EAI Endorsed Transactions
on Smart Cities

Review Article EAI.EU

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

doi: 10.4108/_____

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

*Corresponding author. daniel.minoli@dvicomm.com

end-to-end environment. Table 1 provides a high-level synthesis of the IoT ecosystem.

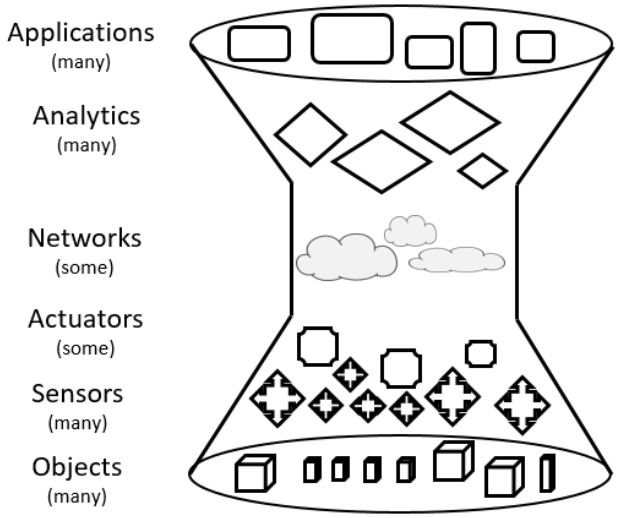

Figure 1. A Logical View of an IoT Ecosystem

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

Area	Subdiscipline
IOT/M2M TECHNOLOGIES	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.
	Networking (especially wireless technologies for personal area networks, fogs, and cores, such as 5G cellular)
	Analytics
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
CYBERSECUTITY	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.

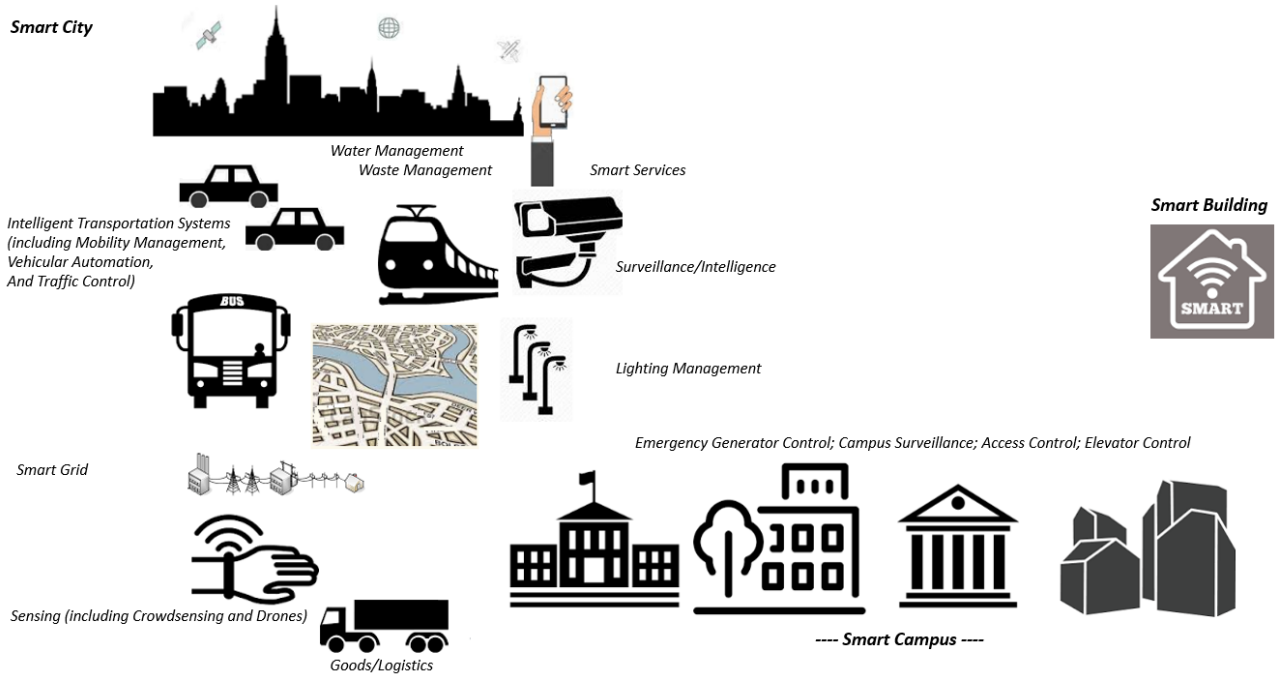

Figure 2. Graphical View of Smart City, SMART Campus, Smart Building Continuum

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

New York State (NYS) Agency Name	No. of buildings	Total SqFt
Metropolitan Transportation Authority	43	~ 11,000,000
Office of General Services	22	~ 19,000,000
Office of Mental Health	24	~ 19,000,000
City University of New York	14	~ 20,000,000
Dep. of Corrections	71	~ 38,000,000
State University of New York	35	~ 86,000,000

Table 3. Typical Smart City Applications

Area	Examples
Public Safety & security, Intelligent Transportation Systems (including Smart Mobility, Vehicular automation and Traffic control)	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).
Smart Grids	For example, Advanced Metering Infrastructure (AMI) and Demand Response (DR)
Lighting Management	Control light intensity when area is empty or sparsely populate and/or when background light is adequate (e.g., depending on lunar phases, seasons, etc.).
Smart Building	For example, building service management, specifically for city-owned real estate to remotely monitor and manage energy utilization
Waste Management	For example, for disposition of public containers or city-owned properties
Sensing (including Crowdsensing, Smart Environments, and Drones)	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
Water Management	For example, to manage water usage or sprinklers, considering rain events
Surveillance/Intelligence	For example, streets, neighborhoods, Ring-of-Steel applications, Gunshot detection
Smart Services	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 Vehicle Location to track the position of buses in real-time via Global Positioning System (GPS) using cellular overlay mechanisms and provide advanced fleet management and next-bus time of arrival notification at bus stops throughout the region and on customer smartphones.
Goods and products Logistics (including Smart Manufacturing)	For example, optimized transportation, warehousing, goods tracking, trucks monitoring

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 accept potential interference from other users since there is no regulatory protection from ISM device operation: the transmissions of near-by devices using ISM (e.g., including other similar radios, cordless phones, Bluetooth devices) can give rise to electromagnetic interference and disrupt radio communication utilizing the same frequency. Fortunately, there are power restrictions mandated by FCC to minimize interference and thus unlicensed low power users are generally able to operate in these bands without being impacted by or causing problems to other ISM users. Traditional Spread Spectrum techniques, where a radio signal generated with a particular bandwidth is by design spread in the frequency domain into a signal with a wider bandwidth, will reduce the interference (however, Spread Spectrum system are slightly more expensive than normal transmitter-receivers.)

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 $L_{dB} = 21.98 + 20*log_{10}(d/\lambda)$, where d is the distance and λ 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.
- Effective Transmit Power Limitations. The FCC Part 15 rules limits 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.

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.

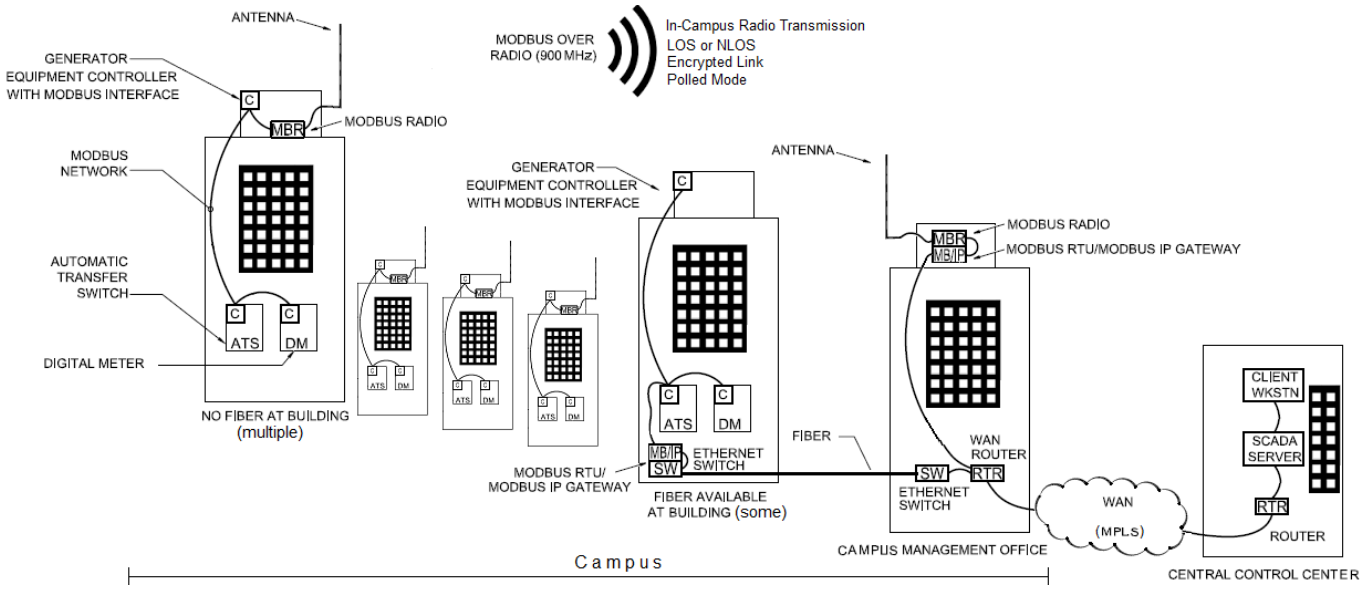

Figure 3. Logical View of IoT/SCADA Design

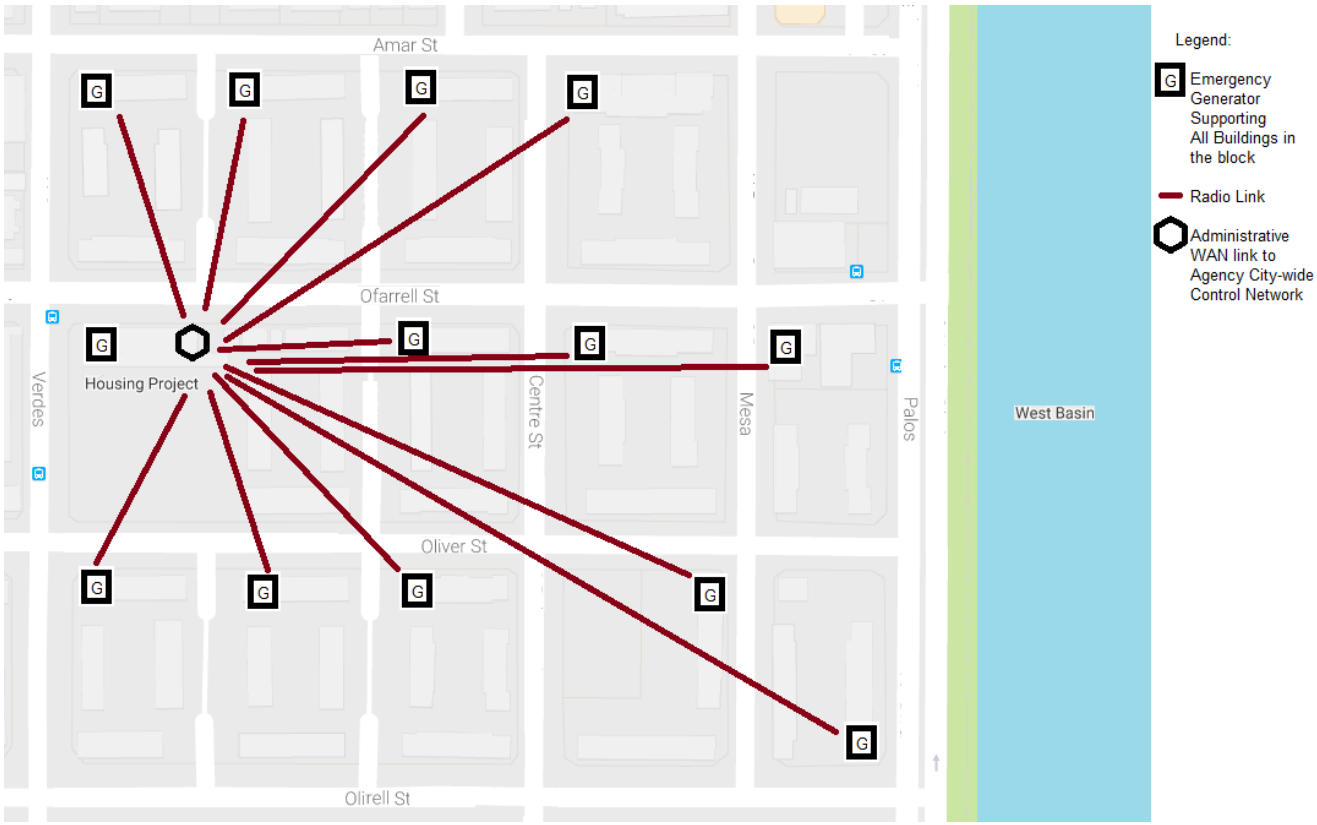

Figure 4. Example of IoT/SCADA Design for a Campus (LOS Solution)

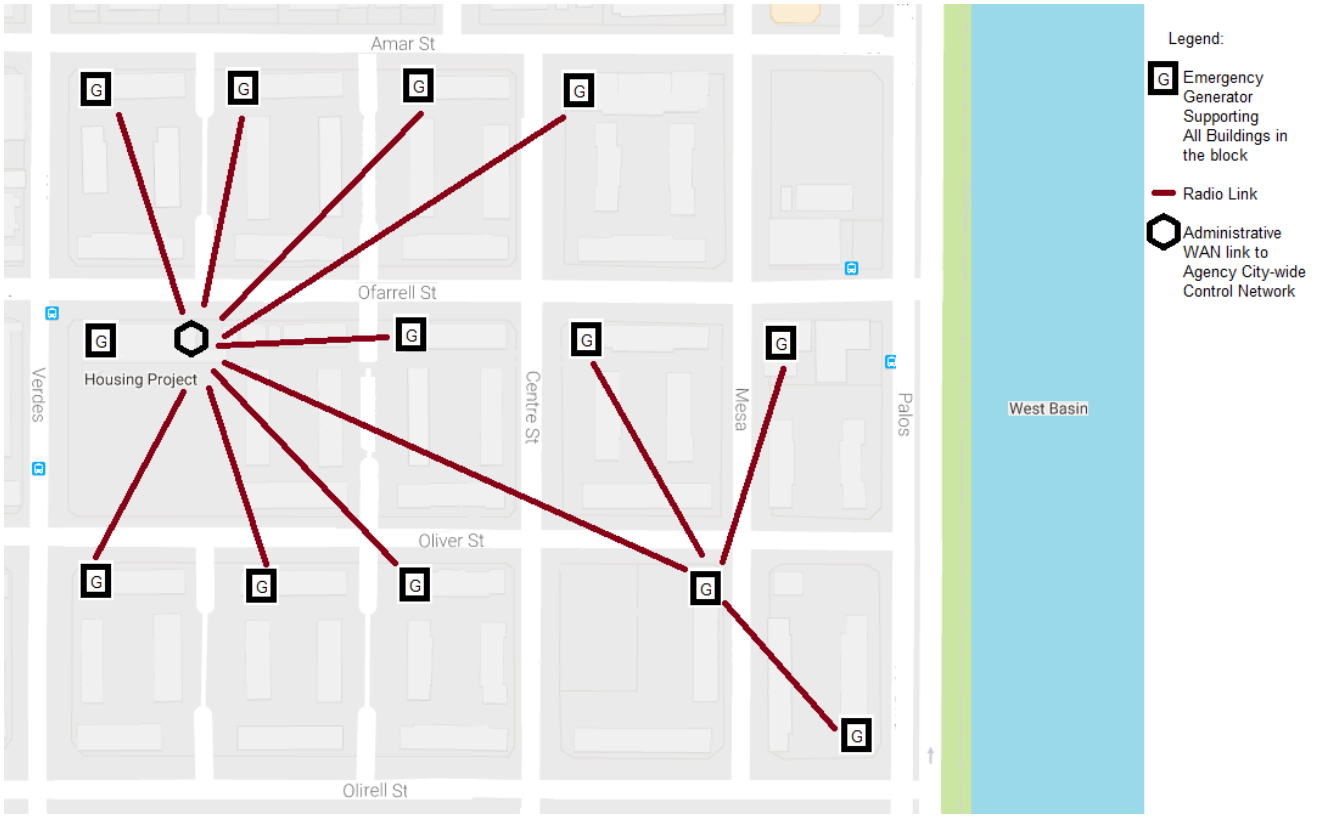

Figure 5. Example of IoT/SCADA Design for a Campus (Repeater Solution)

Conclusion

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

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communication Surveys & Tutorials, Vol. 17, No. 4, Fourth Quarter 2015 pp. 2347ff.

[2] D. Minoli, *Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications,* Wiley 2013.

[3] D. Minoli, *Innovations in Satellite Communication and Satellite Technology — The Industry Implications of DVB-S2X, High Throughput Satellites, Ultra HD, M2M, and IP,* Wiley 2015.

[4] K. Shoraby, D. Minoli, T. Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications,* Wiley 2007.

[5] N. Mali, "A Review on Smart City through Internet of Things (IoT)", International Journal of Advanced Research in Science Management and Technology, Volume 2, Issue 6, June 2016.

[6] D. Kyriazis, T. Varvarigou, D. White, A. Rossi, J. Cooper, "Sustainable smart city IoT applications: Heat and Electricity Management & Eco-conscious cruise control for public transportation", World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th Internat. Symp. and Workshops, 4-7 June 2013.

[7] D. Minoli, et al, "IoT Considerations, Requirements, and Architectures for Smart Buildings – Energy Optimization and Next Generation Building Management Systems", IEEE IoT Journal, February 2017.

[8] H. T. Mouftah, M. Erol-Kantarci, *Smart Grid - Networking, Data Management, and Business Models*, CRC Press, New York, 2016.

[90] S. F. Bush, *Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid*, Wiley-IEEE Press, March 2014, ISBN: 978-1-119-97580-9.

[10] A. Carvallo, J. Cooper, *The Advanced Smart Grid: Edge Power Driving Sustainability*, Second Edition: Edge Power Driving Sustainability, Artech House, Norwood, Mass. 2015. ISBN: 9781608079636.

[11] K. Shoraby, D. Minoli, B. Occhiogrosso, "A Review of Wireless and Satellite-based M2M Services in Support of Smart Grids. 1st EAI International Conference on Smart Grid Assisted Internet of Things", SGIoT 2017, July 12–13, 2017, Sault Ste. Marie, Ontario, Canada.

[12] F. Shroufa, G. Miragliottaa, "Energy Management Based On Internet Of Things: Practices And Framework For Adoption In Production Management", Journal of Cleaner Production, Volume 100, 1 August 2015, Pages 235–246, http://dx.doi.org/10.1016/j.jclepro.2015.03.055.

[13] N. Bui, A. P. Castellani, P. Casari, M. Zorzi, "The Internet Of Energy: A Web-Enabled Smart Grid System", IEEE Network (Volume: 26, Issue: 4, July-August 2012), 23 July 2012, DOI: 10.1109/MNET.2012.6246751.

[14] J. Serra, D. Pubill, A. Antonopoulos, and C. Verikoukis, "Smart HVAC Control in IoT: Energy Consumption Minimization with User Comfort Constraints", The Scientific World Journal, Volume 2014 (2014), Article ID 161874.

[15] L. Kang, S. Poslad, W. Wang, X. Li, Y. Zhang, C. Wang, "A Public Transport Bus as a Flexible Mobile Smart Environment Sensing Platform for IoT", Intelligent Environments (IE), 2016 12th International Conference on, Sept. 2016, DOI: 10.1109/IE.2016.10.

[16] S. H. Sutar, R. Koul, R. Suryavanshi, "Integration of Smart Phone and IoT for Development Of Smart Public Transportation System", Internet of Things and Applications (IOTA), International Conference on, 22-24 Jan. 2016, DOI: 10.1109/IOTA.2016.7562698.

[17] D. Minoli, B. Occhiogrosso, "Internet of Things (IoT)-based Apparatus And Method For Rail Crossing Alerting Of Static Or Dynamic Railtrack Intrusions", Proceedings of Joint Rail Conference (JRC), April 4-7, 2017, Philadelphia, PA.

[18] M. Ferretti, F. Schiavone, "Internet Of Things (IoT) And Business Processes Redesign In Seaports: The Case Of Hamburg", Business Process Management Journal, Vol. 22 Issue: 2, pp.271 – 284, 2016.

[19] L. Cai, W. Xia, P. Li, L. Zhang, J. Liu, "An Intelligent Transportation System For Hazardous Materials Based On The Internet of Things (IoT)", 4th International Conference on Information Technology and Management Innovation (ICITMI 2015), October 2015.

[20] A. Roy, J. Siddiquee, A. Datta, P. Poddar, G.Ganguly, A. Bhattacharjee, "Smart Traffic & Parking Management Using IoT", Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual, Date of Conference: 13-15 Oct. 2016, DOI: 10.1109/IEMCON.2016.7746331.

[21] Q. Wang, et al, "Multimedia IoT Systems and Applications", Global IoT Summit (GIoTS-2017), Organized by Mandat International, IEEE IoT TsC, the IoT Forum and IPv6 Forum (collocated with the IoT Week), 6-9 June 2017, Geneva, Switzerland.

[22] ETSI, ETSI TS 102 690: Machine-to-Machine communications (M2M); Functional architecture. October 2011. Online at http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf

[23] ETSI, ETSI TR 102 691: "Machine-to-Machine Communications (M2M); Smart Metering Use Cases". (2010-05). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex – France.

[24] Various Speakers, "Part I: Smart Campus And IoT", Collaborative Innovation Community Meeting - Internet2, 2016 Technology Exchange, Sept. 25-28, 2016, Miami, FL.

[25] Z. Yu, Y. Liang, B. Xu, Y. Yang, B. Guo, "Towards a Smart Campus with Mobile Social Networking", Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, 19-22 Oct. 2011, Dalian, China.

[26] Y. Huang, S. Ali, X. Bi et al, "Research on Smart Campus Based on the Internet of Things and Virtual Reality", International Journal of Smart Home, Vol.10 No.12 (Dec 2016), pp.213-220.

[27] O. Bates, A. Friday, "Beyond Data In The Smart City: Learning From A Case Study Of Re-Purposing Existing Campus IoT", IEEE Pervasive: Special Issue on Smart Buildings and Cities, Jan. 2017.

[28] R. Gomes, H. Pombeiro, C. Silva et al, "Towards a Smart Campus: Building-User Learning Interaction for Energy Efficiency, the Lisbon Case Study", Handbook of Theory and Practice of Sustainable Development in Higher Education, Part of the series World Sustainability Series pp 381-398, November 2016.

[29] L. Zhang, O. Oksuz, L. Nazaryan et al, "Encrypting Wireless Network Traces To Protect User Privacy: A Case Study For Smart Campus", Wireless and Mobile Computing, Networking and Communications (WiMob), 2016 IEEE 12th International Conference on, 17-19 Oct. 2016.

[30] Y-B. Lin, J-H, Chen, "Keynote Speech 2: Implementing smart campus through IoTtalk", Communication Problem-Solving (ICCP), 2016 International Conference On, 7-9 Sept. 2016.

[31] H. Li, G. Shou, Y. Hu, Z. Guo, "WiCloud: Innovative Uses Of Network Data On Smart Campus", Computer Science & Education (ICCSE), 2016 11th International Conference on, 23-25 Aug. 2016.

[32] J-Y. Rha, J-M. Lee, H-Y. Li et al "From a Literature Review to a Conceptual Framework, Issues and Challenges for Smart Campus", Journal of Digital Convergence, Volume 14, Issue 4, 2016, pp.19-31, Publisher: The Society of Digital Policy and Management, DOI: 10.14400/JDC.2016.14.4.19.

[33] G. Lazaroiu, V. Dumbrava, M. Costoiu et al, "Energy-Informatic-Centric Smart Campus", Environment and Electrical Engineering (EEEIC), 2016 IEEE 16th International Conference on, 7-10 June 2016, Florence, Italy.

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

Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on, 22-24 Aug. 2016, Vienna, Austria.

[35] T. Paraskevakos, “Sensor Monitoring Device”, U.S. Patent 3,842,208, July 1972. And, T. Paraskevakos, W. Bushman, “Apparatus and Method for Remote Sensor Monitoring, Metering and Control”, U.S. Patent 4,241,237 (Dec. 1980). And, T. Paraskevakos, W. Bushman, “Apparatus and Method for Remote Sensor Monitoring, Metering and Control”, U.S. Patent 4,455,453 (June 1984).

[36] CCITT (now ITU-T) Recommendation I.440 (Q.920) ISDN User-Network Interface Data Link Layer-General Aspects, VIIIth Plenary Assembly, October 1984. And, CCITT Recommendation I.441 (Q-921) ISDN User-Network Interface Data Link Layer Specification, VIIIth Plenary Assembly, October 1984. And, CCITT Recommendation I.450 (Q-930) ISDN User-Network Interface Layer 3-General Aspects, VIIIth Plenary Assembly, October 1984. CCITT Recommendation I.451 (Q-931) ISDN User-Network Interface Layer 3 Specification, VIIIth Plenary Assembly, October 1984.

[37] S. M. Garland, J.W. Schull, "Telemetry Access Arrangement", U.S. Patent 5,452,343, Sept. 1995.

[38] N. A. Albal, "Transparent Packet Access Over D-channel of ISDN", U.S. Patent 4,755,992, July 1988.

[39] S.M. Garland, "Remotely Initiated Telemetry Calling System", U.S. Patent 5,327,488, July 1994.

[40] S.M. Garland, D.B. Smith, "Communications Between Service Providers and Customer Premises Equipment", U.S. Patent 6,167,042, Dec. 2000.

[41] S. M. Garland, "Telemetry Feature Protocol Expansion", U.S. Patent 5,394,461, Feb. 1995.

[42] H. T. Mouftah, M. Erol-Kantarci, Smart Grid - Networking, Data Management, and Business Models, CRC Press, New York, 2016.

[43] S. F. Bush, Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid, Wiley-IEEE Press, March 2014, ISBN: 978-1-119-97580-9.

[44] C. Wietfeld, H. Georg, S Gröning, et al “Wireless M2M Communication Networks for Smart Grid Applications”, Wireless Conference 2011 - Sustainable Wireless Technologies (European Wireless), 11th European, 27-29 April 2011, pages 1-7.

[45] Z. M. Fadlullah, M. M. Fouda, N. Kato, et al, "Toward intelligent Machine-To-Machine Communications In Smart Grid", IEEE Communications Magazine, April 2011, Volume: 49 Issue: 4.

[46] M. H. Rehmani, A. A. Khan, M. Reisslein, "Cognitive Radio for Smart Grids: Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols", IEEE Communications Surveys & Tutorials (Volume: 18, Issue: 1, Firstquarter 2016).

[47] National Communications System, Supervisory Control and Data Acquisition (SCADA) Systems, Technical Information Bulletin 04-1, NCS TIB 04-1, October 2004, P.O. Box 4052, Arlington, VA 22204-4052. http://www.ncs.gov.

[48] A. A. Cárdenas, R. Berthier, et al: “A Framework for Evaluating Intrusion Detection Architectures in Advanced Metering Infrastructures”, IEEE Trans. Smart Grid 5(2): 906-915 (2014).

[40] M. Singh, E. V. Sanduja, "Minimizing Electricity Theft by Internet of Things", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015.

[50] S. K. Tan, M. Sooriyabandara, and Z. Fan, "M2M Communications in the Smart Grid: Applications, Standards, Enabling Technologies, and Research Challenges", International Journal of Digital Multimedia Broadcasting, Volume 2011 (2011), Article ID 289015.

[51] D. Minoli, *Satellite Systems Engineering in an IPv6 Environment*, Francis and Taylor 2009.

[52] D. Minoli et al, “IoT Security (IoTSec) Considerations, Requirements, and Architectures”, IEEE CCNC 2017, January 2017.

[53] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the IoT: A Survey of Existing Protocols and Open Research Issues", IEEE Comm. Surveys & Tutorials, Vol. 17, No. 3, 2015, pp. 1294ff.

[54] C. Lai, R. Lu, D. Zheng, H. Li, and X. Shen, "Toward Secure Large-Scale Machine-to-Machine Communications in 3GPP Networks: Challenges and Solutions", IEEE Communications Magazine Communications Standards Supplement, December 2015, pp.12ff.

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, telecom-, 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, IP/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.