IOT APPLICATION DEVELOPMENT ON CLOUD PLATFORMS

(20A35602T)

UNIT 1

FOUR PILLARS OF IOT:

- The Horizontal, Verticals, and Four Pillars
- M2M: The Internet of Devices
- RFID: The Internet of Objects
- WSN: The Internet of Transducers
- SCADA: The Internet of Controllers

INTERNET OF THINGS :

The Internet of Things is a excess of technologies and their applications that provide means to access and control all kinds of ubiquitous(universal) and uniquely identifiable devices, facilities, and assets.

These include equipment that has inherent intelligence, such as transducers, sensors, actuators, motes, mobile devices, industrial controllers, HVAC (heating, ventilation, and air-conditioning) controllers, home gadgets, surveillance cameras, and others, as well as externally enabled things or objects, such as all kinds of assets tagged with RFID, humans, animals, or vehicles that carry smart gadgets, and so forth.

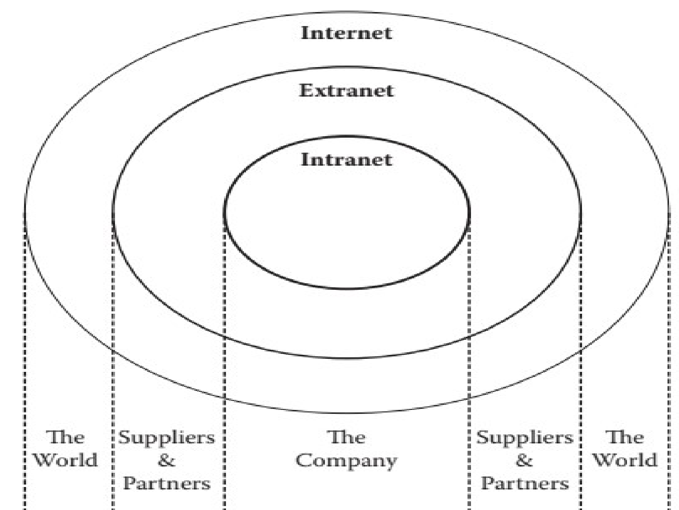


Figure 1.7 Intranet/Extranet/Internet.

Communications are via all sorts of long- and short-range wired or wireless devices in different kinds of networking environments such as Intranet, extranet, and Internet that are supported by technologies such as cloud computing, SaaS, and SOA and have adequate privacy and security measures, based on regulated data formats and transmission standards.

The immediate goal is to achieve pervasive M2M connectivity and grand integration and to provide secure, fast (real time), and personalized functionalities and services such as (remote) monitoring, sensing, tracking, locating, alerting, scheduling, controlling, protecting, logging, auditing, planning, maintenance, upgrading, data mining, trending, reporting, decision support, dashboard, back office applications, and others.

The ultimate goal is to build a universally connected world that is highly productive, energy efficient, secure, and environment friendly.

TRANSDUCER: A transducer is a device that converts energy from one form to another. Usually a transducer converts a signal in one form of energy to a signal in another.

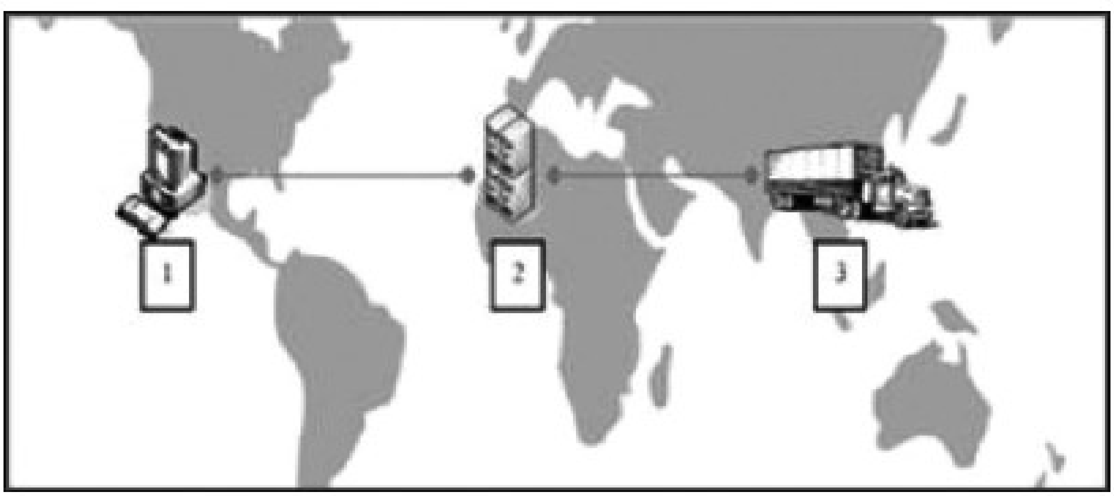
MOTE: A wireless receiver/transmitter that is typically combined with a sensor of some type to create a remote sensor. Some motes are designed to be incredibly small so that they can be deployed by the hundreds or even thousands for various applications.

RFID: Radio Frequency Identification

THE HORIZONTAL, VERTICALS, AND FOUR PILLARS :

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 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 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.

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.

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 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 secret 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, 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 gaining, and automation of industrial assets.

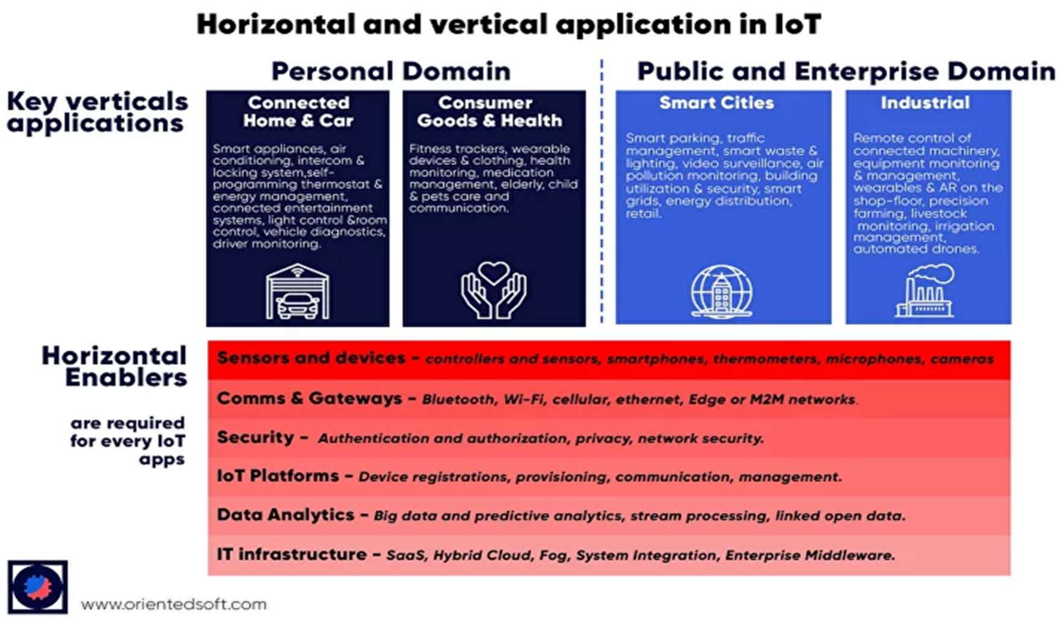
2. RFID is a data-collection technology that uses electronic tags for storing data.

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 is usually associated with industrial-, medical-, and wildlife-tracking applications that transmit small amounts of wireless data.



FOUR PILLARS OF IOT:

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):

1. 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).

2. 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.

3. 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.

4. 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.

There is much less overlap between these four pillars compared with those of the six-pillar categorizations of M2M.

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

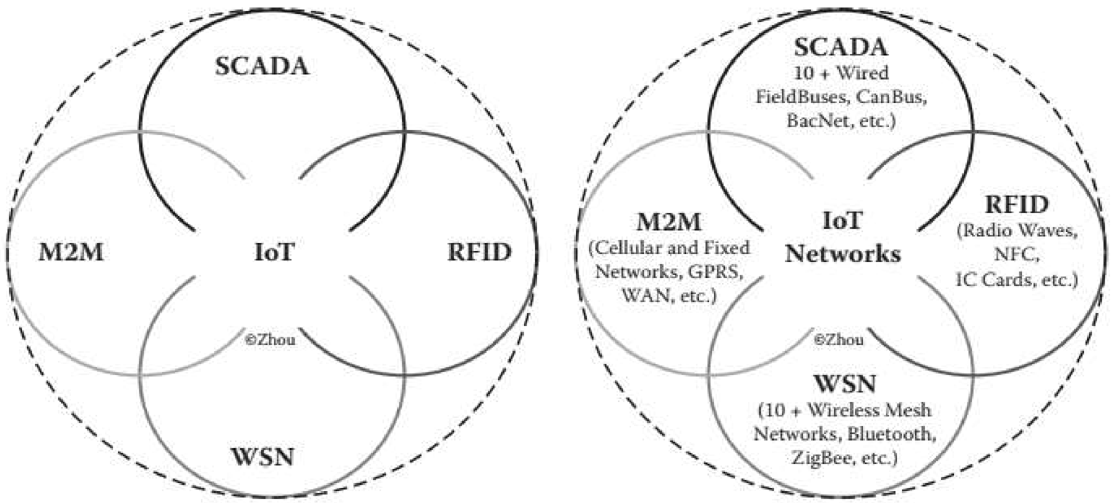


Figure 3.2 The four pillars of IoT paradigms and related networks.

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 and sharing a common platform, which can't happen if companies have to manage multiple, independent systems.

M2M: THE INTERNET OF DEVICES

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.

Two of the six pillars, remote monitoring and smart service, are features or functions of an IoT system rather than pillars.

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 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

However, there is overlap between M2M and the consumer electronics applications. The consumer electronics offerings include the following:

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

Strategy Analytics identifies five key barriers to scaling the global M2M market:

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.

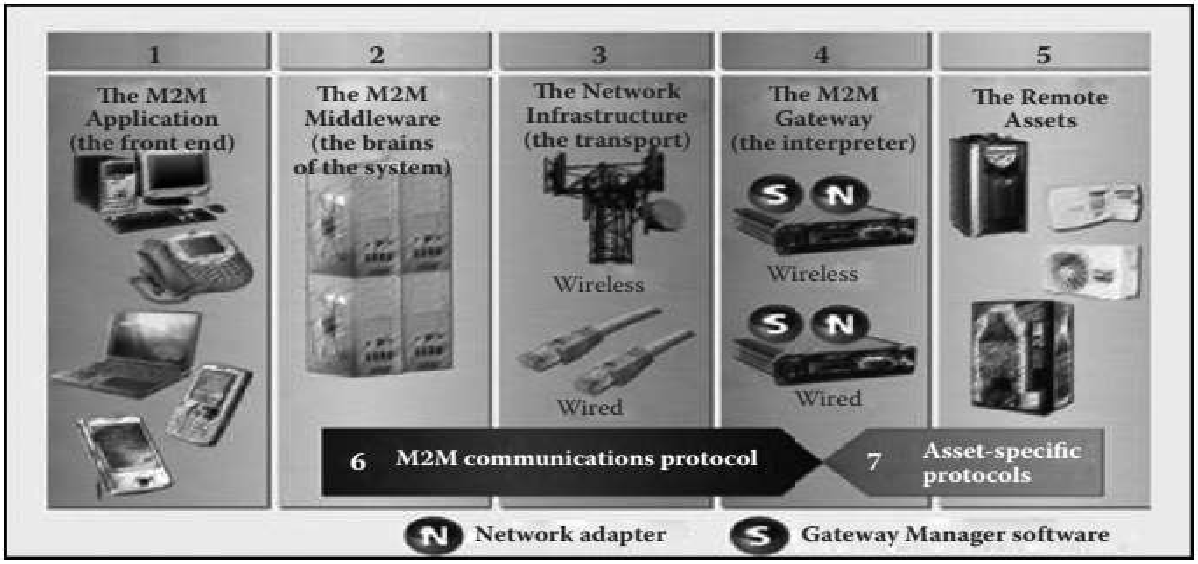


Figure 3.3 BiTX M2M architecture based on middleware.

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.

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.

Table 3.4 Operator's Participation in Value Chain

Activity in Value Chain \ Type of Entity	*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

RFID: THE INTERNET OF OBJECTS

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

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.)

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 semi passive. Passive RFID does not use a battery, while an active has an on-board battery that always broadcasts its signal. A semi passive 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 to make it an instrumented intelligent object for monitoring and tracking, while the other three (M2M, WSN, and Smart Systems) simply connect "intelligent" electronic devices.

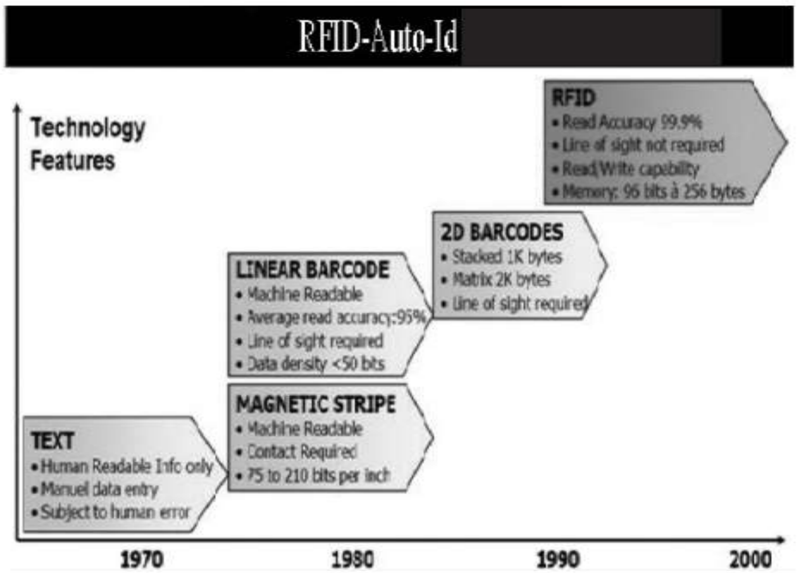


Figure 3.5 Evolution of identifications.

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).

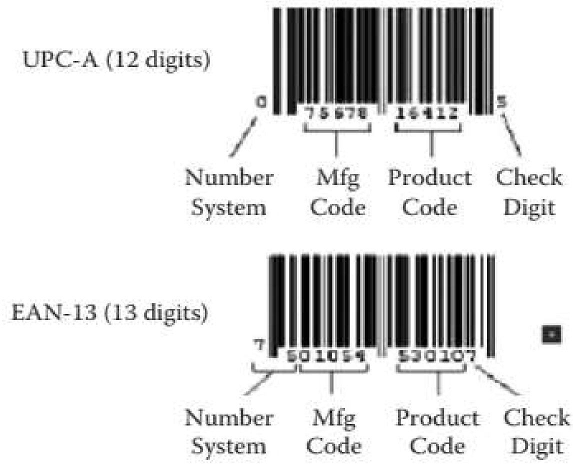


Figure 3.6 Bar code formats. (From James B. Ayers and Mary Ann Odegaard, *Retail Supply Chain Management*, New York: Auerbach Publications, 2008.)

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.

Many companies 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.

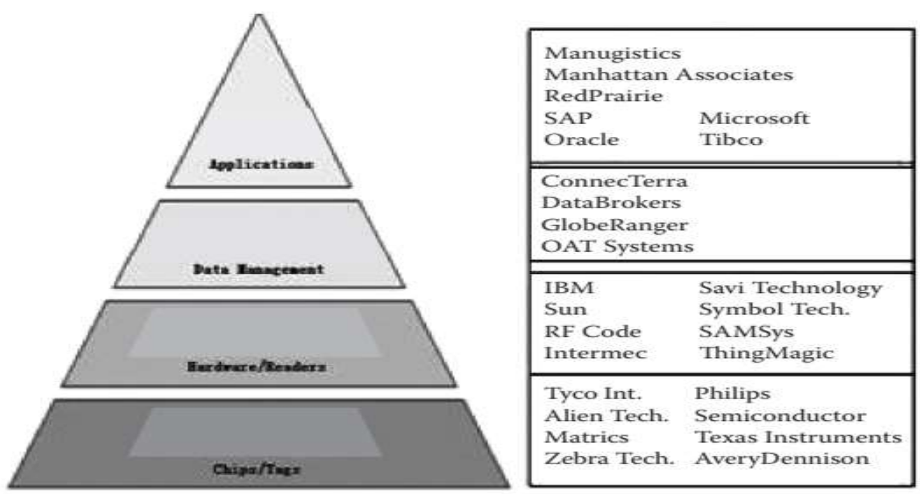


Figure 3.7 RFID value chain and vendors.

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

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 ezM2M middleware-based application system the author's team built for the Beijing Olympic Games in 2008.

Figure 3.8 Example of RFID application.

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.

WSN: THE INTERNET OF TRANSDUCERS

WSN is more for sensing and information-collecting purposes. Other networks include BSN (body sensor network), VSN (visual or video sensor network), vehicular sensor networks (V2V, V2I), underwater (acoustic) sensor networks (UW-ASN), urban/social/participatory sensor networks, interplanetary sensor networks, fieldbus networks 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.

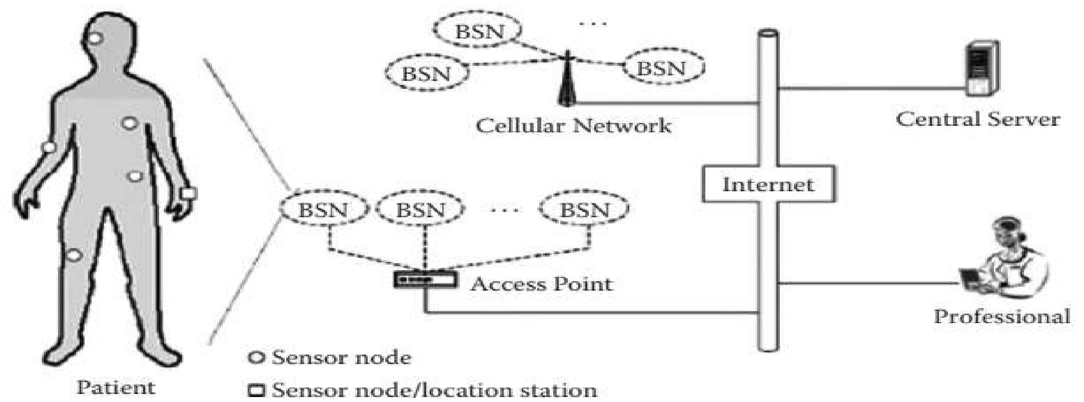


Figure 3.9 Body sensor networks. (From Hui Chen and Yang Xiao (eds.), *Mobile Telemedicine: A Computing and Networking Perspective*, New York: Auerbach Publications, 2008.)

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

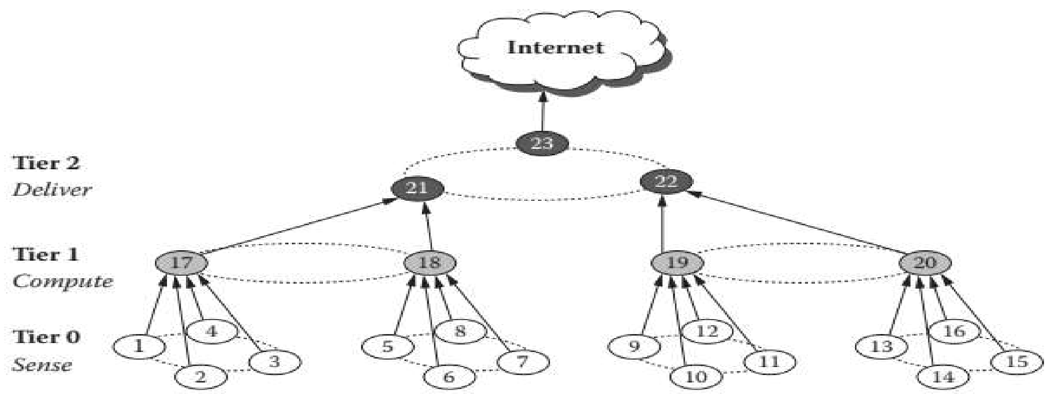


Figure 3.10 Sensor network architecture. (From Mark Yarvis and Wei Ye, "Tiered Architectures in Sensor Networks," in Mohammad Ilyas and Imad Mahgoub (eds.), *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, Boca Raton, FL: CRC Press, 2004.)

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.

Some of the existing WSN platforms are summarized in Table 3.6.

Most of the device designs are still in the research stage. 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 high-level requirements from universal 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.

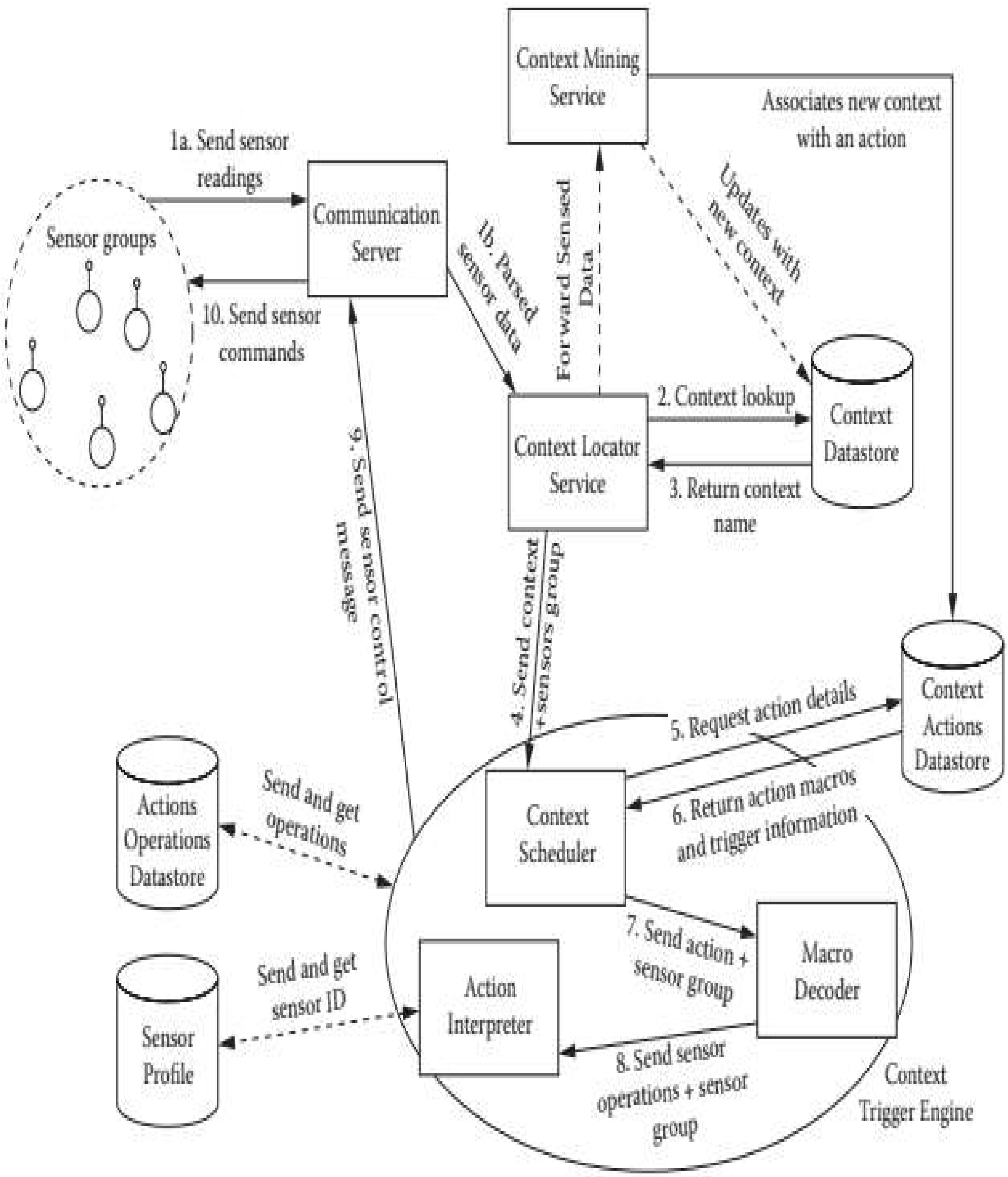


Figure 3.11 Context-aware system based on WSN. (From Seng Loke, *Context-Aware Pervasive Systems: Architectures for a New Breed of Applications*, New York: Auerbach Publications, 2007.)

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.

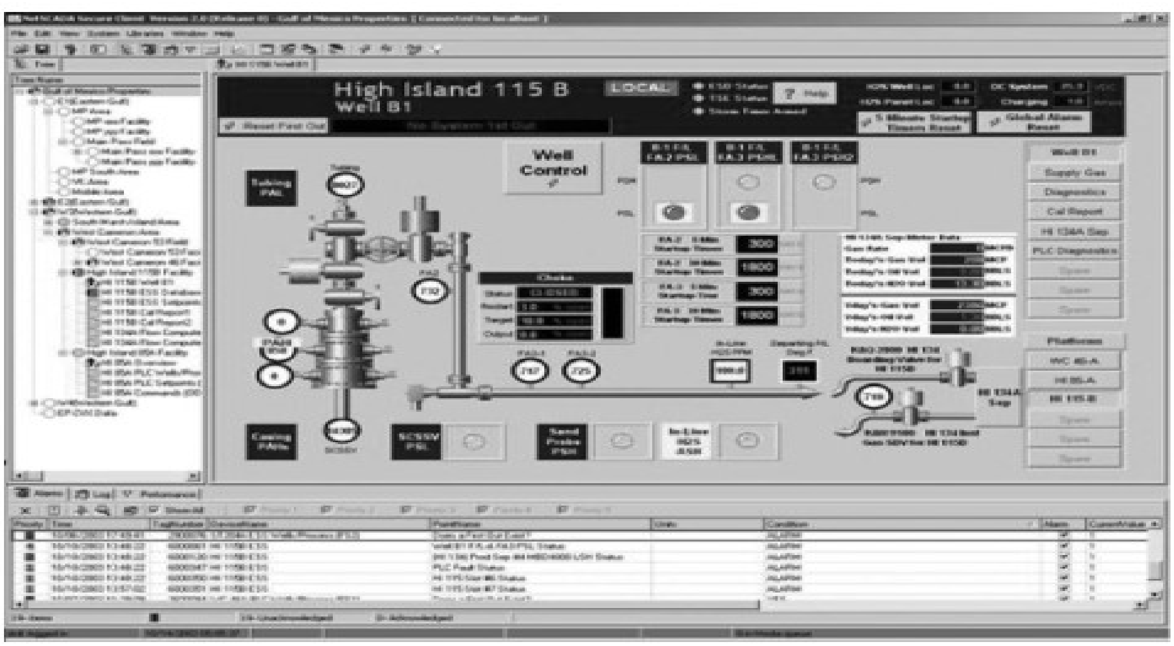
SCADA: THE INTERNET OF CONTROLLERS

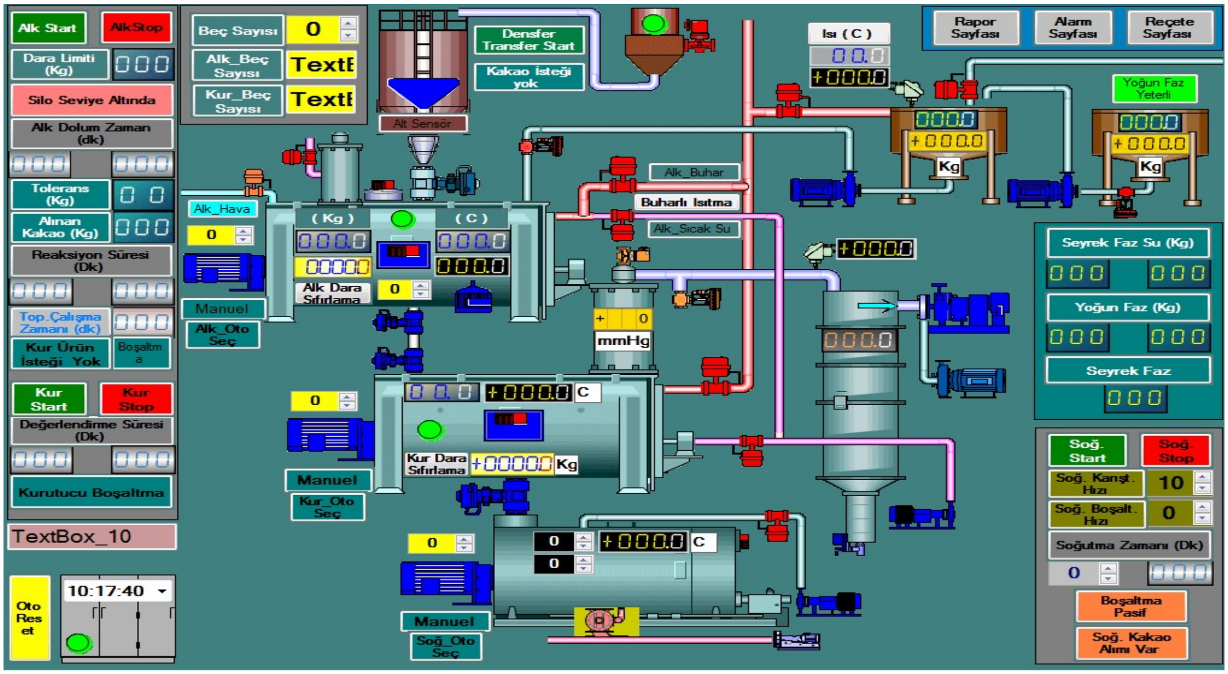
For more than a decade, many in the building industry have been seeing a day when building automation systems (BAS) would become fully integrated with communication and human interface practices and standards widely employed for information technology systems.

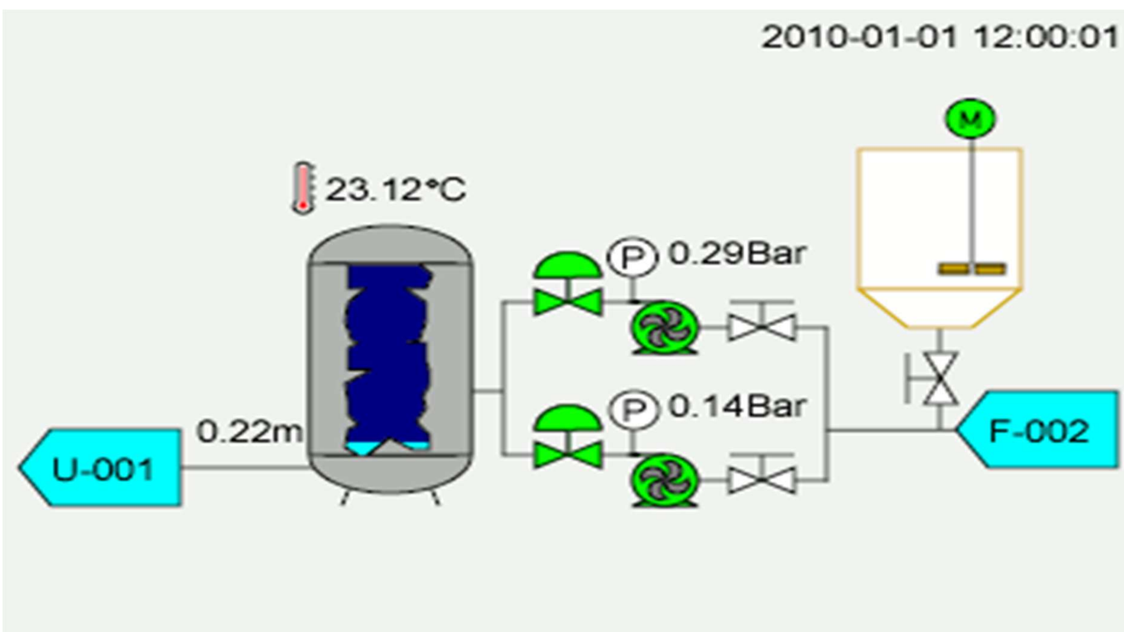
Not long ago, building automation graphical interfaces (Figure 3.12) employed almost no web-browser techniques and technologies; now, web approaches are the basis of many such packages. How close we are to a complete convergence of BAS and IT is difficult to tell, but it is not too much of a stretch to say that when the convergence is complete, there may be nothing to distinguish one from the other.

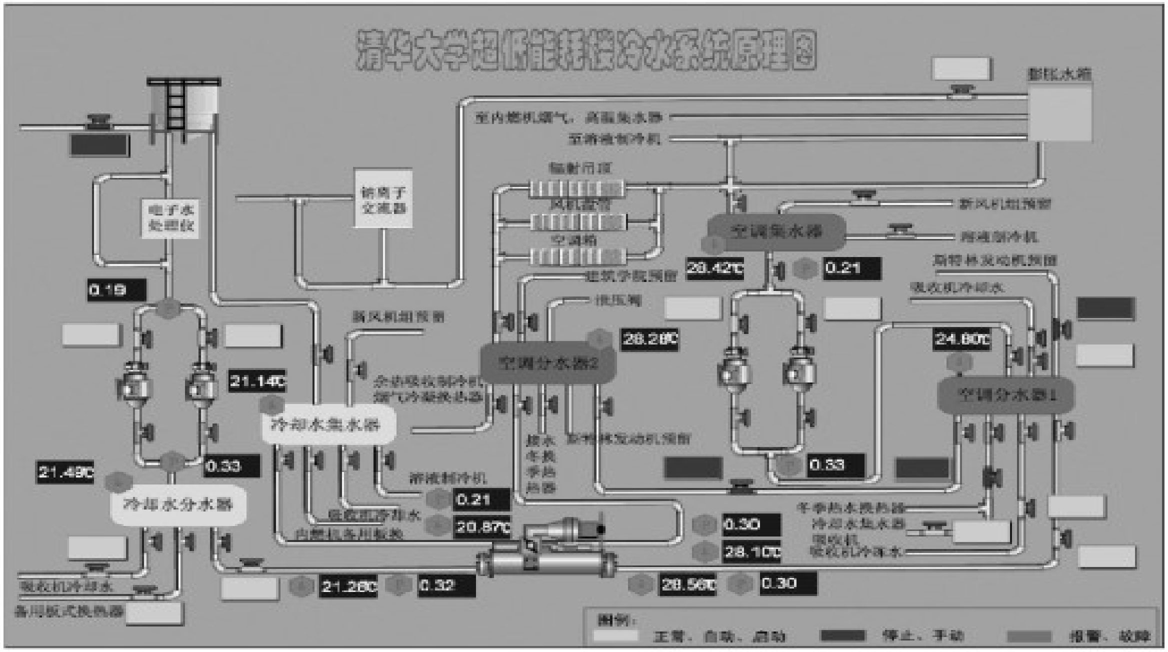
Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes. Infrastructure processes may be public or private and include water treatment and distribution, wastewater collection and treatment, 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.




Alk Start
AlkStop
Dara Limiti (Kg)
Silo Seviye Altında
Alk Dolum Zaman (dk)
Tolerans (Kg)
Alınan Kakao (Kg)
Reaksiyon Süresi (Dk)
Top. Çalışma Zamanı (dk)
Kur Ürün İsteği Yok
Kur Start
Kur Stop
Değerlendirme Süresi (Dk)
Kurutucu Boşaltma
TextBox_10
Oto Reset
10:17:40
Beç Sayısı
Alk_Beç Sayısı
Kur_Beç Sayısı
Textl
Alt Sensör
Densfer Transfer Start
Kakao isteği yok
Isı (C)
Rapor Sayfası
Alarm Sayfası
Reçete Sayfası
Yoğun Faz Yeterli
Kg
Alk_Hava
(Kg)
(C)
Alk Dara Sıfırlama
Manuel
Alk_Oto Seç
Alk_Buhar
Buharlı Isıtma
Alk_Sıcak Su
mmHg
Seyrek Faz Su (Kg)
Yoğun Faz (Kg)
Seyrek Faz
Kur Dara Sıfırlama
Kur_Oto Seç
Soğ. Start
Soğ. Stop
Soğ. Karıştı. Hızı
Soğ. Boşalt. Hızı
Soğutma Zamanı (Dk)
Boşaltma Pasif
Soğ. Kakao Alımı Var
Soğ_Oto Seç


2010-01-01 12:00:01
23.12°C
0.29Bar
0.14Bar
0.22m
U-001
F-002
M
P



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

A human–machine interface (HMI), which is the kit 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.

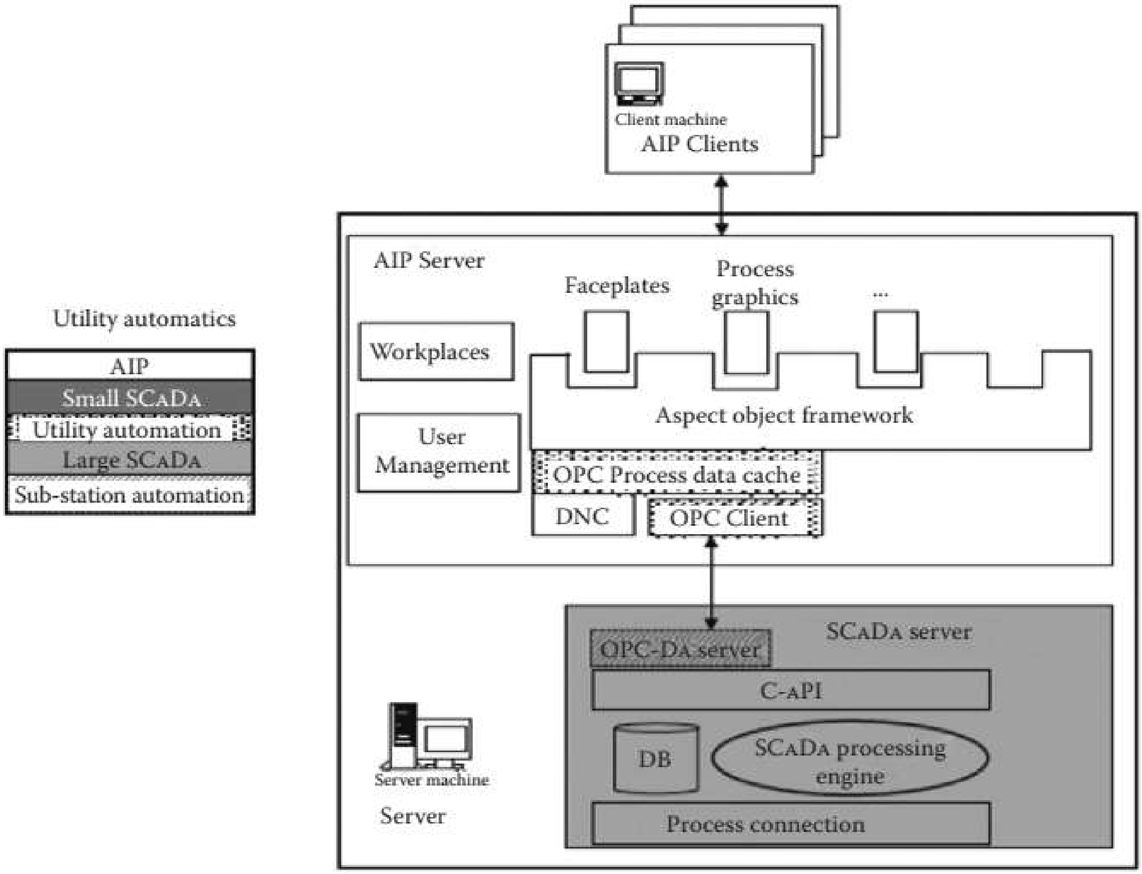


Figure 3.13 Components of a SCADA system. (From Yauheni Veryha and Peter Bort, "Industrial IT-Based Network Management," in Richard Zurawski (ed.), *The Industrial Information Technology Handbook*, Boca Raton, FL: CRC Press, 2005.)

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

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.

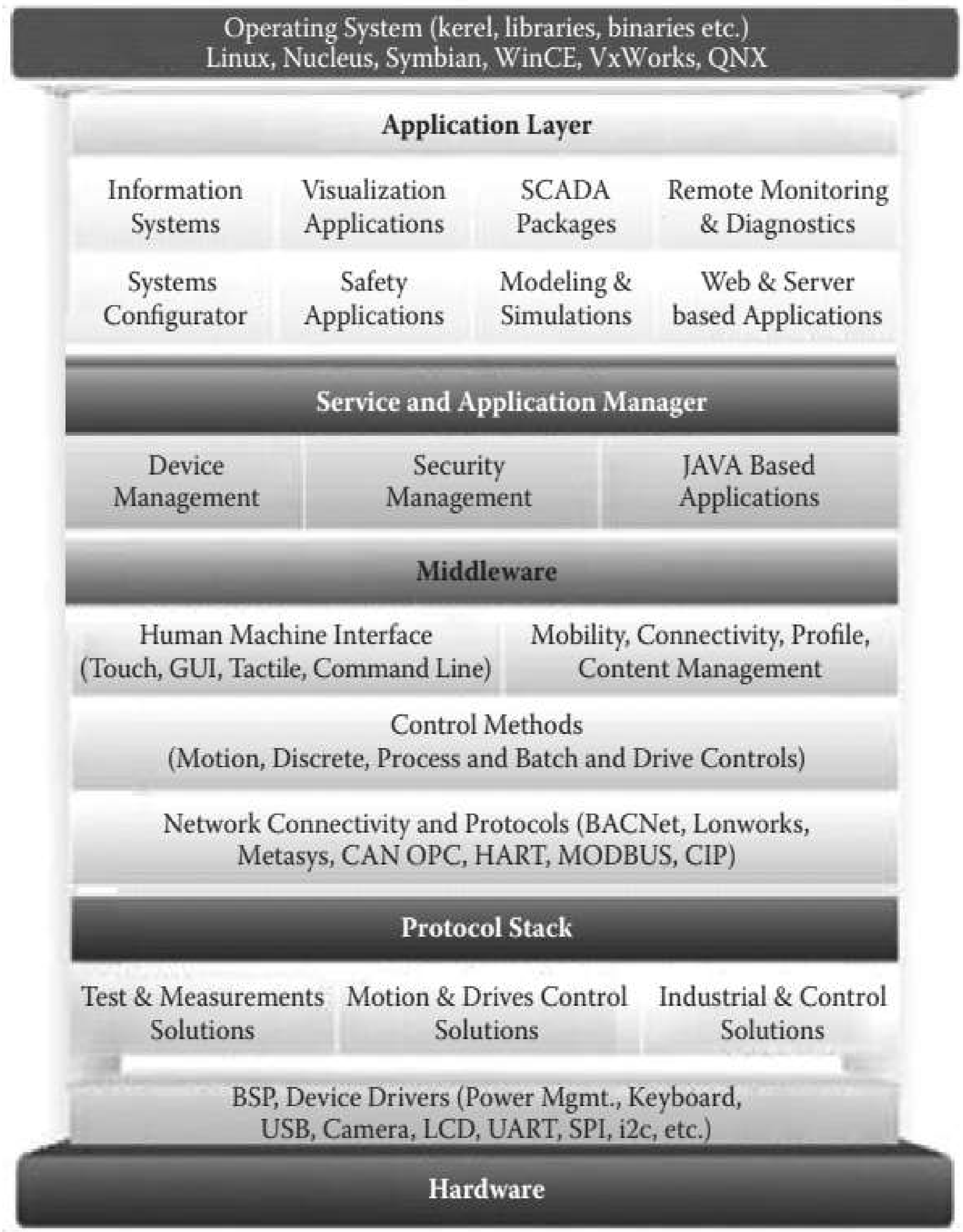


Figure 3.15 Middleware-based SCADA systems.

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.

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.

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.