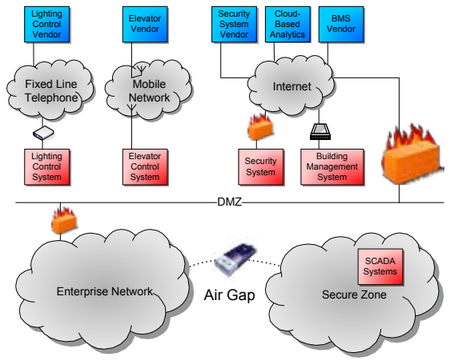
Is Your Building System Secure?

Anton Hofland, MSc
CEO
2024Sight

Today's buildings have become increasingly smart and inter-connected. Every second, Supervisory Control And Data Acquisition (SCADA) building systems controlling the world's connected buildings exchange gigabytes of data with each other and the outside world. Interconnected building SCADA systems bring many enhancements, including optimized resource utilization, improved facility management and increased service levels to building occupants.

But there is a risk with inter-connected building SCADA systems, specifically the exposure of SCADA system vulnerabilities to the outside world, risking outside interference (and consequential damage) to the system and the building. Figure 1 shows an example of building SCADA systems and how SCADA systems may have been installed.



Traditional Connectivity

Just how exposed are SCADA systems? The danger was highlighted in 2012 when research groups identified vulnerabilities in several of the most commonly used systems in the SCADA industry. But even before this research was published, inherent vulnerabilities had caused serious damage. Three examples are:

– An incident destroyed the pumps of a local water company in the USA after hackers logged into a connected SCADA system. It seems the SCADA system was only protected with a limited length password.

– The infamous Stuxnet worm deliberately bridged an air gap in the Natanz installation in Iran in both directions, not once but several times. Later versions of the worm attacked the PLC systems of the enrichment installation, causing serious damage. Stuxnet accidently broke out of the confinement of the Natanz network and spread into the Internet—which is how it was detected.

– In October 2012, an incident occurred in a US power utility where a turbine control system was infected by a variant of the Mariposa malware. The malware had been introduced to the SCADA system using a USB device, which had been used to upload software updates during a scheduled outage. The infection delayed plant restart by approximately three weeks.

There are two main reasons why SCADA systems are becoming increasingly vulnerable:

The first is commoditization of hardware and operating systems. In the past, many systems were running on specialized or proprietary hardware, and used unique operating systems. While 'Security through Obscurity' is not actual security, specialized systems of the past would have presented a higher barrier. Unfortunately, today's technology has well-understood weaknesses that present little or no barrier.

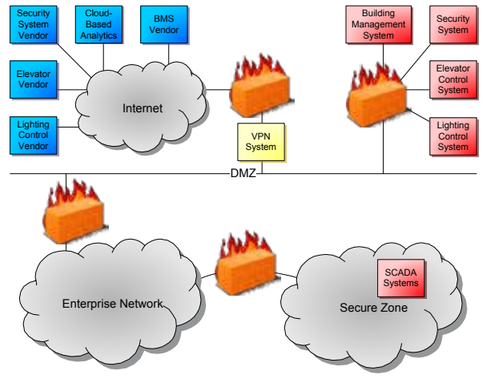
The second reason is the lack of understanding about the complexity and role of these systems. End-users, implementers and manufacturers of SCADA systems must realize that these systems are no longer just electrical systems. They are fully-fledged, connected IT systems with all the advantages, disadvantages, strengths and weaknesses therein. Nevertheless, during construction of a project they are often installed in the same way as their predecessors, i.e. as electrical systems without protection.

How can these systems be protected?

Securing Building Systems by Upgrading

The first thought that comes to mind is to ensure that a SCADA system has malware scanners and is patched to the latest OS and application release levels. While updating, patching, and scanning for malware is sound advice, it seems that those who operate SCADA systems have been slow to implement. There has been a longstanding criticism that systems are not upgraded as quickly as possible and that they are left running un-patched for days, months or sometimes even years.

The main reason for this is simple enough. Upgrading systems brings as much risk of outages as keeping with the status quo. Safe upgrades are only possible when the upgrade has been tested. Testing requires a testing approach, a test environment and effort.



Modern Connectivity

Ideally, you would replicate a system and then test on the replica. How is that to be achieved with your critical building system? Even under the best of circumstances, testing an upgrade and the upgrade implementation is a lengthy and costly process, which requires careful planning. Since delay is inevitable, upgrading systems as the sole remedy is not an effective option.

Building Secure Systems

The other option is to secure building SCADA systems by design. To achieve this, the first and most important step is to accept that today's SCADA systems are IT systems, for which IT experts should design the appropriate environment. While designing the environment, the following areas should be considered:

1. Physical Security: Invite IT infrastructure and IT security experts to participate in the project during the early design stages. Then it is possible to ensure that the physical security and environmental requirements for the building SCADA systems are met in advance, rather than being retrofitted later with great difficulty (and at increased cost).
2. Infrastructure: Engage IT and IT security experts to help you design the appropriate IT infrastructure. A properly designed IT infrastructure will ensure that vulnerable building systems are never directly facing:
   a. The Internet;
   b. Any other remote access connection;
   c. Other building systems; or
   d. Your enterprise network.

   By means of a well placed and carefully managed set of firewalls, the IT experts can design and operate a properly secured network infrastructure. For each SCADA system the firewall configuration should block incoming and outgoing traffic by default. A secure VPN method may be implemented to provide remote access. Figure 2 shows how such a configuration might look.
3. System Standards: IT experts must define standards to specify:
   a. Software and hardware configurations for servers and desktops;
   b. Remote server management facilities; and
   c. Physical installation requirements.

   All SCADA system vendors must meet the standards to be considered for the bidding process.
4. Policies & Procedures: The IT experts create the IT policies and procedures, which the SCADA system vendors must comply with to be considered for the bidding process. Policies should include:
   a. Mandatory removal, disablement or renaming of default accounts;
   b. Password strength and password management;
   c. Malware scanning;
   d. Upgrading, patching and testing;
   e. Interconnectivity and firewalling between building SCADA systems, as well as enterprise and internet-based systems;
   f. Backup and recovery;
   g. Remote access; and
   h. Monitoring, including monitoring of administrative users and the creation of administrative user accounts by third parties.
5. Testing & Commissioning: Ask IT to define a set of testing and commissioning criteria which every system must meet to be accepted.
6. Responsibility: Appoint an organization to be responsible for the management and monitoring of your building SCADA systems, network and security, and seek their input during development and construction.
7. Change Management: Re-evaluate all of the above during the life span of the real estate project. IT develops much more quickly than any real estate project, necessitating ongoing adjustments and changes.

Conclusion

With a concerted plan combining technology, policy, and procedures, it is possible to design and implement a highly secure approach for even the most vulnerable SCADA systems, without having to sacrifice SCADA system connectivity. Building a secure system, however, requires a transformation with respect to when and how IT gets involved with a real estate project. •

The following websites provide further information:

www.ics-cert.us-cert.gov/	US Government Industrial Control Systems Cyber Emergency Response Team
www.securityincidents.net	Repository of Industrial Security Incidents
www.2024sight.com/publications	2024Sight publications

Anton Hofland is the CEO of 2024Sight. He has more than 20 years' experience in IT, IT infrastructure and enterprise networking, gained mostly in the financial industry. Prior to establishing 2024Sight he was the Head of IT for Arcapita Bank in Bahrain. Previously he has worked for several major financial institutions in the City of London. He has also worked in the area of telecommunications regulation and has experience in the telecommunications industry. Anton holds a M.Sc. in mathematics and computer science from Delft University, Netherlands.