

IBM White Papers

ERIS Infotext

Application Security Considerations
ACHIEVING USABILITY AND SECURITY
IN A SITUATIONAL AWARENESS SYSTEM
.....PAGE 2

ERIS Infotext

Analysis and Vision on Sensor Devices
INTEGRATING REAL-TIME SENSOR DATA
WITH BUILDING MODELS
FOR IMPROVED SITUATIONAL AWARENESS
.....PAGE 8

ERIS Infotext

Systems Integration with SOA
USING SERVICE ORIENTED ARCHITECTURE
FOR A FLEXIBLE AND EXTENSIBLE
SITUATIONAL AWARENESS SYSTEM
.....PAGE 12

ERIS Infotext

Mobile Information Access
USING MOBILE WIRELESS TECHNOLOGY
FOR AN EFFECTIVE SITUATIONAL
AWARENESS SYSTEM
.....PAGE 16

e-IDC is a technology aggregator and infrastructure provider located in Annapolis, Maryland.

Application Security Considerations

ACHIEVING USABILITY AND SECURITY IN A SITUATIONAL AWARENESS SYSTEM

Real-Time Situational Awareness

Situational awareness is a term that has become a buzzword in the recent times. It is, perhaps, especially so due to the heightened level of intensity of the struggles occurring in many places of the world that result from acts of terrorism, warfare, or natural disasters. Stakeholders involved in these conflicts and events are required to have a deep level of understanding of their relevant environmental conditions to be able to respond effectively. The term situational awareness refers to three levels of understanding: *the perception of elements; the comprehension of their meaning; and the ability to utilize that comprehension to project future states.*

It is very clear that situational awareness is a critical factor when responding to an emergency situation. The ability to fully perceive and comprehend the state of the relevant environment and the ability to make accurate projections to alter the course of future actions almost completely determines the nature of the response outcomes. In highly charged, mission-critical situations, such as a building fire, or a hostage situation, this factor becomes even more crucial. Decisions must be made within a very short timeline, or structures may collapse and lives may be lost in the process. The ability to acquire situational awareness instantaneously, in real-time, is a requirement for avoiding and minimizing irreparable loss.

Protecting Security and Privacy

While a process for real-time information distribution is critical to achieving higher level situational awareness, it is just as important to ensure that unauthorized access and modification of that information—whether in storage, processing, or in transit—can be prevented. The temptation to allow the highest level of flexibility cannot be greater than during a crisis. In an emergency, perhaps a building fire, or a hostage situation, when the pressure is high for quick access to critical information, it is human nature to perceive the need to be flexible and to disclose any information that can be helpful to resolve the crisis. Unfortunately, criminals understand this trait too well, and have

e-IDC is a technology aggregator and infrastructure provider located in Annapolis, Maryland.

repeatedly taken advantage of this weakness through the application of social engineering—resulting in the compromise of security and privacy and the loss of valuable assets.

Technology can provide the solution for secure, real-time situational awareness. Information systems security deals with the protection of information and the different levels of trust necessary to guarantee confidentiality, uncompromised integrity, and availability. With the proper application of information systems security tools and techniques, the accidental disclosure of private information to unauthorized individuals can be prevented, and the risk of losing of valuable assets can be minimized—even during a time of ongoing crisis.

Risk Factors and Countermeasures

Some of the critical issues that involve information systems security and data privacy include: unauthorized access, improper information disclosure, and compromised operation or loss of service due to hostile actions.

A system that provides improved situational awareness by overlaying 3-dimensional building models and real-time sensor information will contain functions for the timely and accurate collection, analysis, and distribution of critical information.

When access to a situational awareness system is compromised, whether it is prior to or during an emergency situation, the responsible stakeholders—first responders, building owners and managers, and building tenants—cannot continue to rely on the proper operation of the system and the accuracy of the information produced by the system, rendering it unusable. For example, a criminal who has successfully gained unauthorized access to the system may be able to manipulate sensor data, alter the system analysis logic, and disseminate false information to achieve his or her malicious goals.

Similarly, when private information has been compromised through improper disclosure, accidental or not, the operability of the system will be greatly threatened. Sensitive and private information is priceless and its loss or disclosure may cause irreparable damage to the owners. Building models can contain information about the locations and operations of critical infrastructure that could be dangerous in the hands of criminals. The system may also include private information about the building owners, managers, and tenants, such as contact information and physical location. When data owners cannot trust the system to keep their private data secure and inaccessible to those without the proper authority, they will cease use of the system.

Lastly, it is not uncommon for criminals to conduct information security warfare, attacking their target through the misuse of computer hacking techniques, including denial of service and other malicious attacks. A

system that is unable to protect itself from such actions will be rendered useless during a time of crisis.

■ **Managing access.** With the application of role-based access control (RBAC), users of the system are permitted access to various levels of privileges based on the roles to which they have been assigned. This practice allows the simplified provision and management of user access rights.

In conjunction with RBAC, the system could support short-term identities with limited access privileges that could be generated and quickly provisioned for those users that may need access for a very limited time—which is a very common use case during a crisis. The credentials used for these short-term identities are system generated user ID and password that are distributed through out-of-band and trusted channels, and will automatically be invalidated after a preconfigured interval of time. Longer term identities are granted to those users with the need for more permanent access. The credentials for these users may include digital certificates, hardware tokens, biometrics, and other, more trusted, forms of identification. The advantage of this approach is that the lifetime of user identities will correlate more closely with the duration of user needs for access, while at the same time higher levels of manageability and usability are achieved.

By necessity, the system will also manage various types of data with different owners, security levels, and privacy requirements. To enable the proper handling of these data, they must be classified clearly ahead of time. Based on the classification, some may have to be strongly encrypted and made available to a limited set of user roles, and some may only be used in a derivative form, using secure hash algorithms. The proper classification of data ownerships and trust requirements is a key factor in ensuring data security and privacy.

To comply with US government regulations, as well as to aid recovery and investigation in the case of a security breach, the system will include a secure and auditable logging facility that records all security-relevant events—such as system configuration changes, identity changes, data manipulation, and others.

■ **Protecting data security and integrity.** For protecting data security, data that are stored at various points—client machine, and various proxy and server machines—must be encrypted or be stored along with digital signatures based on their levels of privacy and trust requirements.

Strong symmetric encryption algorithms, such as *Rijndael*, or the *Advanced Encryption Standard* (AES), could be used to ensure the highest level of data security and adherence to US government standards. In addition, communications between transitory points that involve such private data could occur over secured channels, using *Secure Socket Layer* (SSL) and *Transport Layer Security* (TLS) along with the *Hypertext Transfer Protocol* (HTTP). Other situations will require

assurance of data integrity, but not privacy. In this case, the *Secure Hash Algorithm* SHA-1 or other standard digital signature algorithms must be used to provide an indicator of data integrity.

The technical measures above will ensure that if access to any machine or network containing private information has been compromised, the protected information will not be usable to the perpetrators without knowledge or possession of the proper encryption keys and that any attempt to alter the contents of protected data will be immediately and clearly apparent.

■ **Protecting against hostile actions.** Although the openness of the public network delivers many benefits for a situational awareness system, such as a higher level of accessibility, it also opens up the door to possible cyber attacks that could result in compromised operations or, at the extreme, loss of service. A sound and well-designed system architecture that addresses security concerns from its foundation and builds into its network infrastructure the best practices for implementing a *layered security approach* could mean the difference between a secure and functional system and one that is inoperable.

A layered security approach means that the network infrastructure is protected at its perimeters with well configured firewalls, intrusion detection and protection systems, and anti-virus software to keep bad traffic off the network. Beyond this first layer, traffic management systems will help recognize traffic anomalies and automate, through the application of well-defined policies, the redirection or reshaping of bandwidth assignments to ensure network availability for the mission critical applications. Next, on the application gateway, the use of SSL *virtual private networks* (VPN) and application-level filters will ensure that traffic reaching this point is clean, efficient, and secure. Lastly, on the host machines, the use of antivirus software, host-based intrusion detection and protection systems, spam filters, and others will provide the protection necessary from attacks clever enough to bypass the previous layers of protection.

To ensure a consistent level of protection from hostile actions, periodic reviews of system security through penetration testing—including white box, gray box, and black box testing efforts—which involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities, and periodic system auditing must be conducted.

In conclusion, it is clear that despite the risk factors that are present involving the attempt of unauthorized access, the potential compromise of data privacy and integrity and the execution of hostile actions, a situational awareness system could be made highly secure and private through the applications of proper technical measures and best practices.

ERIS Features and Benefits

ERIS, an acronym for *Emergency Response Information System*, is an upcoming product of *e-IDC* that will provide a tool to help responsible stakeholders in mission-critical situations to acquire a high-level of situational awareness of affected buildings, structures, and objects. It integrates interactive 3-dimensional models of buildings and structures, and real-time information on animate and inanimate objects acquired from sensor devices or input by human operators in a service oriented application. By overlaying these components and providing a graphical user interface that visualizes the objects and environment and allows their direct manipulation, ERIS supplies the level of detail necessary for acquiring situational awareness—before, during, and after an emergency.

REFERENCES

Bruce Schneier:

[Applied Cryptography](#)

<http://www.schneier.com/book-applied.html>

Wikipedia:

[Information Security](#)

http://en.wikipedia.org/wiki/Information_security

Wikipedia:

[Advanced Encryption Standard](#)

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

e-IDC:

[International Design and Construction Online](#)

<http://www.e-IDC.com/>

Analysis and Vision on Sensor Devices

INTEGRATING REAL-TIME SENSOR DATA
WITH BUILDING MODELS
FOR IMPROVED SITUATIONAL AWARENESS

Real-Time Situational Awareness

Situational awareness is a term that has become a buzzword in the recent times. It is, perhaps, especially so due to the heightened level of intensity of the struggles occurring in many places of the world that result from acts of terrorism, warfare, or natural disasters. Stakeholders involved in these conflicts and events are required to have a deep level of understanding of their relevant environmental conditions to be able to respond effectively. The term situational awareness refers to three levels of understanding: *the perception of elements; the comprehension of their meaning; and the ability to utilize that comprehension to project future states.*

It is very clear that situational awareness is a critical factor when responding to an emergency situation. The ability to fully perceive and comprehend the state of the relevant environment and the ability to make accurate projections to alter the course of future actions almost completely determines the nature of the response outcomes. In highly charged, mission-critical situations, such as a building fire, or a hostage situation, this factor becomes even more crucial. Decisions must be made within a very short timeline, or structures may collapse and lives may be lost in the process. The ability to acquire situational awareness instantaneously, in real-time, is a requirement for avoiding and minimizing irreparable loss.

Networked Sensor Devices

Technology advancement makes it now possible to collect, process, and distribute real-time information easily and at a relatively low cost. A class of devices called *networked sensors*, which can be wired or wireless, allow sound, images, motion, smoke, and other data to be collected and aggregated in real-time. The sensors are typically electronic or electromechanical devices that detect one type of energy and convert it into a measurement. When coupled with an application that can process and distribute the resulting information to the

e-IDC (International Design and Construction Online) is a technology aggregator and infrastructure provider located in Annapolis, Maryland.

responsible stakeholders, the combination provides the level of intelligence necessary for accurate, real-time decision making. Wireless sensors have the added benefit of not requiring existing wired infrastructure for their networked operations. In some cases, and with the right type of devices, wireless sensors can be deployed on the fly to form an ad-hoc network in a disaster location.

It's worth examining the different sensor devices presently available in the marketplace that can be used to detect human presence, smoke, fire, motion, and other pertinent information to see if and how they could be integrated to improve situational awareness at a time of crisis.

■ **Alarm annunciator panels.** Alarm annunciator panels are a centralized monitoring panel for multiple alarm sources in a building that could include heat, smoke, fire and others connected with electrical circuits. Newer models of annunciator panels incorporate features such as VGA displays, public switched telephone network interface, and the ability to inspect or poll multiple alarm sources simultaneously. The conventional analog addressable alarm annunciator panels, although not readily network-enabled, can be made so through the application of networking accessories and peripherals such as multi-channel input/output modules and network communication, modem, and serial interface modules supplied by *Telefire*.

■ **Heat, smoke and fire.** There are many products in the market for smoke and fire detection, some of which can already be monitored using a rack-mounted console system or an alarm annunciator panel.

LINDY, for example, is a company that manufactures and sells a Rack Monitoring System (RMS) that can monitor sensor signals on temperature, humidity, fire and smoke, and motion, and in turn generate alerts through a computer network. The *LINDY* RMS is programmable through direct access or a remote management console that supports the standard Simple Network Management Protocol (SNMP).

NOTIFIER Fire Systems, a part of *Honeywell International*, is a well-known manufacturer and supplier of an array of intelligent sensor and alarm panel products, including the recently introduced and showcased Smart4 (Self-optimizing Multi-criteria Alarm Recognition Technology). This is an adaptive plug-in fire detector combining four separate sensors for all common elements in a fire in a single unit: a carbon monoxide sensor, an infrared sensor, for measuring ambient light levels and flame signatures, an optical smoke detector, and a heat sensor.

■ **Motion and human presence.** The sophistication of motion detection has recently been raised with the introduction of *Siemens Building Technologies Eyetec*, the first sensor device combining a passive infrared and an optical detection system that can recognize motion patterns and capture images with a high degree of accuracy. By using embedded technology that processes infrared radiation and an optical sensor with

fuzzy logic that measures object size, speed, and direction of travel, these devices can sense the body heat of individuals and “see” them as well. When a building is equipped with these sensors, human presence can not only be detected, but also be viewed remotely from a networked computer—information that raises the level of situational awareness dramatically, that could be critical in the event of an ongoing crisis.

■ **Location and multipurpose.** Another sophisticated sensor technology has been developed at the *University of Berkeley* with the cooperation of the Chicago Fire Department. The Berkeley team designed and implemented customized smart helmets constructed of oxygen masks, wireless sensor motes, and miniature near-eye displays. Motes are tiny wireless microelectromechanical systems that are designed to detect various types of information. In the case of the Berkeley-developed device, the sensor motes monitor temperature, smoke levels, and provide position location of the wearer to the command and control post. Undoubtedly, first responders equipped with such wearable computing equipment and sensors will have, and will provide their observers, higher levels of situational awareness.

Clearly, the availability of off-the-shelf sensor products and the advances in the related telecommunication technologies which accurately capture various critical environmental measurements that can be processed, analyzed, and distributed in real-time along with other contextual information can provide deep situational awareness for first responders and other responsible stakeholders during a crisis.

ERIS Features and Benefits

ERIS, an acronym for *Emergency Response Information System*, is an upcoming product of *e-IDC* that will provide a tool to help responsible stakeholders in mission-critical situations to acquire a high-level of situational awareness of affected buildings, structures, and objects. It integrates interactive 3-dimensional models of buildings and structures, and real-time information on animate and inanimate objects acquired from sensor devices or input by human operators in a service oriented application. By overlaying these components and providing a graphical user interface that visualizes the objects and environment and allows their direct manipulation, ERIS supplies the level of detail necessary for acquiring situational awareness—before, during, and after an emergency.

REFERENCES

Wikipedia:

Situational Awareness

http://en.wikipedia.org/wiki/Situational_awareness

Wikipedia:

Wireless Sensor Network

http://en.wikipedia.org/wiki/Wireless_sensor_networks

Telefire:

Fire Alarm Systems Accessories Brochure

<http://www.telefire.co.il/Brochure%20Accessories.pdf>

LINDY:

Rack Monitoring System

<http://www.lindy.com/us/productfolder/03/32/32417/index.php>

NOTIFIER by Honeywell:

Fire Systems Products

<http://www.notifierfiresystems.co.uk/notifier.asp?L=EN>

Berkeley Research:

Bringing Firefighters Back Alive with Smart Technology

<http://research.chance.berkeley.edu/page.cfm?id=11&aid=28>

Siemens Building Technology:

Eyeteq Press Release

http://www.siemens.nl/sbt/nws/nws_051114_d.asp

e-IDC:

International Design and Construction Online

<http://www.e-IDC.com/>

Systems Integration with SOA

USING SERVICE ORIENTED ARCHITECTURE
FOR A FLEXIBLE AND EXTENSIBLE
SITUATIONAL AWARENESS SYSTEM

Real-Time Situational Awareness

Situational awareness is a term that has become a buzzword in the recent times. It is, perhaps, especially so due to the heightened level of intensity of the struggles occurring in many places of the world that result from acts of terrorism, warfare, or natural disasters. Stakeholders involved in these conflicts and events are required to have a deep level of understanding of their relevant environmental conditions to be able to respond effectively. The term situational awareness refers to three levels of understanding: *the perception of elements; the comprehension of their meaning; and the ability to utilize that comprehension to project future states.*

It is very clear that situational awareness is a critical factor when responding to an emergency situation. The ability to fully perceive and comprehend the state of the relevant environment and to make accurate projections to alter the course of future actions almost completely determines the nature of the response outcomes. In highly charged, mission-critical situations, such as a building fire, or a hostage situation, this factor becomes even more crucial. Decisions must be made within a very short timeline, or structures may collapse and lives may be lost in the process. The ability to acquire situational awareness instantaneously, in real-time, is a requirement for avoiding and minimizing irreparable loss.

Interoperability and Extensibility

In addition to providing the most useful functions, a situational awareness decision support system must also be extensible to incorporate unforeseen future requirements, the integration of future technologies and devices, as well as be interoperable with present and future external systems. This is of great consequence in particular because directives from the United States government agencies such as the *Federal Emergency Management Agency (FEMA)* and the *Department of Homeland Security (DHS)* have driven *National Incident Management*

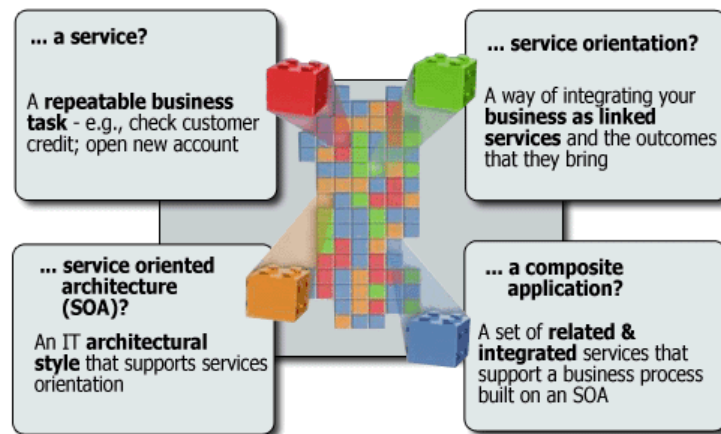
e-IDC (International Design and Construction Online) is a technology aggregator and infrastructure provider located in Annapolis, Maryland.

Systems (NIMS), Crisis Incident Management Systems (CIMS), and Integrated Incident Management Systems (IIMS) to the top of the priority lists of their own and other organizations. In order for a situational awareness system to be successfully and widely adopted, it must be interoperable with current and future systems and products that belong in the large portfolio of NIMS, CIMS, and IIMS solutions.

In addition to their importance for acceptance of the system, extensibility and interoperability are not trivial objectives for at least two reasons. The first reason is rather obvious: To begin, it is very difficult to anticipate new and changing business requirements as well as future governmental regulations. To be a highly responsive product requires the ability to reconstruct and extend the system very quickly while maintaining manageable development, support, and maintenance costs. In addition, there are so many different platforms and technologies that may underlie external systems that a significant amount of resource and effort would be required to be able to integrate with any number of them. In order to meet these vital non-functional requirements, the system must be designed and architected to facilitate and promote these objectives from its very foundation.

Service Oriented Architecture

Service Oriented Architecture (SOA) is an architectural style and a design principle for application development and integration that uses open standards and protocols to define business functions as components that are loosely-coupled and well-defined to support interoperability, improved flexibility, and higher levels of reusability. SOA applications are created through the combination and composition of a number of packaged services—referred to as *service choreography*—allowing rapid and dynamic reconfiguration to align with changing business requirements while maintaining cost effectiveness.



To build a system with SOA, a systems integrator would need to define the components of the system; expose these elements as packaged services; connect them with a standard integration bus; and finally

compose the application by connecting the appropriate services. Because service components are well defined through explicit interfaces in an implementation independent fashion and callable through common and standard communication protocols, applications made out of these services will achieve a high level of interoperability and location transparency. Other applications—*existing* or *new*, *locally* or *externally developed*—will also be able to invoke the same set of services, which results in a high level of reusability.

■ **Business alignment, interoperability, and standards.** With SOA, a service implemented in one operating system and language platform, such as *UNIX* and *Java*, can be combined with another implemented in completely different environments, such as *Microsoft .NET* and *C#*, to create a composite application that can be accessed through the standard Web browser interface. The detailed technical environments of the service components are completely transparent to the composer and the end user of the application—which means a high level of both application extensibility and interoperability with other applications. Moreover, the composition of the application can be rapidly and dynamically modified to use an alternate service implementation if and when it makes business sense to do so. As a result, applications built with SOA will be better aligned with the present business model and can react much more rapidly to changing business models. This reason, and the fact that SOA applications utilize standards-compliant interfaces and common communication protocols, enables SOA applications to be more adaptable to and compatible with future technologies.

Clearly, with the application of SOA a situational awareness decision support system will be able to comply better with interoperability requirements, and will have the inherent ability to be extensible to meet changing business requirements.

ERIS Features and Benefits

ERIS, an acronym for *Emergency Response Information System*, is an upcoming product of *e-IDC* that will provide a tool to help responsible stakeholders in mission-critical situations to acquire a high-level of situational awareness of affected buildings, structures, and objects. It integrates interactive 3-dimensional models of buildings and structures, and real-time information on animate and inanimate objects acquired from sensor devices or input by human operators in a service oriented application. By overlaying these components and providing a graphical user interface that visualizes the objects and environment and allows their direct manipulation, *ERIS* supplies the level of detail necessary for acquiring situational awareness—before, during, and after an emergency.

REFERENCES

US Federal Emergency Management Agency:
National Incident Management System Integration Center

<http://www.fema.gov/emergency/nims/>

US Department of Homeland Security:
Fact Sheet: National Incident Management System

http://www.dhs.gov/xnews/releases/press_release_0363.shtm

IBM:
Service Oriented Architecture

<http://www.ibm.com/software/solutions/soa/>

e-IDC:
International Design and Construction Online

<http://www.e-IDC.com/>

Mobile Information Access

USING MOBILE WIRELESS TECHNOLOGY
FOR AN EFFECTIVE SITUATIONAL AWARENESS SYSTEM

Real-Time Situational Awareness

Situational awareness is a term that has become a buzzword in the recent times. It is, perhaps, especially so due to the heightened level of intensity of the struggles occurring in many places of the world that result from acts of terrorism, warfare, or natural disasters. Stakeholders involved in these conflicts and events are required to have a deep level of understanding of their relevant environmental conditions to be able to respond effectively. The term situational awareness refers to three levels of understanding: *the perception of elements; the comprehension of their meaning; and the ability to utilize that comprehension to project future states.*

It is very clear that situational awareness is a critical factor when responding to an emergency situation. The ability to fully perceive and comprehend the state of the relevant environment and to make accurate projections to alter the course of future actions almost completely determines the nature of the response outcomes. In highly charged, mission-critical situations, such as a building fire, or a hostage situation, this factor becomes even more crucial. Decisions must be made within a very short timeline, or structures may collapse and lives may be lost in the process. The ability to acquire situational awareness instantaneously, in real-time, is a requirement for avoiding and minimizing irreparable loss.

Critical Information Access

In emergency situations, instant access to current and critical information—the exact location of building control panels, the number of current building occupants, the presence of combustible chemicals, and many others—is sometimes unanticipated, but can become critical for first responders. At present, such information, when available, flows as voice communication between the offsite or near-site command and control operators or officers in charge and first responders on the ground via two-way radio frequency (RF) telecommunication devices.

The nature of this information flow in an emergency is not always the most efficient, and typically involves higher transmission latency occurrences than if the first responders have the ability to directly search and retrieve the information. One can imagine the situation if access to critical information could be available ubiquitously to these highly mobile first responders, in the form of sound, static graphical images, or video, as appropriate. While there will be a limitation in the amount and kind of contents that can be served and consumed in this fashion, the benefit of having them available while in high mobility—to complement the traditional voice communication—is tremendous. Even better, when information can flow both ways, with first responders on the ground providing direct feedback to online models that are immediately visible to other responders, better decision making processes can occur because of the deeper level of situational awareness.

In order to facilitate this better way of information sharing, we will need a wireless network infrastructure over which data can be transmitted in full duplex, high bandwidth, and with low latency, as well as portable computing devices with enough computing power, high usability, and the appropriate physical characteristics to be seamlessly embedded into emergency response operations.

Wireless Mobile Technology

There are two key technological elements that make up the solution for enabling mobile information access: *wireless mobile infrastructure* and *wireless mobile devices*.

■ **Wireless mobile infrastructure.** When establishing wireless mobile network infrastructure, there are several different criteria to consider. At present, in the United States, in addition to the options of deploying Institute of Electrical and Electronics Engineers (IEEE) 802.11-based Wi-Fi technology to establish a private wireless local area network (LAN) infrastructure, wireless communication can also be established over commercial mobile phone digital cellular networks or satellite-based Internet connections.

With Wi-Fi, one or more wireless LANs can be established to cover the area where an emergency situation takes place, allowing mobile and fixed network devices to communicate over the 2.4 GHz radio frequency with a maximum data rate of up to 108 Mbps using devices that perform *channel bonding*. The IEEE is also projecting to finalize the 802.11n wireless LAN standard in 2007 that will provide data rate as high as 540 Mbps, while operating on either the 2.4 GHz or 5 GHz radio frequencies. The availability of such high bandwidths enables mobile wireless access and sharing of rich contents, including sound, image, and streaming video.

The drawback of Wi-Fi networks is the relatively limited area of coverage, at a maximum of between 100 to 150 feet, and the possible

interference from other devices operating in the same 2.4 GHz radio frequency, which includes microwave ovens, cordless telephones, and Bluetooth devices. In situations involving high-rise buildings, for instance, Wi-Fi networks would perform poorly without the use of special antennas as the radio signals would degrade considerably across floors.

The next alternative is the use of third generation (3G) commercial mobile phone digital cellular networks, which is available in most United States metropolitan areas from national carriers. Verizon and Sprint, for instance, both offer 1x Evolution-Data Optimized (EV-DO) standard broadband access, that could provide up to 3.1 Mbps download and 1.8 Mbps upload data rates. Although offering much smaller bandwidths than Wi-Fi, wireless connectivity based on this technology covers a much larger area, is not typically affected by local interference, and is readily available without the use of specialized network access points and other routing equipments.

Satellite-based Internet access is a commercial alternative that relies on the connectivity with two-way geostationary satellites to provide up to 2 Mbps download and 500 Kbps upload data rates. The primary benefit of this option over cellular networks is that it does not rely on terrestrial cellular towers, an infrastructure that may disappear in certain emergency situations. However, in addition to the relatively low bandwidth and the high cost of this option, communication through satellite connection has very high network latency because of the large distance between the dish on the ground and the orbiting satellite. Another drawback is that connectivity will degrade quickly due to rain and other weather disturbance.

When relying on limited bandwidth wireless connectivity, such as satellite-based Internet access, it would be beneficial to have Wi-Fi equipments to provide the wireless LAN infrastructure. In this scheme, the satellite-based connectivity could be established at a fixed outdoor location in conjunction with one or more caching servers to provide proxied services to the wireless client devices on the emergency scene.

■ **Wireless mobile devices.** In addition to having a reliable and well-functioning wireless network infrastructure, it is critical to employ the right client equipments for delivering mobile application services to first responders. A wide range of devices fall into this *pervasive computing* category; including the latest generations of smart telephones and *personal digital assistants* (PDAs), ultra-mobile PCs, tablet *personal computers* (PCs), and wearable computers.

A smart telephone is a mobile wireless telephone device with the inbuilt ability to connect to a data network at a high rate. It provides networked client applications that take advantage of that connectivity, such as an Internet browser, an email client, or an *instant messaging* (IM) client. A PDA is very similar to a smart telephone except that it typically focuses on providing personal productivity applications—a task manager, a

calendar, an address book, and others—in addition to the networked client applications.

There are a number of commercial products readily available in the United States from national wireless network operators that can perform smart telephone and PDA functions. These products generally fall in one of the following categories: *Research In Motion, Ltd.* (RIM) BlackBerry devices, Windows Mobile OS devices, Palm OS devices, or Symbian OS devices. The *BlackBerry 8703e*, *Motorola Q*, *Palm Treo 700p* and *700w*, and *Samsung A900* are examples of these devices with support for the EV-DO mobile broadband access and weigh between 4.0 and 6.0 ounces. Their relatively small size makes these devices very portable and results in less power consumption than a typical laptop computer, allowing them to stand-by for as long as 300 hours without charging. However, they also present a limit in the amount of information that can be effectively displayed. User input is also limited to the use of a tiny keyboard, a stylus, or a thumb wheel. Given the limitations of this platform, instant messaging, email, or text, image, and video sharing applications are more appropriate than application services that involve numerous direct manipulations of screen objects.

An ultra-mobile PC (UMPC) is essentially a miniaturized laptop that is so small that it can fit into a shirt pocket. It combines the mobility and portability of a PDA with its small form factor, while having the power of a notebook PC with its higher performance and features. There are several models currently available in the market, including the *OQO model 01+*, *Samsung Q1*, and *SONY VAIO VGN-UX280P Micro PC*. These models feature 5” to 7” liquid crystal display (LCD), an Intel Celeron M, Intel Pentium M, or VIA C7-M processor and a small keyboard, and weigh less than 2 pounds. Network connectivity on these devices is available through the built-in Wi-Fi capability or through support of the EDGE mobile broadband access. Because the form factor of these devices resembles that of smart telephones and PDAs, they may not be appropriate for use to access application services that involve numerous direct manipulations of screen objects.

A tablet PC is not too different from a laptop or notebook PC in form factor, capabilities, and performance, except it entails the use of a touchscreen panel that allows the end user to operate the system with a stylus or a finger. Some models allow the touchscreen panel to be rotated and folded over the keyboard to make the system usable in a slate form factor. The *Panasonic Toughbook 19* is an example of such a convertible tablet PC that has been ruggedized in a full magnesium alloy case and tested to meet MIL-STD-810F specifications. Wide area network connectivity is available through the EV-DO or EDGE mobile broadband access. While it weighs 4.5 pounds, much heavier than a smart telephone or PDA, and with a shorter battery life of 4 to 6 hours, the Toughbook offers a more conventional laptop computing power of the Intel Core Duo processor and input-output (IO) capabilities through the integrated full-size keyboard and 10.4” active-matrix Extended Graphics Array (XGA) resolution display. Given these specifications,

more interactive application services involving a higher level of direct manipulations of screen objects may be served on the tablet PC platform.

The cutting edge of pervasive computing involves the use of various wearable computers. These are wireless computing devices that are worn on the body, such as a wristwatch computer, head-mounted display (HMD), and virtual retinal display (VRD). Although the use of these devices is not widespread, and there is limited commercial availability, specialized research and development in this area is currently ongoing. For example, the *Fire Information and Rescue Equipment (FIRE)* Project, run by a team of students at the University of California at Berkeley, has developed head-mounted displays for use by firefighters to relay performance and safety-enhancing information, such as floor plans with a user location indicator, other company member location indicators, areas where smoke alarms have been activated, and others. The system is custom-built with a number of sensor motes based on *Moteiv* technologies that are integrated into the 11-ounce *Xybernaut Personal Multimedia Appliance (POMA)* wearable computer.

Based on the information above, it is apparent that an effective solution for a situational awareness decision support system can be developed using commercial, off-the-shelf wireless mobile products and technologies.

Usability Considerations

It is worth stressing that the use of wireless and pervasive computing devices during an emergency can only be effective if the overall system—network infrastructure, device, and information system—has been designed to focus on the end user and to provide the right amount of information with a high level of usability.

To gain the level of understanding necessary for accurately designing such a system, a study that develops a model to represent the information absorption rates of the end users as a function of their roles and the situations in which they are involved should be conducted. In this study, multiple subjects can be asked to repeatedly carry out a mission critical and high-pressure task, such as closing the main gas valve in a building, or rescuing a trapped individual, while being presented with varying amounts of information and *disinformation* about the environment. With a sufficient number of representative subjects, a pattern should emerge that will suggest the right amount of information that can be effective to help the typical individual in that role to perform such tasks successfully. This pattern is very valuable, as too much information during a crisis situation can very often have an ill effect and result in poor performance. With this knowledge, the application of pervasive computing devices can be designed to present the optimum level of detail information to the end users.

ERIS Features and Benefits

ERIS, an acronym for *Emergency Response Information System*, is an upcoming product of *e-IDC* that will provide a tool to help responsible stakeholders in mission-critical situations to acquire a high-level of situational awareness of affected buildings, structures, and objects. It integrates interactive 3-dimensional models of buildings and structures, and real-time information on animate and inanimate objects acquired from sensor devices or input by human operators in a service oriented application. By overlaying these components and providing a graphical user interface that visualizes the objects and environment and allows their direct manipulation, ERIS supplies the level of detail necessary for acquiring situational awareness—before, during, and after an emergency.

REFERENCES

Wikipedia:

Wireless LAN

http://en.wikipedia.org/wiki/Wireless_LAN

Wikipedia:

3G

<http://en.wikipedia.org/wiki/3g>

Wikipedia:

Satellite Internet Access

http://en.wikipedia.org/wiki/Satellite_Internet_access

Panasonic:

Toughbook 19 Specifications

ftp://ftp.panasonic.com/pub/Panasonic/toughbook/specsheets/TB-19_ss.pdf

SONY:

UX Micro PC Overview

<http://www.learningcenter.sony.us/Notebooks/UXMicroPC>

University of California at Berkeley:

Fire Project FireEye

<http://fire.me.berkeley.edu/fireeye.html>

moteiv:

Intelligent Wireless System for First Responders

<http://www.moteiv.com/pr/2006-09-27-fire.php>

e-IDC:

International Design and Construction Online

<http://www.e-IDC.com/>