Connecting Buildings to Public Safety Networks

Alan Vinh
David Holmberg
Building Environment Division
Building and Fire Research Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899, U.S.A.

ABSTRACT

The operation of modern commercial buildings uses digital control systems which monitor a vast amount of sensors. These sensors in turn produce data that is available for building control but also can be mission-critical for effective emergency response. First responders can be notified of designated building alerts in real-time so that actions can be performed promptly. The capability to monitor building devices and to keep the first responder community updated with the latest building information during emergency situations, as well as the ability to remotely control certain building devices and processes, can be realized.

This paper presents a framework for standards-based communication of real-time building alerts, via public safety networks, to 9-1-1 dispatch and into the hands of emergency responders. This research will assist in the development and deployment of commercial products with new levels of capability for situational awareness to help save lives and properties in emergency situations.

Keywords: alarm; alert; authentication; authorization; building information and control systems; emergency preparedness; emergency response; public safety networks; secure data exchange

INTRODUCTION

The operation of modern buildings uses control systems that connect to a vast array of devices and sensors. These sensors can be used to monitor pertinent information for daily operation as well as emergency scenarios [1]. For the purposes of emergency response, there needs to be a standards-based framework for public safety officials to connect to all buildings in a geographical area and monitor building automation system (BAS) generated alerts. However, there is no standard method to enable this information transfer. This lack of a cohesive set of standards hinders the delivery of mission-critical data into the hands of public safety officials, and hinders the development of tools and methods that could use this data to improve the performance and safety of first responders in addressing emergency building incidents.

The National Institute of Standards and Technology (NIST) is working with industry to define standard mechanisms for communicating building information such as sensor data, alert data and floorplans to first responders' operations centers and mobile units via the public safety networks to improve situational awareness. In order to achieve these objectives, this paper describes the following necessary elements (1) a framework for monitoring and sending building alerts to the first responder community (2) a standard for encapsulating the alerts and their contents (3) a standard way to classify and to categorize the alerts so that filtering can be done on alert contents (4) a standard mechanism for communicating the alerts between the various public safety networks (5) a standard way to connect back to the building to assess the emergency scenarios (6) a standard format to represent a building floorplan and (7) a standard mechanism to represent the location of a sensor within the standard floorplan. Some of the elements described in this paper have already been implemented as a test system while others are being addressed in cooperation with industry stakeholders.

END-TO-END TRAVERSAL OF ALERTS

The scope and challenge of moving building alert information from the building into the hands of first responders is presented in Figure 1. Collecting building alert data at the building alert server is the first requirement [2, 3]. These alerts must end up at the Public Safety Answering Point (PSAP), a.k.a. 9-1-1 dispatch. Dispatchers can then use the alert information to help dispatch first responders. Figure 1 represents the proposed end-to-end traversal of these alerts. The following steps summarize the proposed events that will occur for typical emergency scenarios as depicted in Figure 1:

1) Alert information generated by sensors is encapsulated using the Common Alerting Protocol (CAP) and sent to the Building Information Services and Control System (BISACS) Base Servers (BBS). The BISACS network of servers will propagate these alerts up the hierarchy to the appropriate BISACS Proxy Servers (BPS).
2) Designated BPS will send their alerts to the Central Station Alarm Network (CSAN) or directly to the Next Generation 9-1-1 (NG9-1-1) network (ESInet) if the CSAN is not available. If the CSAN and the ESInet are not available, then alerts will be sent directly to the Public Safety Answering Point (PSAP). Communications between the various public safety networks are done via the Standard Access Point (SAP).
3) The CSAN system will forward alerts to the ESInet if it is available, otherwise alerts will be sent directly to the PSAP.
4) If the NG9-1-1 system is available (i.e., the ESInet is available), then the NG9-1-1 system will route the alerts to the appropriate PSAP to handle those emergency events.
5) The appropriate PSAP will receive and put the alerts into their Computer Aided Dispatch System (CAD).
6) PSAP communicators will dispatch the appropriate personnel to the sites to handle the emergencies. As part of this process, standard building interface software will be used to connect back to the buildings for better analysis of the situations and the scenarios.

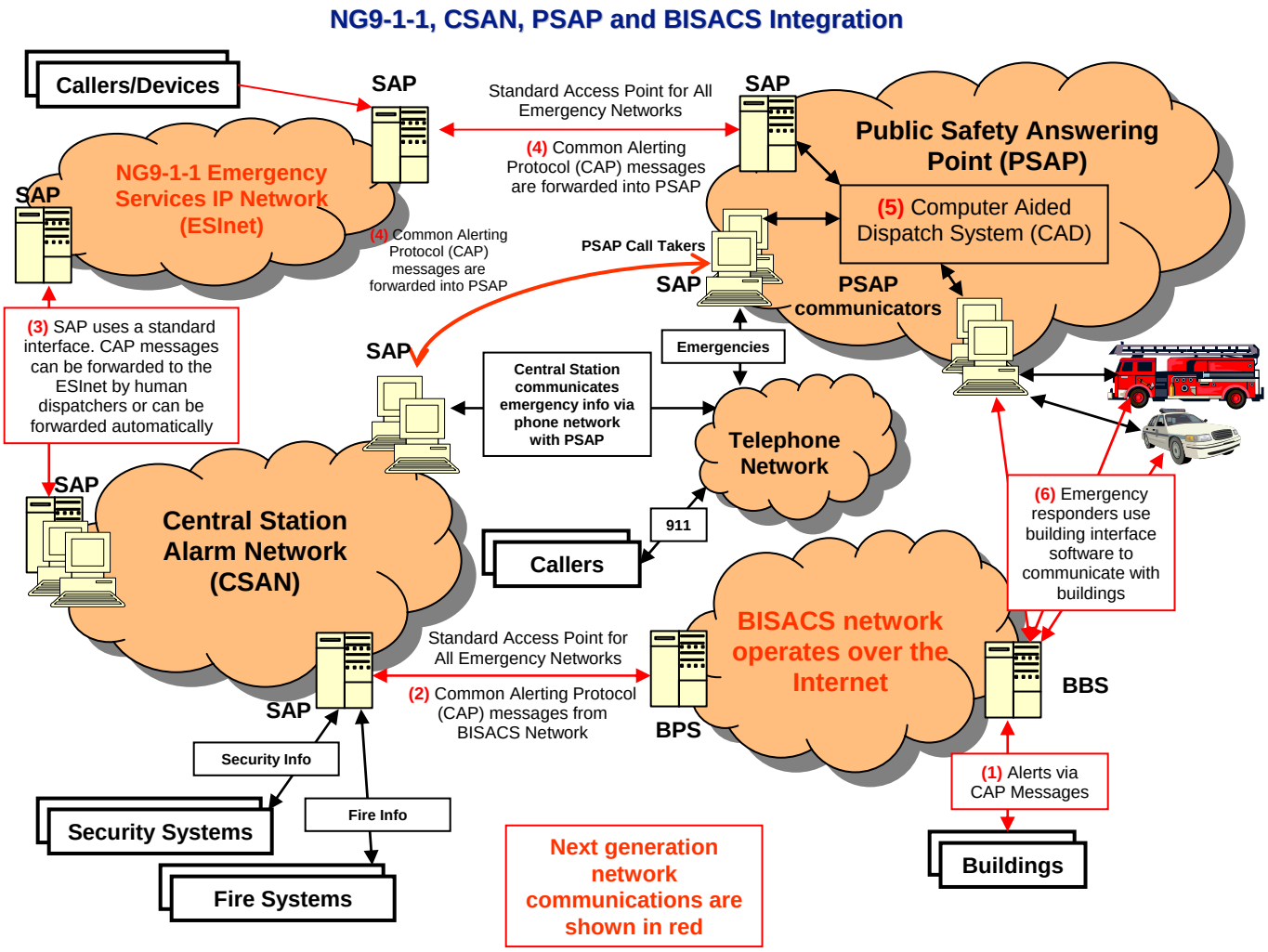

Figure 1 Proposed Next Generation Network Communications for First Responders

1. MONITORING AND SENDING ALERTS

The Building Information Services and Control System (BISACS) was developed and continues to be enhanced by NIST's Building and Fire Research Laboratory (BFRL) as a prototype standards system for exchanging building information with first responders [2,3]. The BISACS consists of a network of servers that monitor entities such as sensor devices and building processes. Software processes or devices such as building sensors send alerts to the BISACS servers, and the BISACS servers propagate the information to various nodes within the BISACS network. Alerts are promoted to "alarm" status based on building owner specified criteria, e.g., when a temperature sensor has its value go past a certain threshold, its value is propagated as an alarm. Typically, only alarms are propagated up the BISACS network hierarchy.

The two main components of the BISACS network are the BISACS Base Server (BBS) and the BISACS Proxy Server (BPS). The BBS monitors and controls one or more networks and their devices such as within a building; while the BPS, external to the building, monitors other BBS or BPS to collect all alarms from the lower nodes in the network. Together they collect and propagate alerts up the BISACS network hierarchy. Figure 2 depicts a sample BISACS network hierarchy.

At the upper level in the network hierarchy, the BPS would be monitoring an appropriate set of servers underneath of it so as to monitor a geographical area such as a jurisdiction. Alerts arriving at the BPS have been promoted to alarm status (via building threshold criteria); filtering mechanisms can be used at each BPS node to control the propagation of specific alarms. Designated BPS(s) would send their alarms to the Central Station Alarm companies (CSA). The CSA can connect back in to the BBS to verify the emergency situation at the building; once the emergency is verified, the CSA can then notify the Next Generation 9-1-1 system (NG9-1-1) by directly forwarding the alarms from the building or by generating new appropriate alarms for the pending emergency. The NG9-1-1 system is responsible for routing any alert/alarm to the correct Public Safety Answering Point (PSAP) that is responsible for that building's location. If the NG9-1-1 system is not available then the CSA can forward those alarms to the responsible PSAP directly.

Once the alarms (via CAP messages) arrive at the PSAP, the dispatcher at the PSAP will dispatch the appropriate personnel and equipment for the incident. Personnel from the PSAP or those first responders that are enroute or at the scene can also log in to the BBS to get more building information to help resolve the emergency.

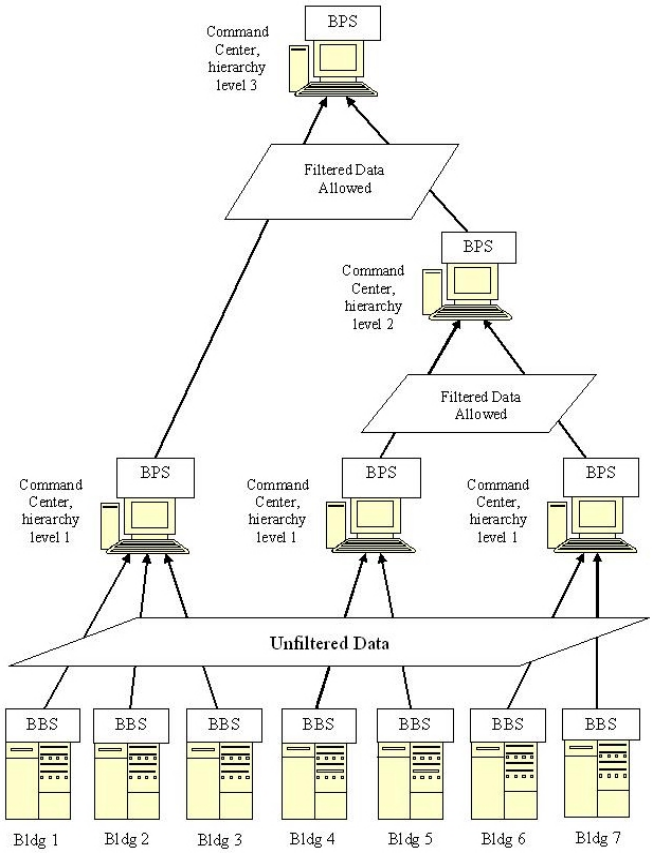

Figure 2 The BISACS Network of Servers

2. DATA ENCAPSULATION FOR AN ALERT

In the context of this research, alerts are indicators of some change of sensor status. The indicators can be normal status information such as a change of value notification within the HVAC system, or alarm notifications typically associated with a fire or security system. The difference between an alert and an alarm is based on building owner specified criteria. Generally only alarms would be passed from the building BBS to the BPS. The BPS should typically contain only alarms, and it should forward those alarms to the CSA or a PSAP so that first responders can be notified.

The BBS monitors its controllers and devices via a software component called the Services Interface (SI). The SI converts the alert information into computer processable contents by using the Extensible Markup Language (XML) [4]. For the BISACS, the Common Alerting Protocol Standard (CAP) [5] is used to encapsulate alert information. The Organization for the Advancement of Structured Information Standards (OASIS) developed the Common Alerting Protocol as a standard in 2005; the CAP is "a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks". Figure 3 shows a sample CAP message represented using XML that is sent between the SI and the BBS. CAP messages are also used for alerts communicated between the BBS and the BPS.

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.1">
  <identifier>1179353147004</identifier>
  <sender>https://p623572.campus.nist.gov:8443/bisacs
  </sender>
  <sent>2008-11-12T18:05:47-04:00</sent>
  <status>Exercise</status>
  <msgType>Alert</msgType>
  <source>alarm1bundle.sensor01</source>
  <scope>Public</scope>
  <info>
    <category>Env</category>
    <category>Fire</category>
    <category>Health</category>
    <category>Rescue</category>
    <category>Safety</category>
    <category>Security</category>
    <event>Smoke</event>
    <urgency>Immediate</urgency>
    <severity>Extreme</severity>
    <certainty>Observed</certainty>
    <expires>2008-11-12T18:06:47-04:00</expires>
    <description>Smoke detector, bldg 226, 3rd flr, rm B346.
    </description>
  </info>
</alert>
```

Figure 3 Sample Common Alerting Protocol Message

3. CLASSIFYING AND CATEGORIZING ALERTS

In order to send specific alerts that have been promoted to alarm status to the first responder community, a mechanism for filtering on the alert information must be made available for this purpose. Furthermore, NIST reviews have shown that the amount of alert information that can be collected by the BBS can be overwhelming. The need to filter on these alerts must be developed so that the user can focus on the alerts of interest. For example, when logged into a building during an emergency to view building information, a fire fighter may not be interested in certain Heating Ventilation and Air Conditioning (HVAC) information but is interested in the information from the temperature sensors and the smoke detectors that are in alarm mode; having a mechanism for the fire fighter to filter on specific sets of alerts/alarms allows the building information to be more manageable and comprehensible. The proposed mechanism used for filtering alarm/alert information is described below.

The proposal is to use the "category" and the "event" elements of the Common Alerting Protocol message for filtering purposes. While the "category" element is well defined by the CAP message, the "event" element of the CAP message is unstructured text. By changing the "event" element to contain a limited set of key words, this would allow the "event" element to be computer processable hence the alert can then be filtered by its "category" and its "event" elements. A list of all available sensor types along with their corresponding categories and event types has been proposed to industry for evaluation. The details of this list are beyond the scope of this paper.

4. THE STANDARD ACCESS POINT

Getting building alerts out to the proposed BISACS servers is the first step. These alerts must successfully arrive at a Public Safety Answering Point, a.k.a. 9-1-1 dispatch, which will handle first responder dispatch based on received alerts. Figure 1 presented the proposed end-to-end traversal of these alerts.

In order for alerts to be sent to the various public safety networks, such as the CSAN, the ESInet and the PSAP (Figure 1), there is a need to have a standard network communications interface. Having a standard alert interface for all public safety networks allows any of these entities to communicate with any of their peers that are available as part of the communication loop. Due to many configurations that are adapted by various jurisdictions, the proposed standard interface must support communications no matter which configuration will be in used.

The standard network interface is proposed to be called the Standard Access Point (SAP) as shown in Figure 1. The SAP will act as the gateway to each public safety network and it will require a standardized interface. The SAP is proposed to be represented as a Web Services Interface that is properly described using the Web Services Description Language (WSDL) [6]. Communication with the SAP will be done using HTTP over TLS [7, 8]. The specification, design and implementation of the SAP are still being worked by NIST and industry stakeholders hence the details are beyond the scope of this paper.

5. CONNECTING BACK TO THE BUILDING

Once the CAP building alerts have been routed through the various networks and end up at the PSAP, these alerts are passed on to dispatched responders through the dispatch system. The responders need a connection to the building BBS so that they can request building data to understand the incident. There needs to be some information within a CAP alert that provides the needed information for a responder to connect back to the building. The "sender" element of the CAP message contains a Uniform Resource Locator (URL) that points back to the BISACS Base Server (BBS) that originated the CAP message (see Figure 3). An Application Specific Client (ASC) with very specific security related processing is proposed to be used for connecting back to the BBS for scenario analysis.

Having a standard user interface is important so that all emergency responders will be familiar with the layout and the various function buttons. NIST's Building and Fire Research Laboratory is working with industry to define such a user interface [9]. The proposed layout for this user interface may look as depicted in Figure 4. The proposed security requirement for the ASC includes using the Hypertext Transfer Protocol with Transport Layer Security [7, 8] over the Transmission Control Protocol [10] for reliable and encrypted communication. X.509 certificates [11] will be used to identify the computer/terminal being used, Personal Identity Verification cards [12, 13] will be used to authenticate the users, and user identifier and password combinations will be used for the authorization process to give out appropriate credentials [14].

The ASC should allow the emergency responder to query the building server for its current set of alerts along with building information such as floorplans, number of stories and preplan information. In Figure 4, the address field indicates the location of the BBS while the sensor's location is actually located in building 226; this is because this particular BBS is monitoring more than one building. The complete requirements and specifications for the ASC are beyond the scope of this paper.

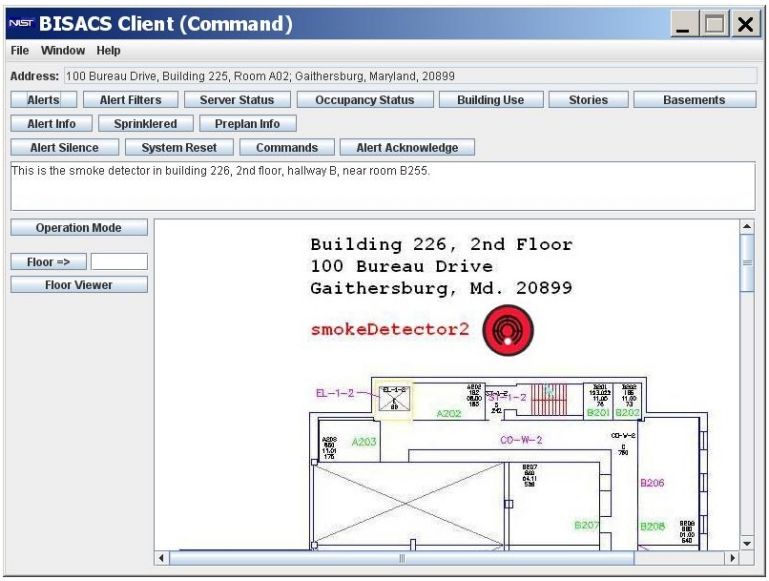

Figure 4 The Application Specific Client User Interface

6. THE BUILDING FLOORPLAN

The ASC in Figure 4 shows the floorplan as a JPEG image [15], however since buildings come in many shapes and sizes, BFRL is working with industry to standardize the mechanisms for communicating building floorplan and sensor location information. Having a standard way to represent building floorplans is important because it can then be used with any of the software vendors. The vendors can use their proprietary graphics engine to convert the standard floorplan into specific images for display purposes.

Having a standard user interface and a standard representation for building floorplans will shift the software vendors' attentions to focus more on value added functions and capabilities. The standard for representing building floorplans is still being researched by industry stakeholders hence the details are beyond the scope of this document.

7. LOCATING A DEVICE WITHIN THE FLOORPLAN

Building alerts typically come from sensors; it follows that the location of these devices must be represented on a floorplan or in a building information model. Having a standard representation for a sensor's location is important because software vendors can map the location information onto the standard floorplan discussed in section 6. Once this mapping is accomplished, the ASC can draw attention to sensors that are in "alarm" mode such as making them blink on the floorplan. The ASC can connect back to a building server and can display its list of alerts; the user can request more information on a specific alert such as its location on a floorplan, its current status and its current value if applicable.

BFRL is working with industry to develop a standard for representing the location for sensors so that this information can be carried with the CAP messages until they reach the PSAP. The

standard for representing a sensor's location is still being researched by industry and is beyond the scope of this paper.

8. CONCLUSIONS

The National Institute of Standards and Technology is working with industry to define alternative ways to communicate building alerts to first responders' operations centers and mobile units via the public safety networks. This paper presented the key elements required for sending building alerts through the various public safety networks in order to reach the first responders as well as the mechanisms required to connect back to the building for emergency assessments. The framework for monitoring and sending building alerts to the first responder community was proposed via the Building Information Services and Control System (BISACS); the Common Alerting Protocol was proposed as the standard for encapsulating the alerts and their contents; a standard way to classify and to categorize the alerts so that filtering can be done on alert contents was proposed; the Standard Access Point was proposed as the standard mechanism for communicating the alerts between the various public safety networks; the Application Specific Client was proposed as the standard way to connect back to the building to assess the emergency scenarios; a standard format to represent a building floorplan was discussed and a standard mechanism to represent the location of a sensor within the standard floorplan was discussed.

By working with industry to standardize these key elements, the ability to send alerts from buildings through the various public safety networks to reach the Emergency Communications Centers so that the appropriate personnel can be dispatched to the emergencies can be achieved; in turn, situational awareness for the first responders will be improved so that lives and properties can be better saved.

9. DISCLAIMER AND COPYRIGHT NOTICE

Certain trade names, documents or organizations are mentioned in this paper to specify adequately the resources used for this research/work. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the resources used are the best available for the purpose.

10. REFERENCES

[1] Holmberg, David G., Davis, William D., Treado, Stephen J., Reed, Kent A., **Building Tactical Information System for Public Safety Officials, Intelligent Building Response (iBR), NIST Internal Report 7314**, January, 2006.

[2] Vinh, Alan B., **Computer-Based Monitoring for Decision Support Systems and Disaster Preparedness in Buildings**, International Muti-Conference on Engineering and Technological Innovation: IMETI 2008, Orlando, FL, United States, 06/29/2008 to 07/02/2008, Vol. II, pp. 285-290, July, 2008

[3] Vinh, Alan B., **Building Information Services and Control System (BISACS): Technical Documentation, Revision 1.0, NIST Internal Report 7466**, November, 2007.

[4] **Extensible Markup Language (XML) 1.0 (Fourth Edition)**, available at http://www.w3.org/TR/xml/, September, 2006.

[5] **Common Alerting Protocol, v. 1.1, OASIS Standard CAP-V1.1**, available at http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf, October, 2005.

[6] **Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language**, available at http://www.w3.org/TR/wsdl20/, June, 2007.

[7] **HTTP Over TLS**, available at http://tools.ietf.org/html/rfc2818, May, 2000.

[8] **The Transport Layer Security (TLS) Protocol Version 1.1**, available at http://tools.ietf.org/html/rfc4346, April, 2006.

[9] **NFPA 72, National Fire Alarm Code**, available at http://www.nfpa.org/freecodes/free_access_agreement.asp?id=7207, August, 2006.

[10] **Transmission Control Protocol, DARPA Internet Program, Protocol Specification**, available at ftp://ftp.rfc-editor.org/in-notes/rfc793.txt, September, 1981.

[11] **Web Services Security, X.509 Certificate Token Profile, OASIS Standard 200401**, available at http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf, March, 2004.

[12] Dray, J., Guthery, S., Schwarzhoff, T., **NIST Special Publication 800-73-1 Interfaces for Personal Identity Verification**, National Institute of Standards and Technology, Gaithersburg, MD 20899, March, 2006.

[13] **FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors**, National Institute of Standards and Technology, Gaithersburg, MD 20899, March, 2006.

[14] Ritter, D., Mundt, H., Isler, B., Treado, S., **Access Control in BACnet, ASHRAE Journal Article**, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta, GA, 2006.

[15] **ISO/IEC 10918-1: Information technology – Digital compression and coding of continuous-stone still images: Requirements and guidelines**, available at http://www.w3.org/Graphics/JPEG/itu-t81.pdf, September, 1992.