CHAPTER

M2M to IoT — The Vision

2

CHAPTER OUTLINE

2.1 Introduction

Our world is on the verge of an amazing transformation; one that will affect every person, town, company, and thing that forms the basis of our society and economy. In the same way that the Internet redefined how we communicate, work, and play, a new revolution is unfurling that will again challenge us to meet new business demands and embrace the opportunities of technical evolution. Old and new industries, cities, communities, and individuals alike will need to adapt, evolve, and help create the new patterns of engagement that our world desperately needs. In response to these issues, we are moving towards a new era of intelligence — one driven by rapidly growing technical capabilities.

From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence.
DOI: http://dx.doi.org/10.1016/B978-0-12-407684-6.00002-4

M2M and the IoT are two of the technologies that form the basis of the new world that we will come to inhabit. Anything in the physical realm that is of interest to observe and control by people, businesses, or organizations will be connected and will offer services via the Internet. The physical entities can be of any nature, such as buildings, farmland, and natural resources like air, and even such personal real-world concepts as my favorite hiking route through the forest or my route to work. This book covers our world's transformation towards the IoT, and it is the authors' hope that we will inspire solutions and provide a technical framework to some of the world's most pressing needs — from environmental change to industrial re-configuration.

2.2 From M2M to IoT

Within this book, we attempt to describe the move from what is today referred to as *Machine-to-Machine* communication towards an emerging paradigm known as the *Internet of Things*. Quite often these terms are used interchangeably. This chapter provides definitions of what we mean by the two terms and sets the stage for the rest of the book by outlining the global trends, capabilities, and drivers towards IoT.

2.2.1 A brief background

Both M2M and IoT are results of the technological progress over the last decades, including not just the decreasing costs of semiconductor components, but also the spectacular uptake of the Internet Protocol (IP) and the broad adoption of the Internet. The application opportunities for such solutions are limited only by our imaginations; however, the role that M2M and IoT will have in industry and broader society is just starting to emerge for a series of interacting and interlinked reasons.

The Internet has undoubtedly had a profound impact across society and industries over the past two decades. Starting off as ARPANET connecting remote computers together, the introduction of the TCP/IP protocol suite, and later the introduction of services like email and the World Wide Web (WWW), created a tremendous growth of usage and traffic. In conjunction with innovations that dramatically reduced the cost of semiconductor technologies and the subsequent extension of the Internet at a reasonable cost via mobile networks, billions of people and businesses are now connected to the Internet. Quite simply, no industry and no part of society have remained untouched by this technical revolution.

At the same time that the Internet has been evolving, another technology revolution has been unfolding – the use of sensors, electronic tags, and actuators to digitally identify, observe and control objects in the physical world. Rapidly decreasing costs of sensors and actuators have meant that where such components previously cost several Euros each, they are now a few cents. In addition, these devices, through increases in the computational capacity of the associated chipsets, are now able to communicate via fixed and mobile networks. As a result, they are able to communicate information about the physical world in near real-time across networks with high bandwidth at low relative cost.

So, while we have seen M2M solutions for quite some time, we are now entering a period of time where the uptake of both M2M and IoT solutions will increase dramatically. The reasons for this are three-fold:

1. An increased need for understanding the physical environment in its various forms, from industrial installations through to public spaces and consumer demands. These requirements are often driven by efficiency improvements, sustainability objectives, or improved health and safety (Singh 2012).
2. The improvement of technology and improved networking capabilities.
3. Reduced costs of components and the ability to more cheaply collect and analyze the data they produce.

What makes the M2M and IoT markets take off today, therefore, is *needs* meeting *enabling technologies* at the right *cost*.

The next section takes a closer look at the drivers of M2M towards IoT.

2.2.2 M2M communication

M2M refers to those solutions that allow communication between devices of the same type and a specific application, all via wired or wireless communication networks. M2M solutions allow end-users to capture data about events from assets, such as temperature or inventory levels. Typically, M2M is deployed to achieve productivity gains, reduce costs, and increase safety or security. M2M has been applied in many different scenarios, including the remote monitoring and control of enterprise assets, or to provide connectivity of remote machine-type devices. Remote monitoring and control has generally provided the incentive for industrial applications, whereas connectivity has been the focus in other enterprise scenarios such as connected vending machines or point-of-sales terminals for online credit card transactions. M2M solutions, however, do not generally allow for the broad sharing of data or connection of the devices in question directly to the Internet.

2.2.2.1 A typical M2M solution overview

A typical M2M system solution consists of M2M devices, communication networks that provide remote connectivity for the devices, service enablement and application logic, and integration of the M2M application into the business processes provided by an Information Technology (IT) system of the enterprise, as illustrated below in Figure 2.1.

The M2M system solution is used to remotely monitor and control enterprise assets of various kinds, and to integrate those assets into the business processes of the enterprise in question. The asset can be of a wide range of types (e.g. vehicle, freight container, building, or smart electricity meter), all depending on the enterprise.

The system components of an M2M solution are as follows:

- *M2M Device*. This is the M2M device attached to the asset of interest, and provides sensing and actuation capabilities. The M2M device is here generalized, as there are a number of different realizations of these devices, ranging from low-end sensor nodes to high-end complex devices with multimodal sensing capabilities.
- *Network*. The purpose of the network is to provide remote connectivity between the M2M device and the application-side servers. Many different network types can be used, and include both Wide Area Networks (WANs) and Local Area Networks (LANs), sometimes also referred to as Capillary Networks or M2M Area Networks. Examples of WANs are public cellular mobile networks, fixed private networks, or even satellite links.
- *M2M Service Enablement*. Within the generalized system solution outlined above, the concept of a separate service enablement component is also introduced. This component provides generic

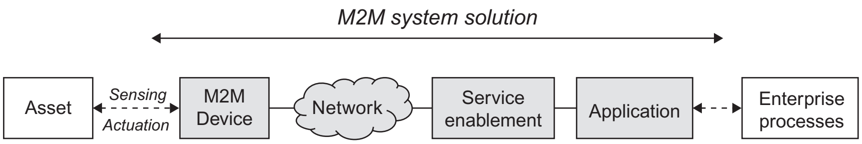

FIGURE 2.1

A generic M2M system solution.

functionality that is common across a number of different applications. Its primary purpose is to reduce cost for implementation and ease of application development. As we will see later and in Chapter 6, the emergence of service enablement as a separate system component is a clear trend.

- *M2M Application*. The application component of the solution is a realization of the highly specific monitor and control process. The application is further integrated into the overall business process system of the enterprise. The process of remotely monitoring and controlling assets can be of many different types, for instance, remote car diagnostics or electricity meter data management.

2.2.2.2 Key application areas

Existing M2M solutions cover numerous industry sectors and application scenarios. Various predictions have been made by analyst firms that provide market information such as key applications, value chains, and market actors, as well as market sizes (including forecasts) (ABI 2012, Berg 2013). A selected summary of main cellular M2M application markets is provided in Figure 2.2, and the figures are estimates of deployed numbers of corresponding M2M devices in the years 2012 and 2016, respectively.

The largest segment is currently **Telematics** for cars and vehicles. Typical applications include navigation, remote vehicle diagnostics,

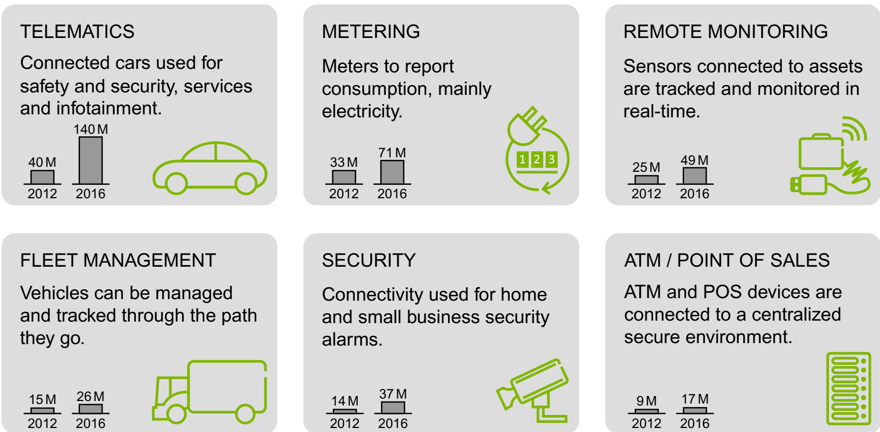

FIGURE 2.2

Summarized cellular M2M market situation.

(Courtesy of Ericsson)

pay-as-you-drive insurance schemes, road charging, and stolen vehicle recovery.

Metering applications, meanwhile, include primarily remote meter management and data collection for energy consumption in the electricity utility sector, but also for gas and water consumption.

Remote monitoring is more generalized monitoring of assets, and includes remote patient monitoring as one prime example.

Fleet management includes a number of different applications, like data logging, goods and vehicle positioning, and security of valuable or hazardous goods.

Security applications are mainly those related to home alarms and small business surveillance solutions. The final market segment is **Automated Teller Machines** (ATM) and **Point of Sales** (POS) terminals.

2.2.3 IoT

The IoT is a widely used term for a set of technologies, systems, and design principles associated with the emerging wave of Internet-connected things that are based on the physical environment. In many respects, it can initially look the same as M2M communication — connecting sensors and other devices to Information and Communication Technology (ICT) systems via wired or wireless networks.

In contrast to M2M, however, IoT also refers to the connection of such systems and sensors to the broader Internet, as well as the use of general Internet technologies. In the longer term, it is envisaged that an IoT ecosystem will emerge not dissimilar to today's Internet, allowing things and real world objects to connect, communicate, and interact with one another in the same way humans do via the web today. Increased understanding of the complexity of the systems in question, economies of scale, and methods for ensuring interoperability, in conjunction with key business drivers and governance structures across value chains, will create wide-scale adoption and deployment of IoT solutions. We cover this in more detail in Chapter 3.

No longer will the Internet be only about people, media, and content, but it will also include all real-world assets as intelligent creatures exchanging information, interacting with people, supporting business processes of enterprises, and creating knowledge (Figure 2.3). The IoT is not a new Internet, it is an extension to the existing Internet.

IoT is about the technology, the remote monitoring, and control, and also about where these technologies are applied. IoT can have a focus on the open innovative promises of the technologies at play, and also on advanced and complex processing inside very confined and close environments such as

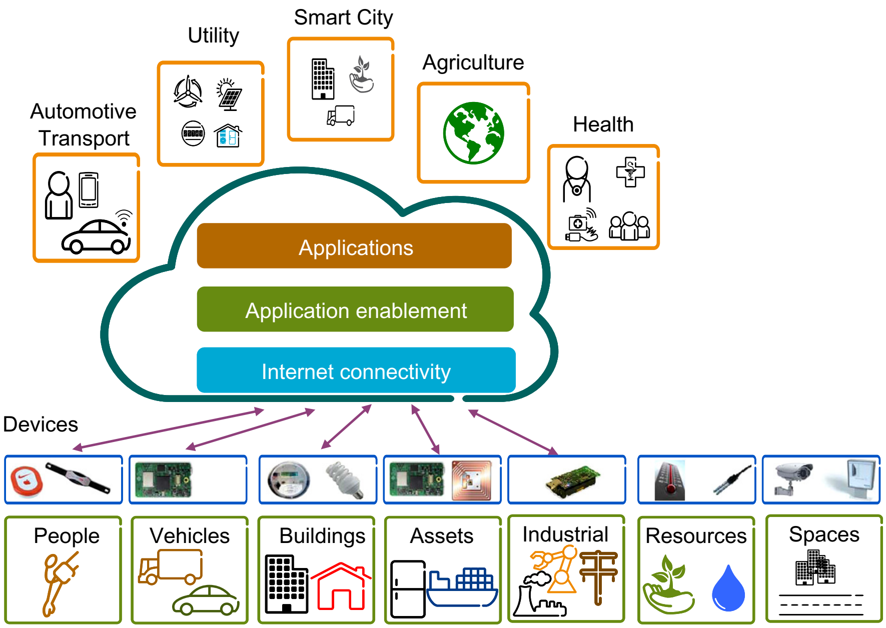

FIGURE 2.3

An IoT.

industrial automation. When employing IoT technologies in more closed environments, an alternative interpretation of IoT could then be "Intranet of Things."

Visions put forward (e.g. SENSEI 2013) have included notions like a global open fabric of sensor and actuator services that integrate numerous Wireless Sensor Network (WSN) deployments and provide different levels of aggregated sensor and actuator services in an open manner for application innovation and for use in not only pure monitor and control type of applications, but also to augment or enrich other types of services with contextual information. IoT applications will not only rely on data and services from sensor and actuators alone. Equally important is the blend-in of other information sources that have relevance from the viewpoint of the physical world. These can be data from Geographic Information Systems (GIS) like road databases and weather forecasting systems, and can be of both a static nature and real-time nature. Even information extracted from social media like Twitter feeds or Facebook status updates that relate to real world observations can be fed into the same IoT system. An example is in the EU FP7 project (CityPulse 2013), and this is also further described in Chapter 15, which is on Participatory Sensing (PS).

Looking towards the applications and services in the IoT, we see that the application opportunities are open-ended, and only imagination will set the limit of what is achievable. Starting from typical M2M applications, one can see application domains emerging that are driven from very diverse needs from across industry, society, and people, and can be of both local interest and global interest. Applications can focus on safety, convenience, or cost reduction, optimizing business processes, or fulfilling various requirements on sustainability and assisted living. Listing all possible application segments is futile, as is providing a ranking of the most important ones. We can point to examples of emerging application domains that are driven by different trends and interests (Figure 2.4). As can be seen, they are very diverse and can include applications like urban agriculture, robots and food safety tracing, and we will give brief explanations of what these three examples might look like.

Urban Agriculture. Already today, more than 50% of the world's population lives in urban areas and cities. The increased attention on sustainable living includes reducing transportation, and in the case of food production, reducing the needs for pesticides. The prospect of producing food at the place where it is consumed (i.e. in urban areas) is a promising

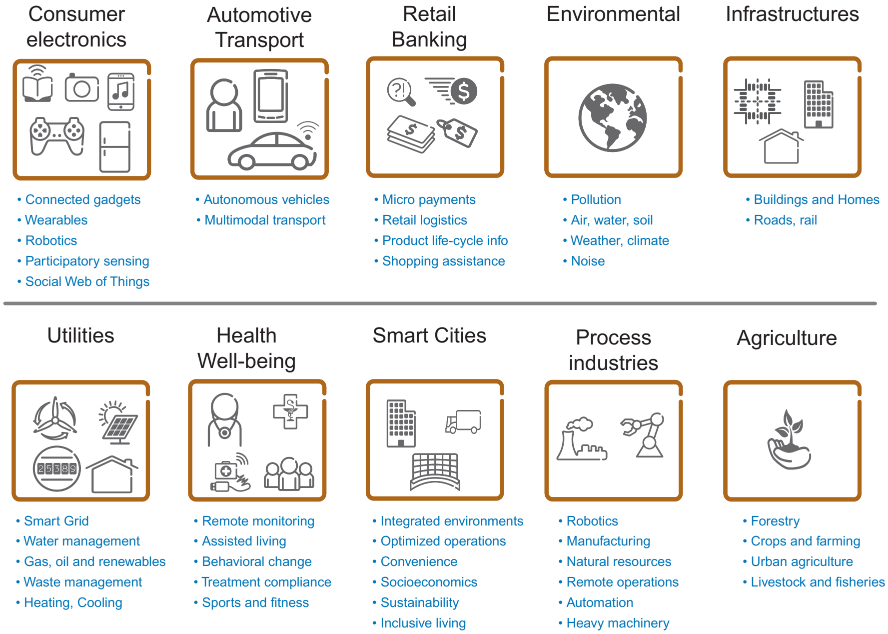

FIGURE 2.4

Emerging IoT applications.

example. By using IoT technologies, urban agriculture could be highly optimized. Sensors and actuators can monitor and control the plant environment and tailor the conditions according to the needs of the specific specimen. Water supply through a combination of rain collection and remote feeds can be combined on demand. City or urban districts can have separate infrastructures for the provisioning of different fertilizers. Drainage can be provided so as not to spoil crops growing on facades and rooftops of buildings, as well as to take care of any recyclable nutrients. Weather and light can be monitored, and necessary blinds that can shield and protect, as well as create greenhouse microclimates, can be automatically controlled. Fresh air generated by plants can be collected and fed into buildings, and tanks of algae that consume waste can generate fertilizers. A vision of urban agriculture is to be a self-sustaining system. Urban agriculture can be a mix of highly industrialized deployments with vertical greenhouses (Plantagon 2013), and collective efforts by individuals in apartments by the use of more do-it-yourself style equipment (Bitponics 2013).

Robots. The mining industry is undergoing a change for the future. Production rates must be increased, cost per produced unit decreased, and the lifetime of mines and sites must be prolonged. In addition, human workforce safety must be higher, with fewer or no accidents, and environmental impact must be decreased by reducing energy consumption and carbon emissions. The mining industry answer to this is to turn each mine into a fully automated and controlled operation. The process chain of the mine involving blasting, crushing, grinding, and ore processing will be highly automated and interconnected. The heavy machinery used will be remotely controlled and monitored, mine sites will be connected, and shafts monitored in terms of air and gases. As up to 50% of energy consumption in a mine can come from ventilation, energy savings can be done by very precise ventilation where the diesel vehicles are operating, and sensors in the mine can provide information about the location of the machines. The trend is also that local control rooms will be replaced by larger control rooms at the corporate headquarters. Sensors and actuators to remotely control both the sites and the massive robots in terms of mining machines for drilling, haulage, and processing are the instruments to make this happen. Companies like Rio Tinto (2012) with their Mine of the Future program, as well as ABB (2013), drive this development.

Food Safety. After several outbreaks of food-related illnesses in the U.S., the U.S. Food and Drug Administration (USFDA) created its Food Safety and Modernization Act (FSMA 2011). The main objective with

FSMA is to ensure that the U.S. food supply is safe. Similar food safety objectives have also been declared by the European Union and the Chinese authorities. These objectives will have an impact across the entire food supply chain, from the farm to the table, and require a number of actors to integrate various parts of their businesses. From the monitoring of farming conditions for plant and animal health, registration of the use of pesticides and animal food, the logistics chain to monitor environmental conditions as produce is being transported, and retailers handling of food — all will be connected. Sensors will provide the necessary monitoring capabilities, and tags like radio frequency identification (RFID) will be used to identify the items so they can be tracked and traced throughout the supply chain. The origin of food can also be completely transparent to the consumers.

As can be seen by these very few examples, IoT can target very point and closed domain-oriented applications, as well as very open and innovation driven applications. Applications can stretch across an entire value chain and provide lifecycle perspectives. Applications can be for business-to-business (B2B) as well as for business-to-consumer (B2C), and can be complex and involve numerous actors, as well as large sets of heterogeneous data sources.

We will progress to see how IoT is driven by a set of diverse needs, and how based on those needs, one can arrive at a set of different needed, recurring capabilities. We will also see how different technologies emerge that will enable building IoT, as well as a generalized model, or architecture, for how to build different target IoT solutions.

2.3 M2M towards IoT — the global context

M2M solutions have been around for decades and are quite common in many different scenarios. While the need to remotely monitor and control assets — personal, enterprise or other — is not new, a number of concurrent things are now converging to create drivers for change not just within the technology industry, but within the wider global economy and society. Our planet is facing massive challenges — environmental, social, and economic. The changes that humanity needs to deal with in the coming decades are unprecedented, not because similar things have not happened before during our common history on this planet, but because many of them are happening at the same time. From constraints on natural resources to a reconfiguration of the world's economy, many people are looking to technology to assist with these issues.

Essentially, therefore, a set of *megatrends* are combining to create *needs and capabilities*, which in turn produce a set of *IoT Technology and Business Drivers*. This is illustrated in Figure 2.5.

A megatrend is a pattern or trend that will have a fundamental and global impact on society at a macro level over several generations. It is something that will have a significant impact on the world in the foreseeable future. We here imply both game changers as challenges, as well as technology and science to meet these challenges. A full description of megatrends is beyond the scope of this book, and interested readers are directed to the many excellent books and reports available on this topic, including publications from the National Intelligence Council (NIC 2012), European Internet Foundation (EIF 2009), Frost & Sullivan (Singh 2012), and McKinsey (McKinsey 2013). In the following section, we focus on the megatrends that have implications for IoT. For the sake of simplicity, we also provide Table 2.1 as a summary of the main game changers, technology and science trends, capabilities, and implications for IoT.

2.3.1 Game changers

The game changers come from a set of social, economic, and environmental shifts that create pressure for solutions to address issues and problems, but also opportunities to reformulate the manner in which our world faces them. There is an extremely strong emerging demand for monitoring, controlling, and understanding the physical world, and the game changers are working in conjunction with technological and scientific advances. The transition from M2M towards IoT is one of the key facets of the technology evolution required to face these challenges. We outline some of these

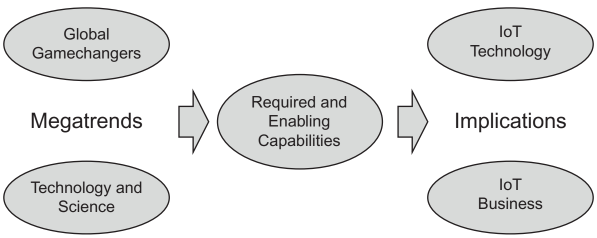

FIGURE 2.5

Megatrends, capabilities, and implications.

Table 2.1 A Summary of Megatrends, Capabilities, and IoT Implications

Megatrends

Global gamechangers

- Natural resource constraints
- Economic shifts
- Changing demographics
- Socioeconomic expectations
- Climate change
- Environmental impacts
- Safety and security
- Urbanization

Technology and Science

- Information and Communication Technologies
- Material science
- Complex and advanced machinery
- Energy production and storage

Capabilities

Required capabilities

- Integrated infrastructures
- Asset-to-expert system integration
- Large scale monitor and control
- Autonomous operations
- Complex remote control
- Workforce offloading
- Domain expertise inside systems
- Visualization
- Data and service exposure
- Advanced analytics
- Increasing levels of security
- Cross value chain integration
- Cost rationalization

Enabling technologies

- Sensing and actuation
- Embedded computing
- Ubiquitous connectivity
- Data processing and storage
- Intelligent software
- Virtualization and cloud
- Application development

Implications

Technology

- Vertical to horizontal systems
- Application independent devices
- Technology consolidation
- IP and Web enabled
- Open software development
- Exposure APIs
- Software enabling architectures
- Cloud deployments
- Intelligence and automation

Business

- Open and innovation driven
- Cloud and as-a-Service delivered
- B2B2C
- Service oriented
- Developer community reach
- Long tail empowerment
- Marketplaces of data and services
- New market roles/value systems
- Cross domain integration
- Commoditized devices
- Application and user driven

more globally significant game changers below, and their relationship to IoT:

- **Natural Resource Constraints**. The world needs to increasingly do more with less, from raw materials to energy, water or food, the growing global population and associated economic growth demands put increasing constraints on the use of resources. The use of IoT to increase yields, improve productivity, and decrease loss across global supply chains is therefore escalating.
- **Economic Shifts**. The overall economy is in a state of flux as it moves from the post-industrial era to a digital economy. One example of this is found in the move from product-oriented to service-oriented economies. This implies a lifetime responsibility of the product used in the service offering, and will in many cases require the products to be connected and contain embedded technologies for gathering data and information. At the same time, there are fluctuations in global economic leadership. Economies across the globe must handle the evolving nature of these forces. As technology becomes increasingly embedded and more tasks automated, countries need to manage this shift and ensure that M2M and IoT also create new jobs and industries.
- **Changing Demographics**. With increased prosperity, there will be a shift in the demographic structures around the world. Many countries will need to deal with an aging population without increasing economic expenditure. As a result, IoT will need to be used, for example, to help provide assisted living and reduce costs in healthcare and emerging "wellcare" systems.
- **Socioeconomic Expectations**. The global emerging middle class results in increasing expectations on well-being and Corporate Social Responsibility. Lifestyle and convenience will be increasingly enabled by technology as the same disruption and efficiency practices evident in industries will be applied within people's lives and homes as well.
- **Climate Change and Environmental Impacts**. The impact of human activities on the environment and climate has been long debated, but is now in essence scientifically proven. Technology, including IoT, will need to be applied to aggressively reduce the impact of human activity on the earth's systems.
- **Safety and Security**. Public safety and national security becomes more urgent as society becomes more advanced, but also more vulnerable. This has to do both with reducing fatalities and health as well as crime prevention, and different technologies can address a number of the issues at hand.

- **Urbanization**. We see the dramatic increase in urban populations and discussions about megacities. Urbanization creates an entirely new level of demands on city infrastructures in order to support increasing urban populations. IoT technologies will play a central role in the optimization for citizens and enterprises within the urban realm, as well as providing increased support for decision-makers in cities.

2.3.2 General technology and scientific trends

Technological and scientific advances and breakthroughs are occurring across a number of disciplines at an increasing pace. Below is a brief description of the science and technology advances that have a direct relevance to IoT. The trends in the ICT sector are described separately in the subsequent section, as it is central for this book.

Material Science has a large impact across a vast range of industries, from pharmaceutical and cosmetics to electronics. MicroElectroMechanical Systems (MEMS) can be used to build advanced micro-sized sensors like accelerometers and gyroscopes. Emerging flexible and printable electronics will enable a new range of innovations for embedding technology in the real world. New materials provide different methods to develop and manufacture a large range of different sensors and actuators, as well being used in applications for environmental control, water purification, etc. Additionally, we will see other innovative uses such as smart textiles that will provide the capability to produce the next generation of wearable technologies. From an IoT perspective, these advances in material science will see an increasing range of applications and also a broader definition of what is meant by a sensor.

Complex and Advanced Machinery refers to tools that are autonomous or semi-autonomous. Today they are used in a number of different industries; for example, robots and very advanced machinery is used in different harsh environments, such as deep-sea exploration, or in the mining industry in solutions such as Rio Tinto's Mine of the Future™ (Rio Tinto 2012). Advanced machines have many modalities, and operate with a combination of local autonomous capabilities as well as remote control. Sensing and actuation are key technologies, and local monitor-control loops for routine tasks are required in addition to reliable communications for remote operations. Often such solutions require real-time characteristics. These systems will continue to evolve and automate tasks today performed by humans — even self-driving cars have started to make headlines thanks to Google.

Energy Production and Storage is relevant to IoT for two reasons. Firstly, it relates to the global interest of securing the availability of electricity while reducing climate and environmental impacts. Smart Grids, for example, imply micro-generation of electricity using affordable photovoltaic panels. In addition, smart grids also require new types of energy storage, both for the grid itself and for emerging technologies such as Electric Vehicles (EVs) that rely on increasingly efficient battery technologies. Secondly, powering embedded devices in Wireless Sensor Networks (WSNs) will increasingly rely on different energy harvesting technologies and also rely on new miniaturized battery technologies and ultra capacitors. As these technologies improve, IoT will be applicable in a broad range of scenarios that need long battery life.

2.3.3 Trends in information and communications technologies

While significant advances in the fields of Material Science, Advanced and Complex Machinery, and Energy Production and Storage will have an impact on IoT, first and foremost, ICT advances will drive the manner in which these solutions are provided as they are the core enabling factors behind M2M and IoT. Ever since the development of integrated circuits during the late 1950s and early 1960s, these technologies have had an increasing impact on enterprises and society. The increasing rates of change have led to a situation where it is now cheap enough to “sensor the planet.”

Today, **sensors, actuators, and tags function as the digital interfaces** to the physical world. Small-scale and cheap sensors and actuators provide the bridge between the physical realm and ICT systems. Tags using technologies such as RFID provide the means to put electronic identities on any object, and can be cheaply produced.

Embedded processing is evolving, not only towards higher capabilities and processing speeds, but also extending towards the smallest of applications. There is a growing market for small-scale embedded processing such as 8-, 16-, and 32-bit microcontrollers with on-chip RAM and flash memory, I/O capabilities, and networking interfaces such as IEEE 802.15.4 that are integrated on tiny System-on-a-Chip (SoC) solutions. These enable very constrained devices with a small footprint of a few mm^2 and very low power consumption (in the milli- to micro-Watt range), yet are still capable of hosting an entire TCP/IP stack including a small web server.

Instant access to the Internet is available virtually everywhere today, mainly thanks to wireless and cellular technologies and the rapid deployment of cellular 3G and 4G or Long Term Evolution (LTE) systems on a global scale. These systems provide ubiquitous and relatively cheap connectivity with the right characteristics for many applications, including low latency and the capacity to handle large amounts of data with high reliability. Existing technologies can be further complemented with last-hop technologies such as IEEE 802.15.4, Bluetooth Low Energy, and Power Line Communication (PLC) solutions to reach even the most cost-sensitive deployments and tiniest devices. Technologies like 6LoWPAN allow IP connectivity to be provided end-to-end, stretching into the capillary network domain, and legacy and proprietary protocols like ZigBee PRO can be avoided with the benefit of IP and the web anywhere. 3GPP are also extending LTE towards the lower end of the scale, providing very low power extensions targeting specific IoT applications, also for more constrained devices. Network access technologies are further described in Section 5.2.

Software architectures have undergone several evolutions over the past decades, in particular with the increasing dominance of the web paradigm. A description of the evolution of software is beyond the scope of this book; here we instead look at those angles of software that are critical for successful IoT solutions. From a simplistic perspective, we can view software development techniques from what were originally closed environments towards platforms, where Open APIs provide a simple mechanism for developers to access the functionality of the platform in question (e.g. Microsoft Windows). Over time, these platforms, due to the increasing use and power of the Internet, have become open platforms — ones that do not depend on certain programming languages or lock-in between platform developers and platform owners.

Software development has started applying the **web paradigm and using a service-oriented approach (SOA)**. By extending the web paradigm to IoT devices, they can become a natural component of building any application and facilitate an easy integration of IoT device services into any enterprise system that is based on the SOA (e.g. that uses web services or RESTful interfaces). IoT applications can then become technology and programming language independent. This will help boost the IoT application development market. A key component in establishing the application development market is Open APIs.

Open APIs, in the same way that they have been critical to the development of the web, will be just as important to the creation of a successful IoT market, and we can already see developments in this space. Put simply, Open APIs relate to a common need to create a market *between* many companies, as is the case in the IoT market. Open APIs permit the creation of a fluid industrial platform, allowing components to be combined together in multiple different ways by multiple developers with little to no interaction with those who developed the platform, or installed the devices. As we will discuss in more detail in Chapter 3, it is impossible for one company to guess what will be successful or liked by all of the customer segments associated with IoT. Open APIs are the market's response to this uncertainty; choice of how to combine components is left to developers who are able to merely pick up the technical description and combine them together.

Without Open APIs, a developer would need to create contracts with several different companies in order to get access to the correct data to develop the application. The transaction costs associated with establishing such a service would be prohibitively expensive for most small development companies; they would need to establish contracts with each company for the data required, and spend time and money on legal fees and business development with each individual company. Open APIs remove the need to create such contracts, allowing companies to establish "contracts" for sharing small amounts of data with one another and with developers dynamically, without legal teams, without negotiating contracts, and without even meeting one another. Open APIs therefore reduce the transaction costs associated with establishing a new market boundary (Mulligan 2011), mitigating the risk of development and help to establish a market for innovative capacity, which encourages creativity and application development.

Meanwhile, within ICT, **virtualization** has many different facets and has gained a lot of attention in the past few years, even though it has been around for a rather long time. The **cloud computing** paradigm, with different *as a Service* models, is one of the greatest aspects of the evolution of ICT for IoT as it allows virtualized and independent execution environments for multiple applications to reside in isolation on the same hardware platform, and usually in large data centers.

Cloud computing allows elasticity in deployment of services and enables reaching long-tail applications in a viable fashion. It can be used to avoid in-house installations of server farms and associated dedicated IT service operations staff inside companies, thus enabling them to focus on their core business. Cloud computing also has the benefit of easing different businesses to interconnect if they are executing on the same platform. Handling of, for example, Service Level Agreements (SLAs) is easily facilitated with a high degree of control in a common virtualized environment. Cloud computing is also a key enabler when moving from a product-oriented offering to a service-oriented offering due to elasticity permitting companies to "pay-as-you-grow."

Closely related to the topic of data centers, **data processing and intelligent software** will have an increasing role to play in IoT solutions. A popular concept now is **big data**, which refers to the increasing number and size of data sets that are available for companies and individuals to collect and perform analysis on. Built on large-scale computing, data storage, in-memory processing, and analytics, big data is intended to find insights in the massive data sets produced. Naturally, these technologies are therefore key enablers for IoT, as they allow the collation and aggregation of the massive datasets that devices and sensors are likely to produce.

IoT is unique in comparison to other big data applications such as social media analysis, however, in that even the smallest piece of data can be critical. Take, for example, a sensor solution implemented to ensure that a large-scale engineering project does not cause subsidence in a residential area while drilling a tunnel beneath the ground. The data collected from a vast quantity of sensors will help with the overall management of the project and ensure the health and safety of those working on it during the several months that it is ongoing. It might only be a tiny piece of data from one sensor, however, that indicates a shift due to tunneling that may mean the collapse of a building on the surface. Whereas the aggregation of the data from all sensors can be usefully analyzed at intervals, the data related to subsidence and possible collapse of a building is critical and required in real-time.

Therefore, IoT data typically also involves numerous and very different and heterogeneous sources, but also numerous and very different usages of the data. The analysis of IoT data may therefore be viewed as a complex set of interactions related to *time* (i.e. when the data is received) and *relevance* (i.e. the overall relevance of the piece of data to the question in hand). Managing these interactions is critical to the success of IoT solutions.

Decision support or even decision-making systems will therefore become very important in different application domains for IoT, as will the set of tools required to process data, aggregate information, and create knowledge. Knowledge representation across domains and heterogeneous systems are also important, as are semantics and linked-data. As a result, we can expect to see an increased usage of cognitive technologies and self-learning systems.

A fundamental addition to the data aspect of IoT is the dimension represented by **actionable services as realized by actuators**. There is a duality in sensing and actuation in terms of fusion and aggregation. Where data analytics is employed to find insights basically by aggregation, one can consider complex multimodal actuation services that need to be resolved down to the level of individual atomic actuation tasks. IoT also calls for intelligence in the form of closed control loops of sensing and actuation, which can be simple or very complex. This duality and the closed control aspect will put new requirements on technologies that stretch the boundaries from what can be achieved based on data-only oriented technologies used in the prevalent approach to "big data."

As is illustrated in this chapter, the IoT market holds incredible promise for solving big problems for industry, society, and even individuals. One key thing to note, however, is the tremendous complexity that such systems need to handle in order to function efficiently and effectively. Partnerships and alliances are therefore critical — no one company will be able to produce all the technology and software required to deliver IoT solutions. Moreover, no one company will be able to house the innovative capacity required to develop new solutions for this market. IoT solutions bring together devices, networks, applications, software platforms, cloud computing platforms, business processing systems, knowledge management, visualization, and advanced data analysis techniques. This is quite simply not possible at scale without significant levels of **system integration and standards development**.

This section discussed the global megatrends associated with technology and society. The following section contains a discussion of the capabilities that are required and delivered due to the IoT.

2.3.3.1 Capabilities

As illustrated in previous sections, there are several recurring characteristics of ICT required to develop IoT solutions. These capabilities address several aspects such as cost efficiency, effectiveness and convenience; being lean and reducing environmental impact; encouraging innovation; and in general applying technology to create more intelligent systems, enterprises, and societies. The aforementioned ICT developments provide us with a rich toolbox to address these different aspects in general, and as part of that, IoT in particular. In the following sections we outline how these required capabilities, driven by global megatrends, can be met through the use of the enabling technologies.

While M2M today targets specific problems with tailored, siloed solutions, it is clear that emerging IoT applications will address the much more complex scenarios of large-scale distributed monitor and control applications. IoT systems are multimodal in terms of sensing and control, complex in management, and distributed across large geographical areas. For example, the new requirements on Smart Grids involve end-to-end management of energy production, distribution, and consumption, taking into consideration needs from Demand Response, micro-generation, energy storage, and load balancing. Industrialized agriculture involving automated irrigation, fertilization, and climate control is another example. We see clearly here heterogeneity across sensor data types, actuation services, underlying communication systems, and the need to apply intelligent software to reach various Key Performance Indicators (KPI).

Take, for example, Smart City solutions: here there is a clear need for integration of multiple disparate infrastructures such as utilities, including district heating and cooling, water, waste, and energy, as well as transportation such as road and rail. Each of these infrastructures has multiple stakeholders and separate ownership even though they operate in the same physical spaces of buildings, road networks, and so on. The optimization of entire cities requires the opening up of data and information, business processes, and services at different levels of the disjoint silos, creating a common fabric of services and data relating to the different infrastructures. This integration of multiple infrastructures will drive the need for a horizontal approach at the various levels of the system, for instance, at the resource level where data and information is captured by devices, via the information level, up to the knowledge and decision level. We cover these issues in more detail in Chapter 14: Smart Cities.

Meanwhile, advanced remotely operated machinery, such as drilling equipment in mines or deep sea exploration vessels, will require real-time control of complex operations, including various degrees of autonomous control systems. This places new requirements on the execution of distributed application software and real-time characteristics on both the network itself, as well as a need for flexibility in where application logic is executed.

IoT will allow more assets of enterprises and organizations to be connected, thus allowing a tighter and more prompt integration of the assets into business processes and expert systems. Simple machines can be used in a more controlled and intelligent manner, often called "Smart Objects." These connected assets will generate more data and information, and will expose more service capabilities to ICT systems. Managing the complexity of information and services becomes a growing barrier for the workforce, and places a high focus on using analytics tools of various kinds to gain insights. These insights, combined with domain-specific knowledge, can help the decision process of humans as individuals or professionals via decision support systems and visualization software.

As society operations involve a large number of actors taking on different roles in providing services, and as enterprises and industries increasingly rely on efficient operations across ecosystems, cross value chain and value system integration is a growing need. This requires technologies and business mechanisms that enable operations and information sharing across supply chains. Even industry segments that have been entirely unconnected will connect due to new needs; an example is the introduction of EVs. EVs are enabled by the new battery and energy storage technologies, but also require three separate elements to be connected — cars, road infrastructure via charging poles, and the electricity grid. In addition, there are new charging requirements that are created by the use of EVs that need new means for billing, and in turn placing new requirements on the electricity grid itself.

These sorts of collaboration scenarios will become increasingly important as industries, individuals, and government organizations work together to solve complex problems involving multiple stakeholders. This places an emphasis on the openness and exposure of services and information at different levels. What is important is to be able to share information and services across organizations in the horizontal dimension, as well as being able to aggregate and combine services and information to reach higher degrees of refinement and values in the vertical dimension. The open and collaborative nature of IoT means methods are required to publish and discover data and services, as well as means to achieve semantic interoperability, but also that care needs to be given to trust, security, and privacy. It also dramatically increases the required capability of system integration and the management of large-scale complex systems across multiple stakeholders and multiple organizational boundaries.

As we come to increasingly rely on ICT solutions to monitor and control assets, physical properties of the real world require not just increased levels of cybersecurity, but what can be referred to as cyber-physical security. In the use of the Internet today, it is possible to exact financial damage via breaking into information technology (IT) systems of companies or bank accounts of individuals. Individuals, meanwhile, can face social damages from people hacking social media accounts. In an IoT, where it is possible to control assets (e.g. vehicles or moveable bridges), severe damage to property, or even loss of life, is possible. This raises requirements for trust and security to be correctly implemented in IoT systems.

2.3.4 Implications for IoT

Having gained a better understanding of capabilities needed, as well as how technology evolution can support these needs, we can note plausible implications on both the technology and business perspectives.

There is already a trend of moving away from vertically oriented systems, or application-specific silos, towards a horizontal systems approach. We see that in the standardization work of the ETSI Technical Committee M2M (ETSI M2M 2013), and now also in the oneM2M project partnership organization, both covered in more detail in Part II of this book. The work in these organizations is primarily based on identifying a common set of service capabilities that are application independent, but they also identify reference points to underlying communication network services as well as reference points to M2M devices.

The use of the TCP/IP stack towards IoT devices represents another horizontal point in an M2M and IoT system solution, and is something driven by organizations like the IETF and the IP for Smart Objects (IPSO) Alliance. In the M2M device area, there is an emerging consolidation of technologies where solutions across different industry segments traditionally rely on legacy and proprietary technologies. Currently within industry segments there is technology fragmentation, one example being Building and Home Automation and Control with legacy technologies like BACnet, Lonworks, KNX, Z-Wave, and ZigBee. An example of this consolidation entering the legacy domain is ZigBee IP (ZigBee Alliance 2013c), where TCP/IP is used in the Smart Energy Profile (SEP) 2.0 (ZigBee Alliance 2013b).

In such situations, where there is a requirement for integration across multiple infrastructures and of a large set of different devices, as well as data and information sharing across multiple domains, there is a clear benefit from a horizontal systems approach with at least a common conceptual interoperability made available, and a reduced set of technologies and protocols being used.

As mentioned previously, M2M is point problem-oriented, resulting in point solutions where devices and applications are highly dedicated to solving a single task. M2M devices are for this reason many times highly application-specific, and reuse of devices beyond the M2M application at hand is difficult, if at all possible. With the increasing requirements to gather information and services from various sources, and to be able to have greater flexibility and variety in IoT applications, devices can no longer be application-specific in the same manner as for M2M. Benefits will be achieved if an existing device can be used in a variety of applications, and likewise if a specific application can use a number of different deployed devices. Here we see a shift from application-specific devices towards application-independent devices. As also mentioned, clear benefits come from relying on the web services paradigm, as it allows easy integration in SOAs and attracts a larger application developer community.

Even though M2M has been around for many years, recent years have seen a tremendous interest in M2M across industries, primarily the telecom industry. This comes from the fact that both devices and connectivity have become viable for many different applications, and M2M today is centered on devices and connectivity. For IoT there will be a shift of focus away from device- and connectivity-centricity towards services, data, and intelligence.

2.3.5 Barriers and concerns

With the explained transformations in moving from M2M towards IoT, which involves many opportunities, we should not forget that some new concerns and barriers will also be raised.

With the IoT, the first concern that likely comes to mind is the compromise of privacy and the protection of personal integrity. The use of RFID tags for tracing people is a raised concern. With a massive deployment of sensors in various environments, including in smartphones, explicit data and information about people can be collected, and using analytics tools, users could potentially be profiled and identified even from anonymized data.

The reliability and accuracy of data and information when relying on a large number of data sources that can come from different providers that are beyond one's own control is another concern. Concepts like Provenance of Data and Quality of Information (QoI) become important, especially considering aggregation of data and analytics. As there is a risk of relying on inaccurate or even faulty information in a decision process, the issue of accountability, and even liability, becomes an interest. This will require new technology tools; an example effort includes the work on QoI related to both sensor data and actuation services in the EU FP7 project SENSEI (SENSEI 2013).

As has already been mentioned, the topic of security has one added dimension or level of concern. Not only are today's economical or social damages possible on the Internet, but with real assets connected and controllable over the Internet, damage of property as well as people's safety and even lives become an issue, and one can talk about cyber-physical security.

Not a concern, but a perceived barrier for large-scale adoption of IoT is in costs for massive deployment of IoT devices and embedded technologies. This is not only a matter of Capital Expenditure (CAPEX), but likely more importantly a matter of Operational Expenditure (OPEX). From a technical perspective, what is desired is a high degree of automated provisioning towards zero-configuration. Not only does this involve configuration of system parameters and data, but also contextual information such as location (e.g. based on Geographic Information System (GIS) coordinates or room/building information).

These different concerns and barriers have consequences not only on finding technical solutions, but are more importantly having consequences also on business and socioeconomic aspects as well as on legislation and regulation. The market perspective is further covered in Chapter 3.

2.4 A use case example

In order to understand how a specific problem can be addressed with M2M and IoT, respectively, we provide a fictitious illustrative example. Our example takes two different approaches towards the solution, namely an M2M approach and an IoT approach. By that, we want to highlight the potential and benefits of an IoT-oriented approach over M2M, but also indicate some key capabilities that will be required going beyond what can be achieved with M2M. Our example is taken from personal well-being and health care.

Studies from the U.S. Department of Health and Human Services have shown that close to 50% of the health risks of the enterprise workforce are stress related, and that stress was the single highest risk contributor in a group of factors that also included such risks as high cholesterol, overweight issues, and high alcohol consumption. As stress can be a root cause for many direct negative health conditions, there are big potential savings in human quality of life, as well as national costs and productivity losses, if the factors contributing to stress can be identified and the right preventive measures taken. By performing the steps of stressor diagnosis, stress reliever recommendations, logging and measuring the impacts of stress relievers for making a stress assessment, all in an iterative approach, there is an opportunity to significantly reduce the negative effects of stress.

Measuring human stress can be done using sensors. Two common stress measurements are heart rate and galvanic skin response (GSR), and there are products on the market in the form of bracelets that can do such measurements. These sensors can only provide the intensity of the heart rate and GSR, and do not provide an answer to the cause of the intensity. A higher intensity can be the cause of stress, but can also be due to exercise. In order to analyze whether the stress is positive or negative, more information is needed.

The typical M2M solution would be based on getting sensor input from the person by equipping him or her with the appropriate device, in our case the aforementioned bracelet, and using a smartphone as a mobile gateway to send measurements to an application server hosted by a health service provider. In addition to the heart rate and GSR measurements, an accelerometer in the smartphone measures the movement of the person, thus providing the ability to correlate any physical activity to the excitement measurements. The application server hosts the necessary functionality to analyze the collected data, and based on experience and domain knowledge, provides an indication of the stress level. The stress information can then be made available to the person or a caregiver via smartphone application or a web interface on a computer. The M2M system solution and measured data is depicted in Figure 2.6.

As already pointed out, this type of solution that is limited to a few measurement modalities can only provide very limited (if any) information about what actually causes the stress or excitement. Causes of stress in

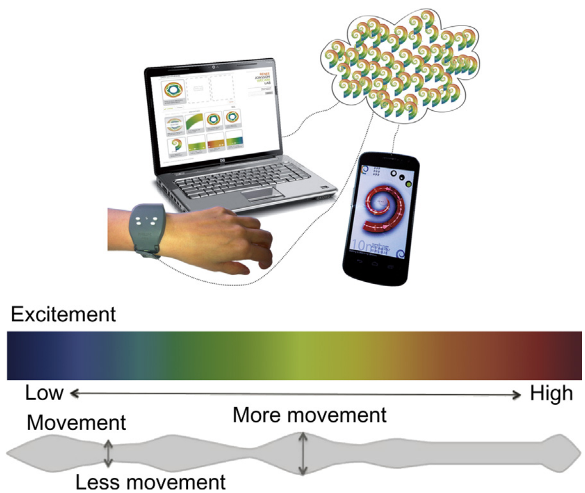

FIGURE 2.6

Stress measurement M2M solution.

(Courtesy of Swedish Institute of Computer Science and Ericsson)

daily life, such as family situation, work situation, and other activities cannot be identified. A combination of the stress measurement log over time, and a caregiver interviewing the person about any specific events at high levels of measured stress, could provide more insights, but this is a costly, labor-intensive, and subjective method. If additional contextual information could be added to the analysis process, a much more accurate stress situation analysis could potentially be performed.

Approaching the same problem situation from an IoT perspective would be to add data that provide much deeper and richer information of the person's contextual situation. The prospect is that the more data is available, the more data can be analyzed and correlated in order to find patterns and dependencies. What is then required is to capture as much data about the daily activities and environment of the person as possible. The data sources of relevance are of many different types, and can be openly available information as well as highly personal information. The resulting IoT solution is shown in Figure 2.7, where we see examples of a wide variety of data sources that have an impact on the personal situation. Depicted is also the importance of having expert domain knowledge that can mine the available information, and that can also provide proposed actions to avoid stressful situations or environments.

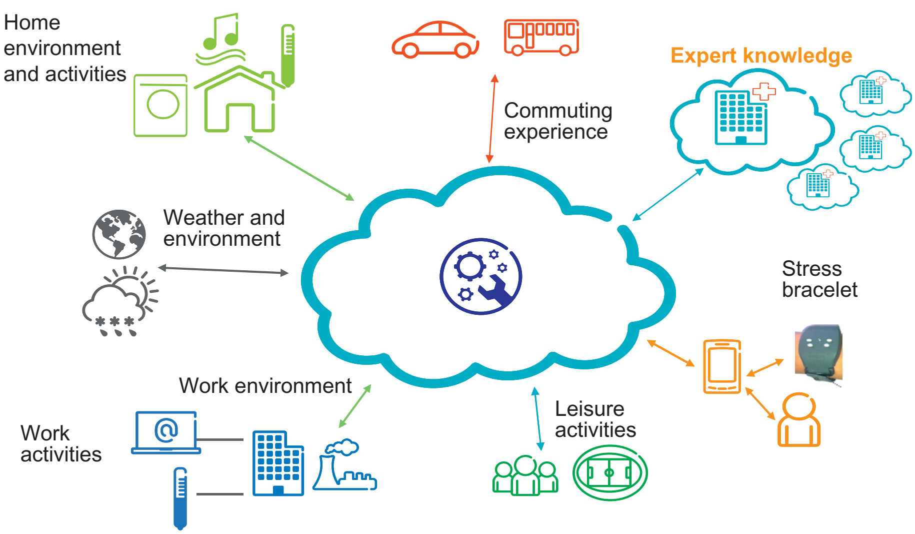

FIGURE 2.7

IoT-oriented stress analysis solution.

(Courtesy of Ericsson)

The environmental aspects include the physical properties of the specific environment, and can be air quality and noise levels of the work environment, or the nighttime temperature of the bedroom, all having impacts on the person's well-being. Work activities can include the amount of e-mails in the inbox or calendar appointments, all potentially having a negative impact on stress. Leisure activities, on the other hand, can have a very positive impact on the level of excitement and stress, and can have a more healing effect than a negative effect. Such different negative and positive factors need to be separated and filtered out; see Figure 2.8 for an example smartphone application that provides stress analysis feedback.

The stress bracelet is in this scenario is just one component out of many. It should also be noted that the actual information sources are very independent of the actual application in mind (i.e. measurement and prevention of negative stress).

By having the appropriate expert knowledge system in place, analytics can be proactive and preventive. By understanding what factors cause negative stress, the system can propose actions to be taken, or even initiate actions automatically. They could be very elementary, such as suggesting to lower the nighttime bedroom temperature a few degrees, but also be

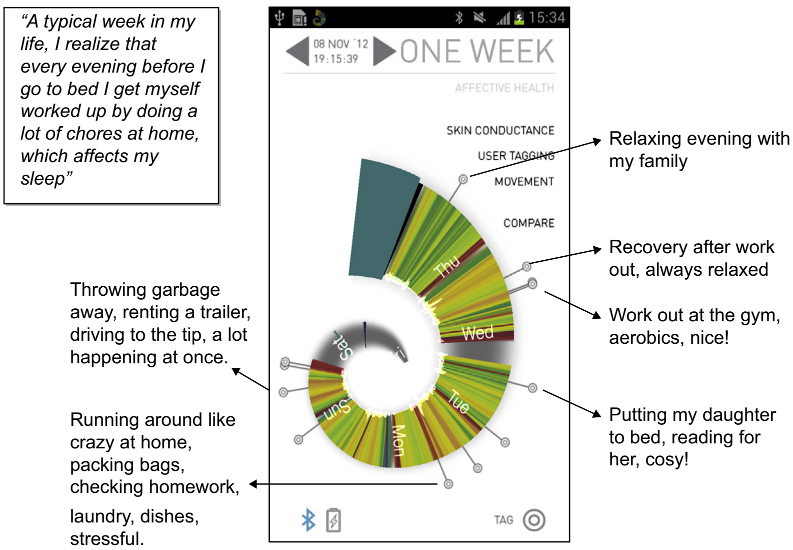

FIGURE 2.8

Stress analysis visualization.

(Courtesy of Swedish Institute of Computer Science and Ericsson)

more complex, such as having to deal with an entire workplace environment.

As this simple example illustrates, an IoT-oriented solution to solving a particular problem could provide much more precision in achieving the desired results. We also observe some of the key features of an IoT solution; in other words, to take many different data sources into account, relying both on sensor-originated data sources, but also other sources that have to do with the physical environment, and then also to rely on both openly available data as well as data that is private and personal. The data sources, such as sensor nodes, should also focus on providing the information and should to the greatest extent be application-independent so that their reuse can be maximized. We also see the central role of analytics and knowledge extraction, as well as taking knowledge into actionable services that can involve controlling the physical environment using actuators. The increased complexity also comes at a cost. The solutions must ensure security and protection of privacy, and the need to deal with data and information of different degrees of accuracy and quality needs to be addressed in order to provide dependable solutions in the end.

2.5 Differing characteristics

To summarize, today's M2M solutions and deployments share a few common characteristics. First of all, any M2M solution is generally focused on solving a problem at a particular point for one company or stakeholder. It does not typically take a broad perspective on solving a larger set of issues or ones that could involve several stakeholders. As a result, most M2M devices are special purpose devices that are application-specific, often down to the device protocols. M2M solutions are therefore also vertical siloes with no horizontal integration or connection to adjacent use cases, and are primarily of a B2B-type of operation. M2M applications are built by very specialized developers, and deployed inside enterprises. As M2M has a rather long history, technologies used are very industry-specific, and especially on the device side, technology use is highly fragmented with little or no standards across industries. M2M is also very device- and communication-centric, as both are the two current cornerstones for remote access to assets.

The transition from M2M towards an IoT is mainly characterized by moving away from the mentioned closed-silo deployments towards something that is characterized by openness, multipurpose, and innovation.

Table 2.2 A Comparison of the Main Characteristics of M2M and IoT

Aspect	M2M	IoT
Applications and services	Point problem driven	Innovation driven
	Single application - single device	Multiple applications - multiple devices
	Communication and device centric	Information and service centric
	Asset management driven	Data and information driven
Business	Closed business operations	Open market place
	Business objective driven	Participatory community driven
	B2B	B2B, B2C
	Established value chains	Emerging ecosystems
	Consultancy and Systems Integration enabled	Open Web and as-a-Service enabled
	In-house deployment	Cloud deployment
Technology	Vertical system solution approach	Horizontal enabler approach
	Specialized device solutions	Generic commodity devices
	De facto and proprietary	Standards and open source
	Specific closed data formats and service descriptions	Open APIs and data specifications
	Closed specialized software development	Open software development
	SOA enterprise integration	Open APIs and web development

This transition consists of a few main transformations, namely: moving away from isolated solutions to an open environment; the use of IP and web as a technology toolbox, the current Internet as a foundation for enterprise and government operations; multimodal sensing and actuation; knowledge-creating technologies; and the general move towards a horizontal layering of both technology and business. The main differing characteristics between M2M and IoT highlighted in this chapter are summarized in Table 2.2.