IoT Applications to Smart Campuses and a Case Study

D. Minoli* and B. Occhiogrosso
DVI Communications, New York, NY

Abstract

Internet of Things (IoT) concepts are now being broadly investigated for actual deployment initiatives. Although ecosystem-wide architectures and standards are still slowly evolving and/or still lacking, some progress is being made; standardization fosters flexibility, cost-effectiveness, and ubiquitous deployment. Applications range from infrastructure and critical-infrastructure support (for example smart grid, smart city, smart building, and transportation), to end-user applications such as e-health, crowdsensing, and further along, to a multitude of other applications where only the imagination is the limit. This article discusses a specific example of an IoT application supporting Smart Campuses. Smart Campuses are part of a continuum that spans cities at the large-scale end to smart buildings at the small-scale end, and encompass universities, business parks, hospitals, housing developments, correctional facilities, and other real estate environments. The specific Use Case example covered in this article relates to an actual project to automate some key functions at a set of large campuses, but the nature of the campus is not directly revealed. After a review of the applicable IoT and control technologies, this Best Practices article describes technological solutions that were employed to support the requisite control functions and serves as an example for the applicability of IoT to Smart Campus applications.

Keywords: IoT, Smart Campus, SCADA, M2M, Emergency Generators, wireless, 900 MHz radio, ISM.

Received on 23 November 2017, accepted on 29 November 2017, published on 19 December 2017

Copyright © 2018 D. Minoli and B. Occhiogrosso, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/3.0/), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi: 10.4108/eai.19-12-2017.153483

1. Introduction – What is the IoT

The basic concept of the Internet of Things (IoT) is to enable objects of all kinds to have sensing, actuating, and communication capabilities, so that locally-intrinsic or extrinsic data can be collected, processed, transmitted, concentrated, and analyzed for either cyber-physical goals at the collection point (or perhaps along the way), or for process/environment/systems analytics (of predictive or historical nature) at a processing center, often “on the cloud”. Applications range from infrastructure and critical-infrastructure support (for example smart grid, smart city, smart building, and transportation) [1-20], to end-user applications such as e-health, crowdsensing [21], and further along, to a multitude of other applications where only the imagination is the limit (noting that the references included are only a miniscule subset of the available literature). Some refer to the field as “connected technology”. While the reach of IoT is (expected to be, or become) all-encompassing, a more well-established subset deals with Machine-to-Machine (M2M) communication, where some architectural constructs and specific Use Cases have already been defined by the standardization community, including but not limited to ETSI, the European Telecommunications Standards Institute [22, 23].

A discussion of the ecosystem entails an assessment of the end-point sensors (their capabilities, cost, power supply, communication interfaces, security, and data reduction or computing mechanisms – if any), the local edge network (typically but not always wireless [4]), the aggregating network (e.g., a Low Power Wide Area Network [LPWAN]), and the advanced analytics engines needed for appropriate processing. Figure 1 provides a logical view. Many IoT applications, especially M2M applications, require only low data-rate streams; however, some evolving applications involving real time multimedia (e.g., surveillance) entail higher data-rate streams and also specified Quality of Service (QoS) goals. Nearly all IoT streams require the basic Confidentiality, Integrity, and Availability (CIA) security mechanisms encompassing the
end-to-end environment. Table 1 provides a high-level synthesis of the IoT ecosystem.

The Use Case example covered in this article relates to an actual project to automate some key functions at large (but geographic-confined) campuses. After a review of the applicable IoT and control technologies, the article describes technological solutions that were employed to support the requisite control functions. This real-life case serves as an example for the applicability of IoT to Smart Campus applications.

Table 1. A Taxonomy Of The Requisite Synthesis To Achieve Broad-Scale Deployment Of IoT

<table>
<thead>
<tr>
<th>Area</th>
<th>Subdiscipline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOT/M2M TECHNOLOGIES</strong></td>
<td>Sensors, including electric and magnetic field sensors; radio-wave sensors; optical-, electro-optic-, and infrared-sensors; radars; lasers; location/navigation sensors; seismic sensors; environmental parameter sensors (e.g., wind, humidity, heat); pressure-wave/presence sensors, biochemical and/or radiological sensors, gunshot detection/location sensors, and vital sign sensors for e-health applications.</td>
</tr>
</tbody>
</table>

**SYSTEM ARCHITECTURES**

- Proposed IoT Architectures, e.g., Arrowhead Framework, Internet of Things Architecture (IoT-A), the ISO/IEC WD 30141 Internet of Things Reference Architecture (IoT RA), and Reference Architecture Model Industrie 4.0 (RAMI 4.0)
- M2M Architecture (ETSI High level architecture for M2M)
- Architectures particularly suited for SCADA-based legacy systems

**IOT/M2M STANDARDS**

- Layer 1, Wireless (ISM, PAN, LPWAN)
- Layer 2/3, IP, IPv6, MIPv6
- Upper Layers
- Vertical-specific

**CYBERSECURITY**

- Confidentiality
- Integrity
- Availability

2. Smart City/Smart Campus/Smart Building

There is a relatively small body of literature on the topic of smart campus; a few key references include [24-35]. In the context of infrastructure management, a subset of IoT applications apply to the physical continuum that spans a Smart City, a number of institutional campuses, and a plethora of independent smart buildings, as illustrated in Figure 2. A campus is typically comprised of several buildings under one administrative jurisdiction, such as a (private) university or college, or a hospital complex encompassing of several structures in a small geographic area. Some also consider a stadium to be a campus. A campus can also be seen as a group of clusters in various regions, but all managed by an oversight entity, for example a state university that may have a number of campuses (say two dozen or more) throughout the state, or a state prison system with a number of sites, each comprised of several buildings. An example of campuses in New York State (NYS) is included in Table 2, compiled from public sources.
Typically, one building acts as an administration office where all the campus communications might terminate, e.g., if there is a control center, and where possibly there is a Wide Area Network (WAN) handoff. In multi-site campuses, there may be one centralized site where the various data (environmental parameters, control, video, and so on) is centralized to one, say state-wide or city-wide, control center for monitoring, processing, storage, or analysis. The in-campus connectivity may be supported by campus fiber, or may not be present a priori (or even if present, not usable for M2M/IoT applications for various administrative, security, or technological reasons.) A newly built campus, e.g., a business park (for example, the Capital One Financial campus in Goochland County, Virginia) may well have interbuilding fiber connectivity, but older campuses may not have such wired connectivity. Either way, a dedicated campus network for M2M applications may be needed, and it may typically be wireless in nature.

While the applications that are being considered for Smart Cities are fairly encompassing, as seen in Table 3, the applications that are typically considered for smart campus are somewhat more limited. These might include external campus surveillance; internal and external surveillance; building Emergency Generator, Automatic Transfer Switch (ATS) and Digital Meter (DM – aka Smart Meter) monitoring and control; elevator monitoring and control; and HVAC monitoring and control. Other campus-related applications include remote door control, water leak detection, washing machine scheduler, smart parking, smart trash cans, light control, and emergency notification [24]. Energy efficiency and conservation are becoming more important, especially considering governmental mandates in many jurisdictions to reduce energy consumption by 20% by 2020 or 2025; IoT-based capabilities can facilitate the achievement of these goals (e.g., tracking the electricity use of various systems and appliances in the building by monitoring the energy usage data from a smart meter). It goes without saying that Smart Building IoT applications (e.g., occupancy, lighting, daylight harvesting, access control, fire safety, and so on) also can be considered to be part of Smart Campus applications [7].

Table 2. Example of NY State Campuses

<table>
<thead>
<tr>
<th>New York State (NYS)</th>
<th>No. of buildings</th>
<th>Total SqFt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metropolitan Transportation Authority</td>
<td>43</td>
<td>~ 11,000,000</td>
</tr>
<tr>
<td>Office of General Services</td>
<td>22</td>
<td>~ 19,000,000</td>
</tr>
<tr>
<td>Office of Mental Health</td>
<td>24</td>
<td>~ 19,000,000</td>
</tr>
<tr>
<td>City University of New York</td>
<td>14</td>
<td>~ 20,000,000</td>
</tr>
<tr>
<td>Dep. of Corrections</td>
<td>71</td>
<td>~ 38,000,000</td>
</tr>
<tr>
<td>State University of New York</td>
<td>35</td>
<td>~ 86,000,000</td>
</tr>
</tbody>
</table>
Table 3. Typical Smart City Applications

<table>
<thead>
<tr>
<th>Area</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Safety &amp; security, Intelligent Transportation Systems (including Smart Mobility, Vehicular automation and Traffic control)</td>
<td>For example, traffic monitoring, to assess traffic density and vehicle movement patterns, e.g., to adjust traffic lights to different hours of the day, special events and public safety (e.g., ambulances, police and fire trucks).</td>
</tr>
<tr>
<td>Smart Grids</td>
<td>For example, Advanced Metering Infrastructure (AMI) and Demand Response (DR)</td>
</tr>
<tr>
<td>Lighting Management</td>
<td>Control light intensity when area is empty or sparsely populated and/or when background light is adequate (e.g., depending on lunar phases, seasons, etc.).</td>
</tr>
<tr>
<td>Smart Building</td>
<td>For example, building service management, specifically for city-owned real estate to remotely monitor and manage energy utilization</td>
</tr>
<tr>
<td>Waste Management</td>
<td>For example, for disposition of public containers or city-owned properties</td>
</tr>
<tr>
<td>Sensing (including Crowdsensing, Smart Environments, and Drones)</td>
<td>Environmental monitoring, for example sensors on city vehicles to monitor environmental parameters. In crowdsensing the citizenry at large uses smartphones, wearable, and car-based sensors to collect and forward for aggregation a variety of visual, signal, and environmental data</td>
</tr>
<tr>
<td>Water Management</td>
<td>For example, to manage water usage or sprinklers, considering rain events</td>
</tr>
<tr>
<td>Surveillance/Intelligence</td>
<td>For example, streets, neighborhoods, Ring-of-Steel applications, Gunshot detection</td>
</tr>
<tr>
<td>Smart Services</td>
<td>As an example, the New York City Transit Department of Buses has recently designed a 700/800 MHz radio digital system to be deployed in up to 6,500 city buses and 1,500 non-revenue generating vehicles. Applications include advanced Computer-aided Dispatch Automatic</td>
</tr>
</tbody>
</table>

3. Early Efforts

Automatic meter reading (AMR) is a process for automatically collecting consumption information from energy metering devices or water meters and transmitting that information to a processing site, typically to process billing statements. Some basic concepts and systems were developed in the 1970s and early 1980s [35]. As noted, meters that support data transition are known as DMs or Smart Meters.

The basic Open Systems Interconnection Reference Model (OSIRM), is applicable in this context. At the lower layers one has physical and networking communication mechanisms. At the Application layer (or beyond) one has a control protocol such as SCADA (Supervisory Control And Data Acquisition), although the layering may not be perfectly pristine with this early control protocol.

At the lower layers, the issue of ubiquitous connectivity was a limiting factor. One of the design goals of the Integrated Services Digital Network (ISDN) was to support a cost-effective packet-based “D channel” that not only supported out-of-band-signaling but also cost-effective distributed data collection for meter reading, home security systems, and telemetry, effectively an early version of IoT/M2M [36]. For example, U.S. Patent 5,452,343 (September 1995) states that “this invention relates to a method and apparatus for accessing customer meters and for controlling customer devices over a telephone line” [37]; a variety of related research emerged in the late 1980s-early 1990s (e.g., but not limited to [38] - [41]). Unfortunately, ISDN proved too expensive, too complex, and not innovative enough to see broad deployment in the U.S., or for that matter in other parts of the world. More cost-effective solutions were sought, including wireless technologies that ranged from non-standard metro-level packet transmission, to 2 G and 3 G cellular. (Two decades later, the currently-evolving NarrowBand-IoT [NB-IoT], a cellular technology connecting IoT devices that replaces a GSM carrier with an NB-IoT cell and provides ~25 kbps in downlink and ~64 kbps in uplink, and/or LPWAN systems, may eventually play a key role in this arena.)
4. SCADA is an Example of M2M

Effectively, SCADA is an example of an early M2M protocol [42-50]. SCADA is a well-known control system architecture for industrial process management. SCADA concepts have roots to work done in the U.S. in the 1940s. General Electric and Westinghouse advanced the concept in the 1960s and 1970s (with the advent of computers.) The term SCADA per se came into use after the utilization of a computer-based master station became common, by the mid-1960s (e.g. Westinghouse PRODAC systems and GE GETAC systems.) SCADA has evolved through four generations: (1)"Monolithic" systems based on minicomputers (e.g., DEC PDP-11s) and the communication protocols used were proprietary. (2) "Distributed" systems, where SCADA information and command processing was distributed across multiple LAN-connected stations. (3) "Networked" systems based on standardized components connected through Internet-suite communication protocols. And, (4) "IoT/cloud based" computing, where SCADA systems have progressively adopted Internet-oriented transmission protocols and "utility computing" methods. SCADA system performs four functions: (i) Data acquisition; (ii) Networked-based data communication; (iii) Data presentation; and (iv) Control. These functions are performed by four kinds of SCADA components:

1. Sensors (either digital or analog) and control relays that directly adjoined with the managed system.
2. Remote telemetry units (RTUs), effectively small computerized units located in the field at sites where the entity to be monitored/managed resides. RTUs serve as local collection points for gathering information from sensors and delivering commands to control relays.
3. SCADA master units, high-power computer workstations or consoles that operates as the central processor. These units provide a human interface to the system and automatically manages the system under control in response to sensor inputs.
4. The communications network that connects the SCADA master unit to the dispersed RTUs.

For the purpose of this project, the campuses RTUs are located the emergency generator, the ATS, and the DM.

Modbus is a defacto protocol standard that defines how the SCADA data is communicated over networks. Modbus was originally a serial communications protocol developed in the late 1970s for use with Programmable Logic Controller (PLC) devices; the basic machinery is currently utilized for connecting many types of industrial electronic devices connected on different types of networks. Multiple RTUs and/or Intelligent Electronic Devices that supports the Modbus protocol can be connected to the same physical network to create a Modbus network. Modbus uses a basic message structure: it transacts raw words and bits. More specifically, Modbus-RTU and Modbus-TCP are the specifications on how this SCADA data is packaged for transmission over specific types of networks:

- Modbus-RTU addresses transmission of data over serial communication networks, by adding a Station ID and Cyclic Redundancy Check (CRC) trailer to the SCADA data. This approach typically operates over serial connections (RS-485.)
- Modbus-TCP addresses transmission of data over IP networks, by adding an IP header and Checksum trailer to the SCADA data.

Modbus-TCP is the more ‘modern’ solution; when usable, Modbus-TCP approaches may be ideal and afford excellent flexibility and the ability to integrate, if desired, multiple (IoT/M2M) campus applications. These environments are comprised of SCADA devices that support the Modbus-TCP protocol and utilize 10BaseT Ethernet (or faster) for their connectivity. In Modbus-TCP the SCADA data payload is wrapped with TCP/IP; the devices then communicate over a Modbus network structured with an IP infrastructure (e.g., an intranet, if desired.) In large or tall buildings, however, there may be distance limitations for the raw Ethernet runs.

Modbus-RTU uses RS-485 links to connect the devices to the local controller. Depending on the height, conduits, and cable runs of the building, the 100-meter limit of Ethernet may be exceeded, and intermediary (active) switched may be required. RS-485 (also called TIA-485) is a serial interface that allows up to 32 devices to communicate in a half-duplex mode on a single pair of wires (plus a ground wire), at distances up to 1200 m. All devices are individually addressable, allowing each device to be accessed independently. The RS-485 standard specifies differential signaling on two lines; the information is transmitted differentially to provide high noise immunity over the twisted pair medium. An RS-485 arrangement can be configured as "two-wire" or "four-wire." In the "two-wire" case the transmitter and receiver of each device are connected to a twisted pair, while "four-wire" arrangements have one master port with the transmitter connected to each of the "slave" receivers on one twisted pair (the "slave" transmitters are all connected to the "master" receiver on the second twisted pair.) Only one device can actively drive the line at a time. Two-wire RS-485 networks have lower wiring costs and the ability for nodes to communicate amongst themselves but transmission is limited to half-duplex; four-wire arrangements allow full-duplex operation, but are limited to master-slave setups where a "master" node must request information by polling individual "slave" nodes ("slave" nodes cannot communicate with each other.)

5. Applicable Radio Technologies

For campus wireless connectivity, typically, one wants to make use of license-free Industrial, Scientific, and Medical (ISM) bands. While a number of such bands exist, the ISM unlicensed radio band at 900 MHz (specifically at 902-928 MHz) may optimally be employed due to better weather-related performance, due to the reduced congestion from Wi-Fi and other devices (operating in the 2.4 GHz or 5 GHz
region), and due to the support for “long distance links”, being that these links can span several miles. However, wireless services operating in the ISM band(s) must intrinsically need to clear 60%; a

Trees and other obstructions can be a problem. 900 MHz

Case Study

Edged Execution Environments (TEEs)

Fresnel Zone clearance. In order to obtain proper

Antenna gain. This relates to the amount of signal
nenvironment. For a given physical size, the antenna gain at

Effective Transmit Power Limitations. The FCC Part 15
rules limit the Effective Transmit Power of transmitters
in the ISM bands to 36 dBm. The Maximum transmitter
output power into the antenna must not exceed 30 dBm
(1 watt) and the Maximum Effective Isotropic Radiated
Power (EIRP) must be less than 36 dBm (4 watts).

Antenna gain. This relates to the amount of signal energy received. The gain of a reflector-type antenna increases as one increases the area of the parabolic surface. For a given physical size, the antenna gain at 2.4 GHz is higher than an antenna at 900 MHz (e.g., for a semi-parabolic grid antenna measuring 40x24 inches, has a 15 dBi gain at 900 MHz and 24 dBi at 2.4 GHz). For small campuses (e.g., 1 mile x 1 mile), the use of a whip (omnidirectional) or Yagi (directional antenna) may suffice, although both of these have low gain.

For the purpose of this Use Case we assume that the campuses in question are relatively small: 1 mile x 1 mile (or at most, 2 miles x 2 miles); the institutional campuses (universities, housing complexes, hospitals, business parks) fit this description. Some of the transmission considerations to be taken into account include the following:

• Signal attenuation, such as free space loss (FSL) and atmospheric attenuation. FSL is due to propagation, according to the laws of electromagnetism; attenuation relates to the spreading of the wave front in free space (vacuum). This is \[ L_{dB} = 20 \log_{10} \left( \frac{d}{\lambda} \right) \], where d is the distance and \( \lambda \) is the wavelength of the transmission [51]. For any given distance the free space loss at 2.4 GHz is 8.5 dB larger than at 900 MHz. For small campuses (e.g., 1 mile x 1 mile), the FSL loss is relatively small. Oxygen, water vapor, fog and rain will add to the FSL attenuation (their effects are worst at 2.4 GHz); however, the total attenuation is still fairly small and is usually no worse than 0.02 dB/Km. For small campuses (e.g., 1 mile x 1 mile) this attenuation a non-issue in most reasonable weather conditions.

• Trees and other obstructions can be a problem. 900 MHz transmission (and much more so at 2.4 GHz) mode requires Line of Site (LOS) (or at least Near LOS) for proper and predictable operation (trees typically cause more higher attenuation at 2.4 GHz.) The expectation is that for small campuses (e.g., 1 mile x 1 mile) that have tall buildings (8-10-12-14 stories high), tree will not be an issue; however, intervening buildings will be an issue – to address this challenge, repeaters will be used in the appropriate topological configuration. Regardless, the design goal is to elevate the antennas so that one clears all obstructions.

• Fresnel Zone clearance. In order to obtain proper propagation conditions one typically need to clear 60% of the first Fresnel zone (a long imaginary ellipsoid between the two end points). At 900 MHz, for a 1 Km link one will need one to elevate the antennas 6.5 meters above the roof line on both sides to clear obstruction (e.g., another building), at mid-point.

These parameters (and some others) need to be fed into a Link Budget Analysis calculation, to ascertain that there is sufficient transmission and reception margin. For small campuses (e.g., 1 mile x 1 mile) the expectation is that the margins are adequate when using typical off-the-shelf radio components. Round-robin polling by the SCADA master allows a conflict-free management of the radio channel and transmissions.

IoT Security (IoTSec) in general, as well as and especially in the case of critical infrastructure and/or wireless links, is very important [52] – [54]. Link encryption, encryption of data at rest, and Trusted Execution Environments (TEEs) (also Intel’s Trusted Execution Technology [TXT] and others) at the Operating System (OS) level are needed at a minimum.

6. Case Study

This case study is drawn from actual deployment projects. It deals with interconnecting emergency generators on roof of buildings in institutional campuses, where the ATS and DM is located in the basement. The campus may or may not have available fiber, therefore a radio network is needed to interconnect the various buildings to a designated administrative building. That building may have a control center, or in the case of a larger agency there may be clusters of campuses over a geographic region, with only one centralized city-wide or region-wide control center; in this case it is assumed that a WAN network is present to interconnect the dispersed campuses to the control center. The electrical devices are SCADA controlled. There will be a need to connect the RTUs in the basement and the RTU at the generator on the roof. Because the building may be tall, the Modbus-RTU (RS-485) approach is used. These networks can be variously classified as Campus Area Networks (CANS), Neighborhood Area Networks (NANS), or even Field Area Networks (FANS).
Figure 3 depicts an example of a deployment at the logical level. The actual project entails providing connectivity at 30+ campuses with an average of 8 buildings per site (but some campuses have a larger number of buildings.) These campuses are not greenfield. All buildings that do not have fiber will be equipped with radios. Roof-top radios and equipment will be housed in a NEMA enclosure. Omnidirectional whip antennas are planned to be used, but if directional Yagis are needed (perhaps in very high-density campuses), they will be used. The goal is to create star topologies with LOS links, as shown in an illustrative example in Figure 4. If repeaters are needed due to building obstructions, they will be judiciously employed as illustrated in Figure 5. Strong link encryption is utilized for security.
Conclusion

This paper described a real-life Use Case of an IoT/M2M/SCADA application in a Smart Campus environment.

References


[34] A. Alghamdi, S. Shetty, "Survey Toward a Smart Campus Using the Internet of Things", Future Internet of...


BIOS

Daniel Minoli, Principal Consultant, DVI Communications, has published 60 well-received technical books, 300 papers and made 85 conference presentations. He has many years of technical-hands-on and managerial experience in planning, designing, deploying, and operating secure IP/IPv6-, VoIP, telecomm-, wireless-, satellite- and video networks for global Best-In-Class carriers and financial companies. Over the years, Mr. Minoli has published and lectured extensively in the area of M2M/IoT, network security, satellite systems, wireless networks, IPv6/Metro Ethernet, video/IPTV/multimedia, VoIP, IT/Enterprise Architecture, and network/Internet architecture and services. Mr. Minoli has taught IT and Telecommunications courses at NYU, Stevens Institute of Technology, and Rutgers University.

Benedict Occhiogrosso is a Co-Founder of DVI Communications. He is a graduate of New York University Polytechnic School of Engineering. Mr. Occhiogrosso's experience encompasses a diverse suite of technical and managerial disciplines including sales, marketing, business development, team formation, systems development, program management, procurement and contract administration budgeting, scheduling, QA, technology operational and strategic planning. As both an executive and technologist, Mr. Occhiogrosso enjoys working and managing multiple client engagements as well as setting corporate objectives. Mr. Occhiogrosso is responsible for new business development, company strategy, as well program management. Mr. Occhiogrosso also on occasion served as a testifying expert witness in various cases encompassing patent infringement, and other legal matters.