



LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

A Systems Approach to HVAC Contractor Security

K. M. Masica

April 24, 2014

A Systems Approach to HVAC Contractor Security

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

A Systems Approach to HVAC Contractor Security

< Ken Masica, Lawrence Livermore National Laboratory, April 2014 >

In the wake of the Target Corporation breach that occurred last November, there has been increased awareness of the need to provide enhanced cyber security of Building Automation Systems (BAS). Trade press reports indicated that a remote access account granted to an HVAC contractor may have been compromised by the attackers to gain access to the Target corporate network and eventually inject malware in the Point-of-Sale (POS) systems that collect and process credit card purchase data. Although details of the attack have not been made public, the incident clearly highlights the need for BAS owners to provide cyber security oversight and monitoring of contractors and vendors that perform work on their installed systems. Hopefully BAS owners are reviewing and strengthening their remote access policies and security measures if they grant remote access to contractors (or perhaps even reviewing the need for remote access). Equally important, however, is the need to provide security oversight and implement security controls when contractors are performing work on-site. This is especially important for large campus installations that may have an extensive BACnet communication system that interconnects the various BAS components over a TCP/IP network.

This article will address cyber security considerations for HVAC contractor oversight when they are on-site accessing the building automation system to perform work such as equipment and controller installation, programming, software/firmware updates, commissioning, troubleshooting, and maintenance activities. The article will begin by discussing the need for a security plan, followed by an overview of the different components of a modern, network-based building automation system that may be accessed by HVAC contractors during on-site work. Subsequent sections will describe a systems approach to HVAC contractor security in which security guidelines are provided for each of the different components that comprise a BAS system. A concluding section will summarize the cyber risks associated with contractor access and the need to apply security measures to the BAS system to mitigate those risks.

Start with a Security Plan

Your organization should have a security plan for the BAS that specifies the policies and procedures for how it is protected, accessed, and monitored. This includes both cyber and physical protections. An example policy statement would be whether remote access by contractors is permitted. If permitted, a set of procedures should be specified to ensure authorized individuals are vetted, authenticated, and limited to the minimum necessary access and privileges needed to perform their work. At Lawrence Livermore National Laboratory (LLNL), there is a dedicated security plan for the BAS system that prohibits remote access by contractors. However, because HVAC contractors must perform work on-site, there are policies and procedures specified for contractor access and oversight. The plan identifies potential cyber threats and security controls implemented to mitigate those threats.

In general, security plans will vary in content and scope based on the type of organization writing the plan, existing institutional security policies and requirements, and the size and complexity of the BAS

implementation. For customers without a BAS security plan, a starting point might be to add them to an existing organizational cyber security plan in consultation with the Security or IT departments. For those wanting to pursue a dedicated plan, security plan templates are available at sites such as <http://www.sans.org/security-resources/policies> although they will need to be tailored to address the unique requirements of a building automation system.

Whether you have an existing BAS security plan or need to develop one, contractor oversight during on-site work performance is a critical element to include. The following sections will describe a systems approach to identifying the primary components of a BAS so that security measures for contractors can be implemented in a comprehensive manner.

Take a Systems View

Getting a handle on HVAC contractor security begins with an understanding of the interconnected components of a modern BAS system which are increasingly based on open network protocols for interconnectivity and open industry standards for interoperability. By taking a systems approach to security, each primary component of the BAS can be identified and security controls applied. A systems approach ensures the entire BAS system is covered and also addresses the manner in which the components are networked together.

There are numerous BAS vendors and system architectures available in the market place, so attempting to describe them all here would be impractical. However, for the purposes of this article, I will provide an example BAS system architecture that would be representative of a contemporary multi-building, network-based campus automation system. Customer implementations may not have all of these components or they may be interconnected differently, but the objective here is to identify the primary pieces of your BAS system for inclusion in a security plan. In addition to variations in the BAS architecture, there will also be variations in the components themselves. For example, some controllers that interface directly to the LAN network may have embedded web server capability while others will not depending on the vendor selected and the product options specified during the design phase.

Listed below are the primary components of a BAS system for inclusion in a security plan. An example BAS system architecture that includes these components is shown in Figure-1. In subsequent sections, the purpose of each of these components will be discussed as well as security considerations for contractor access.

- 1) *Automation Software*
- 2) *Automation Server*
- 3) *Engineering Tools*
- 4) *System Database*
- 5) *Operator Workstations*
- 6) *Mechanical Equipment & Sensors*
- 7) *Control Modules*
- 8) *Building Fieldbus Networks*
- 9) *LAN Network*

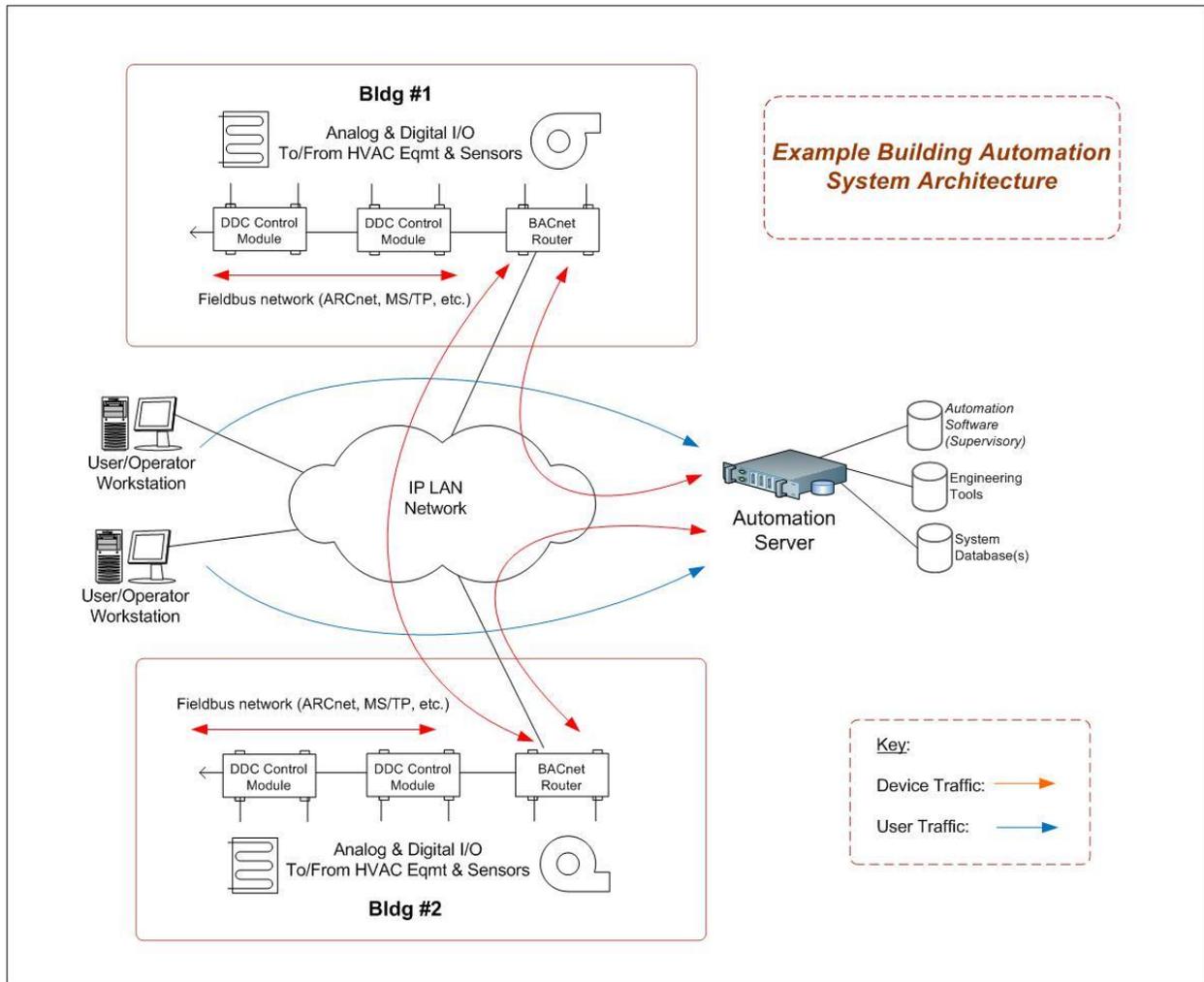


Figure-1: An example Building Automation System architecture

The BAS system described above provides Direct Digital Control (DDC) of HVAC equipment through the control modules that interface to the mechanical equipment and sensors (closed loop control). There is also a supervisory function provided by the automation software that allows the BAS owner to monitor the DDC process and graphically view the operation of the HVAC equipment from a local workstation. The BAS owner can view, trend, schedule, and (optionally) command system points as part of this supervisory capability.

Automation Software

This software component of the BAS provides the main graphical user interface for users to monitor HVAC system operation, view point values and historical trends, receive and process alarms, change operating parameters such as set points and schedules, and perform supervisory control of equipment when necessary. Users are typically given individual login accounts to access the automation software,

and each account is associated with a set of privileges that define what actions the user can perform within the software.

Security considerations for contractors accessing the automation software revolve primarily around the user accounts defined in the software and the system privileges associated with them. The first consideration is to determine whether the contractor will work directly with the software and therefore require a user account or if the customer support staff will be using the software to make the planned changes required by the contractor to complete the planned scope of work. If the BAS Security Plan policy allows contractors to directly access and use the automation software, then procedures defining the creation, privileges, termination, and auditing of the account should be specified.

A best practice here would be to create a temporary account for the contractor for the duration of the planned work while they are on site performing the work, run a system audit report showing all the changes made, and then deleting the account after completion of the work. During the planning stage of the work, a discussion regarding when the account is needed, the duration the account is needed, and the specific system privileges needed to perform the work should have been determined to make this a fast and easy process and be consistent with the security principle of least privilege.

Automation Server

The server is where the automation software runs and is typically a commercial operating system such as Windows or Linux. Identifying the server as a BAS component is important because a contractor may need to directly access the file system depending on the type of work being performed.

The primary concern with the server is file system access and file transfer if required by the scope of work. For example, a new control program or firmware version may need to be transferred to the server and then downloaded to a controller through the automation software. The automation software itself may also need to be updated with a patch or new release. Best practice here would be for the customer to perform these tasks, ideally by a server administrator from the IT department or an engineer comfortable work at the operating system level of the server. Virus checking all files prior to transfer is important as well as executing any change control processes defined by the customer such as engineering review, approval, testing, and documentation of the changes made.

Engineering Tools

In addition to the main automation software, there are supporting software applications that are used to create the control programs, graphical process views, and overall BAS system configuration. For example, you may have either a graphical or textual engineering tool for creating the control programs that are downloaded to the control modules. If you have these engineering tools in your BAS environment, it is important to include them in the security plan if a contractor will use them when performing their work.

The need for the contractor to access and use these software applications for engineering or configuring the system should be discussed in advance during the work planning stage given their potential to

impact the BAS system through modifications to the configuration database. The first consideration is whether the contractor will access and use the tools directly or if the customer will use them to make the changes required. If the security policy permits direct access, the temporary contractor account approach described earlier can be used if the tools require an operator account or another form of authentication. Logs from the tools used should be saved and archived as part of the record of tasks performed and changes made during the work execution.

System Database

The number and type of databases used by the BAS system will vary by vendor implementation, but typically there is at least one main database that the automation software uses to store system configuration information. The same database or potentially separate database instances are also used for storing additional information such as trend, alarm, and auditing data. Some BAS implementations may have a separate server dedicated to running the database software for performance and scalability reasons.

As noted, the system database is a vital component of a BAS system and contains all the system configuration information as well as control programs, graphics, alarms, trends, and audit data. Normally the database is not accessed directly but through the automation software or engineering tools and so policies and procedures defined for contractor access to the automation software and engineering tools will protect the BAS database.

An additional security consideration regarding the database is release to a contractor in advance of on-site work to be performed. If a contractor will be performing programming work that involves changes beyond simple parameter changes, they may request the database to perform the programming in advance of the site visit and then transfer or import the programming changes during the on-site work phase. If the BAS database is requested, customers may want to address concerns regarding non-disclosure, distribution to subcontractors, retention period, copying, and other limitations if there are any sensitivity issues regarding what is being released. For example, detailed floor plan graphics, building numbers, or network addresses may be a concern for government agencies. The best way to address this issue is to have a policy in the BAS Security Plan that specifies whether the database can be released to the contractor and what restrictions apply in the form of a binding non-disclosure agreement.

Operator Workstations

Those who need to access the BAS automation software will typically login into the application from a workstation such as a standard desktop computer or perhaps a laptop in the case of an HVAC technician working on equipment in a mechanical room. Procedures for how contractors will access the automation software from user workstations or laptops is an important element to include in the BAS Security Plan.

The security plan should address whether contractors will be given direct access to an operator workstation in order to access the automation system during the on-site work phase. If permitted, considerations regarding the user account, method of authentication, and duration of the workstation or directory account should be specified as procedures. Some government agencies may require computer security escorts procedures in which a designated employee provides direct oversight of the contractor while they are using the workstation to access the BAS system.

Mechanical Equipment & Sensors

HVAC equipment such as boilers, chillers, fans, and pumps comprise the mechanical equipment component of a BAS system and various types of sensors measure variables such as temperature and air flow used in the closed loop DDC control process. How contractors physically access the equipment as well as how laptops may be connected to configuration interfaces should be a consideration in the BAS Security Plan.

The primary security consideration regarding equipment is whether contractors are permitted escorted or unescorted access to mechanical rooms and other HVAC spaces. Government agencies with sensitive data processing areas where contractors require equipment access need to provide security escorts but corporations may also want to determine and specify the level of autonomy provided to contractors. At a minimum, locked mechanical rooms and/or BAS panels will need to be opened by customers at the start of work and locked when work is completed. Modern BAS systems may also have an IT drop in the mechanical room where an IP/Ethernet gateway device interfaces the field bus control network to the LAN, so security procedures should be specified when contractors have access to the BAS panel containing the gateway device.

Control Modules

There are a wide variety of control modules on the market that interconnect to the mechanical equipment and sensors in order to provide HVAC system DDC closed loop control and data acquisition functions. Control programs are typically developed using an engineering tool and then downloaded into the modules where the control logic is executed.

The BAS Security Plan should address direct access to controller hardware by the contractor when required by the scope of work. Changes to installed controllers will normally be done through the automation software for minor parameter changes or through engineering tools for logic changes, in which case the primary security considerations are controller-related privileges associated with the user account under which the work is performed. However, during new controller installations or during changes requiring physical access to the controller, a laptop is normally used to plug into one or more communication ports. Depending on the controller and the change being made, the laptop will typically connect to either a serial port or an Ethernet port. The BAS Security Plan should specify whether the contractor is permitted to use their own laptop or if the site must provide the laptop. Best practice would be for the customer to provide the laptop with the necessary software installed (e.g. terminal emulation program, engineering tools, etc.). This will allow the customer to ensure that the laptop

meets the cyber security requirements of their organization (e.g. anti-virus scanning, password policies, etc.)

Fieldbus Networks

Within a building, control modules are often networked together to allow distributed control of equipment and permit sensor values and control information to be exchanged between the modules. The generic term for the interconnected network of control modules is a fieldbus because the modules are wired directly to HVAC equipment and sensors and typically share information over a token-passing bus. Examples of BAS fieldbus standards supported by the BACnet standard are ARCnet and MS/TP. In a modern BAS system architecture, one device module in the fieldbus network has BACnet router capability and serves as a gateway between the field bus and the LAN network where the automation server, operator workstations, and other fieldbus gateways reside. Important security considerations for the fieldbus network are physical access by contractors during initial installation and commissioning as well as during expansion of a BAS system. Fieldbus networks may also be based on Ethernet connectivity in which case direct access by contractors from a laptop within the building becomes a security concern.

LAN Network

The IP-based LAN network is the component of the BAS architecture that interconnects the automation server, user workstations, and fieldbus networks located in the different buildings. Ideally, the BAS LAN is a dedicated network that does not interconnect with the general-purpose corporate LAN network (i.e. separate physical Ethernet cabling to each building or logical separation of the BAS traffic using VLAN technology.) Because of its central role in connecting the major pieces of the BAS architecture, LAN access policies and procedures for contractors should be included in the BAS Security Plan. A primary concern for on-site BAS system work by contractors is the need for laptop access to the LAN. Best practice would be for the organization to have a laptop dedicated for BAS system support with the automation software and engineering tools needed to install, commission, troubleshoot, and expand the BAS system when needed.

Conclusion

The Target Corporation breach has demonstrated an urgent need to implement HVAC contractor security, not only for remote access but also during work performed on-site. A BAS system that is well designed and managed is not only functional and reliable but also secure against unauthorized access, modification, and operation. This article has described a systems approach to providing HVAC contractor security by first identifying the interconnected components of a modern, network-based BAS system and then suggesting guidelines and cyber security considerations to ensure authorized access and modification by contractors during work execution. Customers will need to tailor the security measures they adopt based on the size and complexity of their BAS implementation and existing institutional security requirements. The security measures adopted should be included in a BAS Security Plan.

About the Author

Ken Masica is a Project Engineer in the Systems Engineering Group at Lawrence Livermore National Laboratory in Livermore, CA. He has developed and implemented secure communication solutions and system architectures for a variety of scientific, industrial, and infrastructure applications as well as performed cyber vulnerability assessments of large-scale control systems and U.S. critical infrastructure throughout the country. He currently oversees the building automation network, software, and system security at LLNL.



Prepared by LLNL under Contract DE-AC52-07NA27344