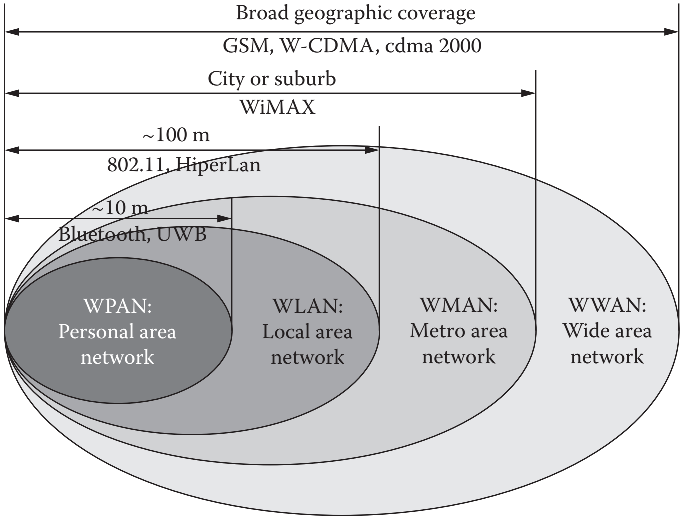

Figure 4.6 Short- and long-range wireless networks. (From Yuan Lin et al., "Baseband Processing Architectures for SDR," in Vijay Madisetti (ed.), *Wireless, Networking, Radar, Sensor Array Processing, and Nonlinear Signal Processing*, Boca Raton, FL: CRC Press, 2009.)

telecommunications for a large number of ubiquitous sensors or actuators scattered over wide areas in the land mobile service," which are at the center of the M2M ecosystem. The U.S. Telecommunications Industry Association (TIA) has also launched a new engineering committee centered on smart device communications (TIA TR-50).

Figure 4.6 shows the spectrum of wireless communications standards from short-range to long-range. RFID and NFC are parts of WPAN.

Short-range wireless sensor networks can also be treated as access networks [221] to IP-based Internet for many vertical applications such as building automation and others.

Wireless communications can be via RF, microwave (long-range line of sight via highly directional antennas, or short-range), or infrared (short-range, consumer IR devices such as remote controls). Some of the standards that have not been discussed previously are as follows:

- 6LowPAN (IPv6 over low power wireless personal area networks): a working group of IETF
- BSN (body sensor network): IEEE 802.15.6
- Broadband fixed access: LMDS, AIDAAS, HiperMAN
- DASH7: active RFID standard
- DECT (digital enhanced cordless telecommunications): cordless telephony
- EnOcean: low-power, typically battery-less, proprietary wireless technology
- HomeIR: wireless IR home networking
- HomeRF: wireless RF home networking
- IEEE 1451: a set of smart transducer interface standards by the IEEE
- InfiNET: from home automation industry leader Crestron
- INSTEON: dual-mesh technology from SmartLabs
- IrDA: from Infrared Data Association
- ISA100.11a: an open wireless networking technology standard developed by the International Society of Automation (ISA)
- Land mobile radio or professional mobile radio: TETRA, P25, OpenSky, EDACS, DMR, dPMR, etc.
- ONE-NET: open-source standard for wireless networking
- OSIAN: open-source IPv6 automation network
- TransferJet: a new type of close-proximity wireless transfer technology by touching (or bringing very close together) two electronic devices; allows high-speed exchange of data
- Wavenis: a proprietary technology by Coronis Systems in 2001. In 2008, the Wavenis Open Standard Alliance Wavenis-OSA was created to manage and govern the technology moving forward.

Apart from new standards emerging from MTC improvements, other new technologies and standards can also help in advancing the Internet of Things:

- Orthogonal frequency division multiplexing (OFDM) and orthogonal frequency division multiple access (OFDMA): two different variants of the same broadband wireless air interface. LTE is an OFDMA-based technology standardized in 3GPP. OFDM technologies typically occupy nomadic, fixed, and one-way transmission standards, ranging from TV transmission to Wi-Fi as well as fixed WiMAX and newer multicast wireless systems like Qualcomm's Forward Link Only.
- Ad hoc sensor network: a short-lived network of two or more mobile devices connected to each other without the help of intervening infrastructure. In contrast to a fixed wireless network, an ad hoc network can be deployed in remote geographical locations and requires minimal setup and administration costs. The integration of an ad hoc network with a bigger network such as the Internet or a wireless infrastructure network increases the coverage area and application domain of the ad hoc network.
- Software defined radio (SDR): SDR is the result of an evolutionary process from purely hardware-based equipment to fully software-based equipment. All functions, modes, and applications, such as transmit frequencies, modulation type, and other RF parameters, can be configured and reconfigured by software (SW) defines all waveform properties, cryptography, and applications, is reprogrammable, and may be upgraded in the field with new capabilities;
- Cognitive radio (CR): CR is a form of wireless communication in which a transceiver can intelligently detect which communication channels are in use and which are not, and instantly move into vacant channels while avoiding occupied ones. This optimizes the use of available RF spectrum while minimizing interference to other users. SDR is a required basic platform on which to build a CR. SDR and CR extend the software and middleware capabilities a

step further into the communicating devices and increase the ubiquity, versatility, and smartness of devices in the Internet of Things.

4.3.3 Satellite IoT

A communications satellite (COMSAT) is a specialized wireless transponder in space, receiving radio waves from one location and transmitting them to another (also known as a *bent pipe*). Hundreds of commercial satellites are in operation around the world. These satellites are used for such diverse purposes as wide-area network communications (to ships, vehicles, planes, as well as hand-held terminals and phones), weather forecasting, television and radio broadcasting, amateur radio communications, Internet access, and the global positioning system (GPS). Satellites have many important uses other than communications; for example, weather reports rely on satellite information, and GPS works because of a linked set of satellites. Satellite communications are especially important for transportation, aviation, maritime, and military use.

Modern communications satellites use a variety of orbits:

- GEO: Geostationary Earth Orbit, 120 satellites maximum, examples include Inmarsat (4 + 5 Satellites)
- MEO: Medium Earth Orbit, examples include the GPS satellite constellations
- LEO: Low (polar and nonpolar) Earth Orbit (theoretically unlimited); examples are Iridium (66 satellites; rent for global Iridium satellite phones is as low as $24.95 per week shown on the company's website), ORBCOMM (30 satellites), Globalstar (48), ICO (10 + 2), Ellips0 (17), Teledesic (288 satellites); constellations of satellites required for coverage
- ELI: Elliptical Orbit
- Molniya Orbit and HAPs (high-altitude platforms)

The satellite industry is a subset of the telecommunications and space industries. According to a SIA (Satellite Industry Association) report [67], the worldwide revenue of the satellite industry was $168.1 billion in 2010.

It's obvious that satellite technologies (other than positioning-oriented global navigation satellite system or GPS, which will be discussed in Chapter 6 of the book) can be used for IoT applications (such as M2M, SCADA, and telemetry) just like cellular networks, with better coverage in remote areas.

When people think of M2M communication, they usually think of cellular networks. For vehicles that move in urban areas or on major highways, cellular coverage is usually good enough, but what about construction equipment at remote locations, agricultural equipment, or ships? That's where satellite communication comes into play.

There are two issues about satellite communications: speed and cost. Although satellites can transmit large amounts of data, like Direct TV, this is done primarily one-way and to a large antenna. Two-way transmission to a small antenna has a much lower bandwidth capability than cellular communication. And the cost per byte of satellite communication is much more expensive. But if you have an application with small data requirements and broad coverage needs, satellite pricing can be very competitive.

Another option is dual-mode devices. This combines satellite and cellular in a single-edge device, giving you the best of both worlds. For example, the Axeda SmartLink platform is designed to handle dual-mode communication (via partnership with ORBCOMM) that switches between the communication modes based on price and urgency. Basic status information can be saved locally and then sent when a cellular connection is available, but an emergency condition could be sent immediately by the most economic means available.

ORBCOMM Inc. also provides M2M services to customers such as Caterpillar and Volvo Trucking, in industries ranging from commercial transportation to heavy equipment, industrial fixed assets, and marine/homeland security to track, monitor, and control their mobile and fixed assets. With ORBCOMM, these companies monitor everything from trucks and railcars to marine vessels, which are often in areas beyond the reach of terrestrial systems. ORBCOMM has deployed an M2M services portal that relies on Sierra Wireless AirVantage™ Services Platform and gives ORBCOMM's customers the ability to seamlessly track and manage their equipment around the world, even over the ocean.

In a report titled "World Satellite Machine-to-Machine Communications Market," Frost and Sullivan finds that the market earned revenues of $726 million in 2009. It estimates that this number will reach $1.90 billion in 2016. The United States dominates the world satellite M2M communications market with 62 percent market share. The Asia-Pacific region is expected to experience maximum growth in the long term. Major satellite market participants include Iridium, Inmarsat Standard C, Satamatics, SkyWave, Globalstar, Qualcomm Omnitracs, ORBCOMM, Skybitz, Wireless Matrix, and Thuraya.

Network Innovations provides a suite of mobile and stationary satellite communications solutions for wireless SCADA/telemetry data communications that operate globally. Dedicated, satellite-based business communications using relatively small dish antennas or very small aperture terminals (VSATs) are no longer only for governments and colossal corporations. An industry study predicted in 1990 that SCADA services would become a market for VSAT technology by the mid-1990s, which did happen. VSAT SCADA is now an important tool in the oil, pipeline, and electric utility markets, fulfilling the prediction. The global SCADA/M2M/LDR (low data rate) market is projected to reach US$3 billion by 2018 based on data published in April 2011 by Northern Sky Research, LLC. An example satellite SCADA system for monitoring and controlling a city's fresh water supply system is available [222].

4.4 Manage: To Create New Business Value

The previously described first two stages of the DCM model show the processes and venues of how the information is captured from various types of devices and how this information is aggregated via various gateways and transported across access networks and the core backbone to the central servers. The machine-generated information comes in large volumes much bigger and faster than information generated by humans; however, much of the data are of low value or even noises, which must be filtered out by middleware at the edge as described before in the RFID sections. And then those preprocessed data are transformed into high-value information via a cognitive application platform, most of the times a high-performance cloud computing (or high-throughput computing) platform.

In the current customer-driven, technology-based environment, it is no longer enough to offer a service or product and expect it to satisfy your customers. Even if you have the best customer service in the industry, you have to be able to extend out your offerings to meet current demand to keep the customers satisfied. The Internet of Things brings enormous possibilities and potentials for creating new business value and generating new revenue ecosystems with data processing and managing rules that combine intelligence from remote assets unreachable before with your intelligent enterprise systems.

With IoT, more and more areas of the real world become part of the ICT world, as shown in http://consen.org/node/9 from the IoSS (Internet Architecture for Optimization Sensing Systems) project in Europe. Disruptive applications beyond current imagination will appear. Smart grid, connected car, fleet control, mobile surveillance, and remote monitoring are listed as the top five disruptive applications out of a total of 65 identified, according to reports from the Boston Consulting Group. All of the top five are IoT applications. For example, with the wide use of telematics, things like total vehicle life cycle management, refined used car price estimate, Pay as

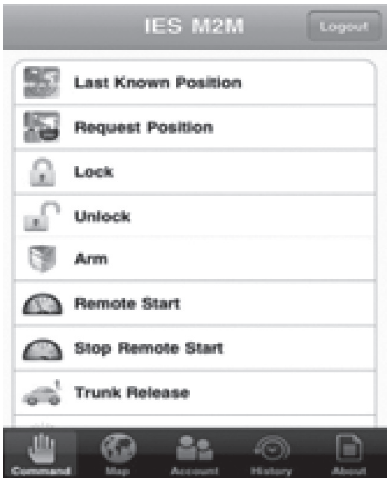

Figure 4.7 iPhone M2M application.

You Drive insurance policy, neighbor-to-neighbor car-sharing business such as those provided by startup RelayRides become possible, and the list goes on and on.

Let's take a look again at the typical capabilities of an M2M platform and how they support the business of a mobile operator or an M2M enabler/partner. With those functions and roles (as shown in http://machine2twomachine.files.wordpress.com/2011/08/fig-16.jpg [265]), both the mobile operator and the M2M partner can attain additional revenue by offering advanced services to their M2M partners (Figure 4.7). For example, the M2M platform and the fleet management system the author's team built for China Mobile utilize its existing Operation Support System/Business Support System (OSS/BSS) for SIM card issuing, billing, and other services, and China Mobile collects the revenue from the customers and shares it with us. China Unicom has also built and operates a telematics service support platform on top of their OSS/BSS, aiming to provide foundation services to a variety of TSPs (telematics service providers).

M2M applications that can be linked inside the network to people's existing mobile subscriptions offer mobile operators enormous advantages in the competitive M2M marketplace. Using smartphones as connected portable navigation devices is such an example of potentially great market growth opportunity. The application stores' model of Apple and Google Android has turned smartphones into M2M terminals. One example is the application from Portman Electronics Ltd.'s IES iPhone M2M Tracking System. It is a real time GPS/GSM/GPRS tracking service. Another example of nonoperator vendor is SeeControl, who empowers you to use sensors, GPS trackers, barcode scanners, RFID, and smart web forms to collect asset data from anywhere and manage business processes.

In the industrial automation scenario, the layering of the value chain components or subsystems looks as depicted in Figure 4.8. One of the major issues has been or still is that

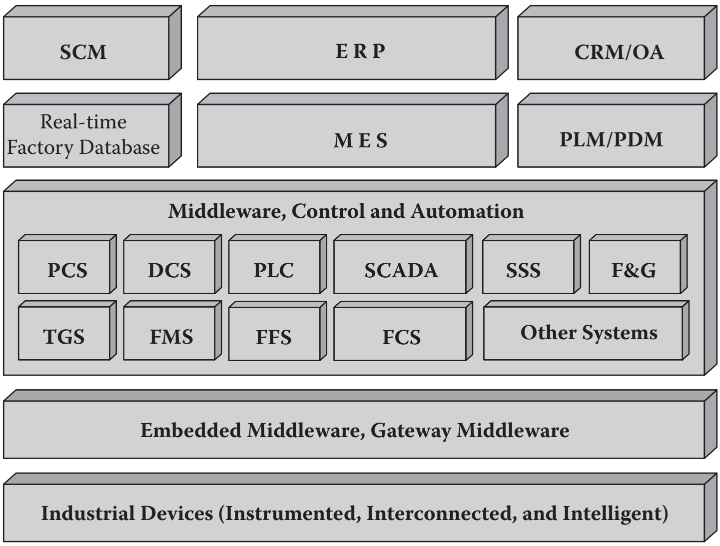

Figure 4.8 The industrial automation stack. FCS = Field Bus Control System; DCS = Distributed Control System; PLC = Programmable Logic Controller; SCADA = Supervisory Control and Data Acquisition; TMS = Tank Management System; FMS = Flow Metering System; F&G = Fire and Gas; SSS = Safety Shutdown System; FFS = Firefighting System; MES = Manufacturing Execution System; ERP = Enterprise Resource Planning.

most of these subsystems are not integrated; operators have to deal with various subsystem interfaces to run the operation. Sometimes, the factory database has to be manually keyed in to the IT database. When you want to expand and/or integrate the entire plant, you will need a solution provider with the expertise to provide the solution for you.

Before the advent of IoT or perhaps at the same time, people found out that efficient plant operations require the total integration of the field devices to the subsystems, then the integration of subsystems into a single centralized SCADA system that provides a single user interface or HMI. This is also where the new IoT system fits and sits. On top of this, those subsystems are further integrated into the MES and ERP as well as SCM, WMS, and other systems. All of those happen within an enterprise, it's an Intranet of Things ecosystem.

The vision of IoT augmented with advances in software technologies and methodologies such as SOA (service-oriented architecture), SaaS (software as a service), cloud computing, and others is causing a paradigm shift where devices can offer more advanced access to their functionality and business intelligence. As such, event-based information can be acquired, and then processed on-device and in-network. This capability provides new ground for approaches that can be more dynamic and highly sophisticated and that can take advantage of the available context. Cross-layer collaboration is expected to be a key issue in such a highly dynamic and heterogeneous infrastructure such as the Real World Internet (RWI) or IoT [68]. Device relation management and intelligent device management are some of those cross-layer M2M paradigms or product concepts proposed by Axeda and Questra a few years ago, and now those products and services are serving more and more customers.

As mentioned before, the three layers of DCM are not the run-time architecture of an IoT system, but a gross classification of the IoT value chain. For an MNO or network operator in general, IoT system architecture consists of the following seven layers [70], and the focus is on network infrastructure and service capabilities similar to those provided by telcos' existing Business and Operations Support System (BOSS).

1. M2M applications
2. M2M service capabilities
3. Core network
4. Access network
5. M2M gateway
6. M2M LAN
7. M2M devices

For other parties in the IoT value chain, the diagrams from ETSI and Digi International [69] demonstrated more generic IoT system architectures. The key is to have a single common platform that can be used for all kinds of vertical applications of IoT. The data-collecting layer of IoT, from the last mile WSNs and the gateway, to the access networks, and finally to the core network, can be distributed and replicated (and, of course, there may be cross-layer connections and Intranet of Things systems which are treated as subsystems). However, the layers above the core network should be highly integrated and centralized on top of a single common (platform as a service) PaaS + SaaS platform agnostic of and accommodating the variations of the connectivity including the IaaS (infrastructure as a service) layers.

The discussion of the PaaS + SaaS middleware layer is the focus of this book, which will be covered in more detail in the followed chapters.

In China, companies such as Datang, ZTE, and Huawei have also done extensive research on IoT/M2M because the Internet of Things is highly visible in the Chinese government and many grants have been allocated to sponsor such research activities. The sample architecture diagrams in Figure 4.9 are from Datang and ZTE.

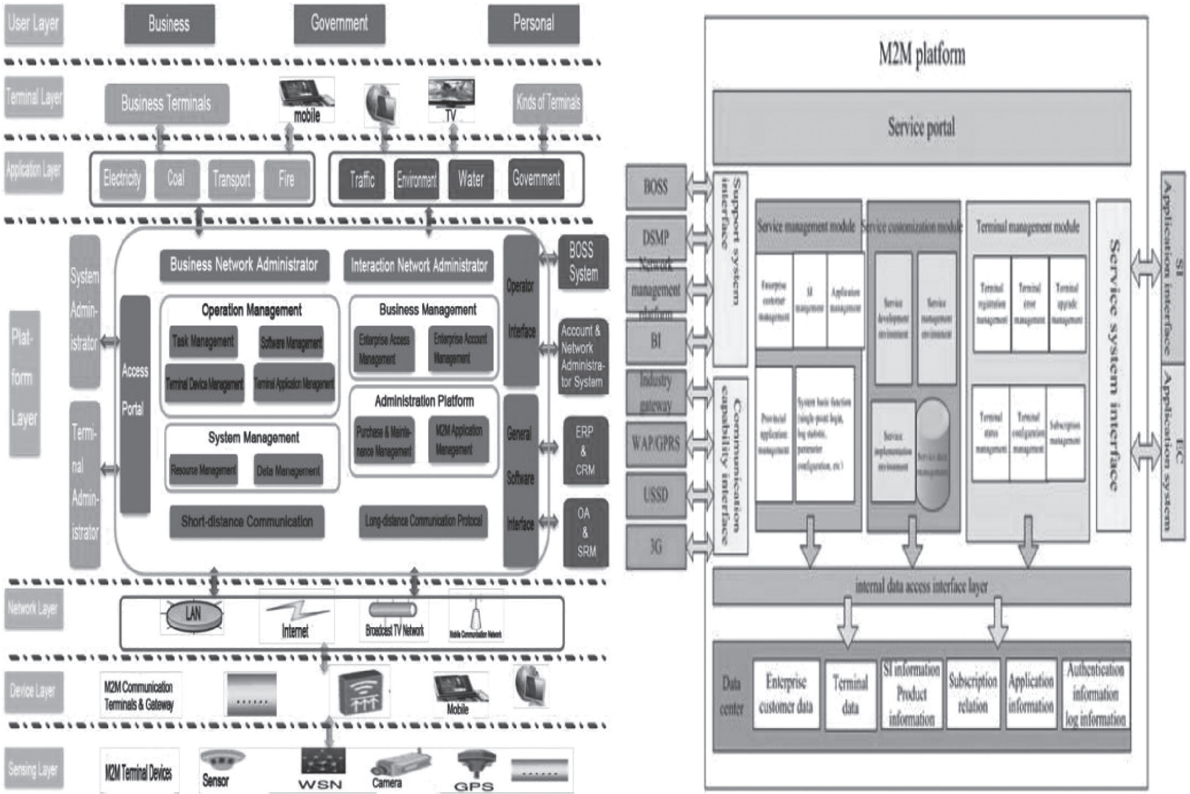

Figure 4.9 Unified IoT architecture efforts in China.

4.4.1 More Ingredients: LBS, GNSS, RTLS, and Others

Other technologies and components are widely used and required in IoT applications; however, those ingredients are not needed for all IoT systems at all times. According to SRI Consulting Business Intelligence, the technologies of the Internet of Things are summarized in Table 4.3. In the Building Blocks column we have discussed almost all of the IoT technologies, which is the goal of this book, except the Location Technology, which must be covered. Positioning capabilities and location-based services (LBS) are required for all mobility IoT applications such as telematics, fleet management, assets tracking in supply chain, and so on.

Table 4.3 IoT Technologies

Enabling Building Blocks	*Synergistic Technologies*
These technologies directly contribute to the development of the IoT.	*These technologies may add value to the IoT.*
Machine-to-machine interfaces and protocols of electronic communication	Geotagging/geocaching
Microcontrollers	Biometrics
Wireless communication	Machine vision
RFID technology	Robotics
Energy-harvesting technologies	Augmented reality
Sensors	Mirror worlds
Actuators	Telepresence and adjustable autonomy
Location technology	Life recorders and personal black boxes
Software	Tangible user interfaces
	Clean technologies

LBS is a type of context-aware computing, a term first introduced by Schilit in 1994 [71]. In 1996, the Federal Communications Commission issued the order for enhanced-911 (E-911) to provide the location of wireless callers using 911 emergency services, resulting in significant development in wireless location technologies and later location-based services. LBSs enable a customer to see the location of its devices in real time and retrieve basic information such as whether the device is registered as well as the history of data sessions. This valuable information enables the customer and the M2M solution providers to determine if the device is functioning as intended and its exact location. Should a service call, such as a part change, become necessary, they have the means to quickly and accurately locate the device. LBS can enhance the stickiness of any M2M/IoT application, especially for highly mobile solutions; new business lines and incremental revenue streams can be realized using LBS [182] creatively. A group of startups such as FourSquare, Gowalla, Loopt, myTown, BrightKite, Rummble, and others as well as Google's Latitude are providing innovative LBS services.

LBSs work using one or more of a combination of three technology protocols to determine a device's location. If the device has a GPS chip and line of sight to the navigation satellites, GPS provides the most accurate location: 15 to 100 feet. Should a pure GPS reckoning not be available due to atmospheric conditions or line-of-sight issues, assisted GPS or differential GPS will be used, providing a hybrid of satellite and cell tower location–based information, resulting in accuracy of 15 to 50 feet. If a device does not have any type of GPS technology, then enhanced cell ID will be used, which will triangulate the location of the device according to the nearest cell towers and the relative signal strength between them. This method has an accuracy of 500 to 800 feet, although it can be less accurate in more rural areas where fewer cell towers exist. More information on the major locating technologies, their accuracies, and their implementation cost range can be found in McBeath [223].

A global navigation satellite system (GNSS) is a system of satellites that provides autonomous geospatial positioning with global coverage. It allows small electronic receivers to determine their location (longitude, latitude, and altitude) to within a few meters using time signals transmitted along a line of sight by radio from satellites. Such satellites are often medium earth orbit communications satellites (discussed in the last section) that are also used for M2M communications.

The U.S. NAVSTAR GPS was the only fully operational GNSS before October 2011. The Russian GLONASS (Global Orbiting Navigation Satellite System) achieved full global coverage in October 2011 after the successful launch of the latest GLONASS satellite. China is in the process of expanding its regional Compass (Beidou) navigation system into a GNSS by 2020. The European Union's Galileo positioning system is a GNSS in initial deployment phase, scheduled to be fully operational by 2020 at the earliest. All of those GNSS satellites use CDMA for communications. The Indian Regional Navigational Satellite System is an autonomous regional satellite navigation system being developed by Indian Space Research Organization. Other countries such as France and Japan are also developing their own GNSSs.

A local positioning system (LPS) is a navigation system that provides location information in all weather, anywhere within the coverage of the network where there is an unobstructed line of sight to three or more signaling beacons of which the exact position on Earth is known. Beacons include cellular base stations, Wi-Fi access points, RFID readers, radio broadcast towers, and so on. In the past, long-range LPSs have been used for navigation of ships and aircraft. Examples are the Decca Navigator System and LORAN. Nowadays, LPSs are often used as complementary or alternative positioning technology to GPS, especially in areas where GPS does not reach or is weak, for example, inside buildings or urban canyons.

A special type of LPS is the real-time locating system (RTLS), which uses simple, inexpensive badges or tags attached to the objects, and readers receive wireless signals from these tags to determine their locations. According to IDTechEx, the market for RTLS is $380 million in 2011 rising to $1.6 billion in 2021.

A wide variety of wireless systems can be leveraged to provide real-time locating including active RFID, infrared, low-frequency signpost identification, ultrasonic ranging, ultra-wideband (UWB), Wi-Fi, Bluetooth, and so on. The locating methods or algorithms include angle of arrival, line of sight, time of arrival, time difference of arrival, time of flight, received channel power indicator, received signal strength indication, symmetrical double sided–two way ranging, near-field electromagnetic ranging; and so on.

A geographic information system (GIS)—a fusion of cartography, photogrammtery (the author worked at the Institute of Photogrammetry of ETH Zurich on related research in the late 1980s), statistical analysis, and database technology—is a system designed to capture, store, manipulate, analyze, manage, and present all types of geographically referenced data. A GIS map labeled with a variety of points of interests is a fundamental tool for many vertical IoT applications. Traditionally, maps are made up only of the more permanent fixtures of the earth's surface: roads, rivers, mountains, streets, to name a few. Over the past two decades, however, the widespread availability of GPS and mapping software has changed the landscape. Today, for example, a GPS device fed by sensors can show the state of congestion of the roads in real time on a GIS, such as the INRIX traffic services, an air-traffic controller is able to see a real-time GIS map of airplane traffic, and so on. All these possibilities and more are shifting GIS from the relatively leisurely process of analyzing static data to a far more dynamic process of real-time monitoring and decision making. With the advent of the Internet of Things, GIS will involve much more real-time situation monitoring and assessment that treat information as continually changing.

4.5 Summary

In this chapter, we talked about the technological aspects of the DCM layers of the IoT value chain. The focus was on IoT-related hardware and networks. A comprehensive collection of sensors and related technologies was discussed. A greater, more detailed overview of numerous wired and wireless, short-range and long-distance communication technologies and their mapping and relevance to and enhancements (such as MTC) for the four pillar applications of IoT were provided.

A diagram from Wireless Technologies [224] depicts the participating entities of the IoT/M2M value chain.

1. The business or consumer is involved in the consumption of the service. One possible way of their influencing the IoT is in terms of the demand. Changes in demand would lead to different configurations among the players in the business, in order to generate economically viable business models.
2. The system or service operator provides the basic M2M service to the end-user. The system operator works in tandem with the network operator to provide M2M services. The service operator has a direct relationship with the end-user.
3. The network operator provides the basic communications transport network service to the service operator.
4. The application provider or developer develops M2M value-added services for a service operator to be consumed by the end-user.
5. The end-user equipment vendor provides M2M-enabled equipment. A player in this role would typically work with the systems integrator.
6. The mobile equipment vendor provides the necessary mobile infrastructure such as GSM/GPRS/3G routers for M2M communications. A player in this role would typically work with the network operator.

7. The system integrator plays a major role in providing an end-to-end M2M solution. A player in this role can be an application developer and would work with network operators, end-user, and equipment vendors.

System integrators and service operators as well as application developers are in the “M” domain, network operators and equipment vendors are in the “C” domain, and end-user equipment vendors are in the “D” domain.

In the next chapter, we will be getting to the core parts of the book and talking about middleware in general and, more importantly, its role in and relevance to IoT applications.