WHITE PAPER

BUILDING RESISTANCE

A LOOK AT OT, IT AND MITIGATING RISK

Part 1 | **Smart buildings: A perfect storm of vulnerability**

How Did We Get Here?

Cyberattacks are increasing, and threat actors are continually evolving and looking for easy access. As IT boundaries strengthen, control systems offer a path of least resistance for these cyberthreats. The easy access that control systems offer began with years of focus on system availability to facility engineers and open protocols to allow interoperability between various manufacturer platforms and system types. Creating ease of serviceability by vendors to reduce maintenance cost and response speed has also widened this access for attackers. In addition to hacking risks, the severe fragmentation and turnover of contractors creates significant inconsistencies that lead to operational risks. Together, these factors form a perfect storm of vulnerability.

The Evolution of Control Systems

What is a control system?

A control system is an interconnection of components forming a system configuration that will provide the desired system response. Devices are distributed throughout a building and perform specific functions. Some devices act independently, such as power meters, air condition unit controllers or lighting controllers. In most cases, these devices communicate back to a head-end or front-end device. The front-end serves up web pages to the users, sends scheduling and control commands to the various devices in the field, and collects operational data.

The history of building control

Before the late '60s and early '70s, pneumatics were used to control valves and pumps to condition the space in buildings. In the late '70s and early '80s, this control transitioned to a mix of pneumatics and electric/electronic control, known as direct digital control (DDC). DDC exploded, and many control companies were established during the mid-'80s and '90s. These new companies were able to bring low-cost and highly functional systems to the market. However, most systems were proprietary, meaning that after installing a particular brand of control system only the manufacturer's product could be used for upgrades and expansions.

By the mid-'90s, the cost of DDC was much lower than the cost of pneumatics. This rapidly fueled the replacement of pneumatic controls and the expansion of traditional and nontraditional automation markets.

Image 1

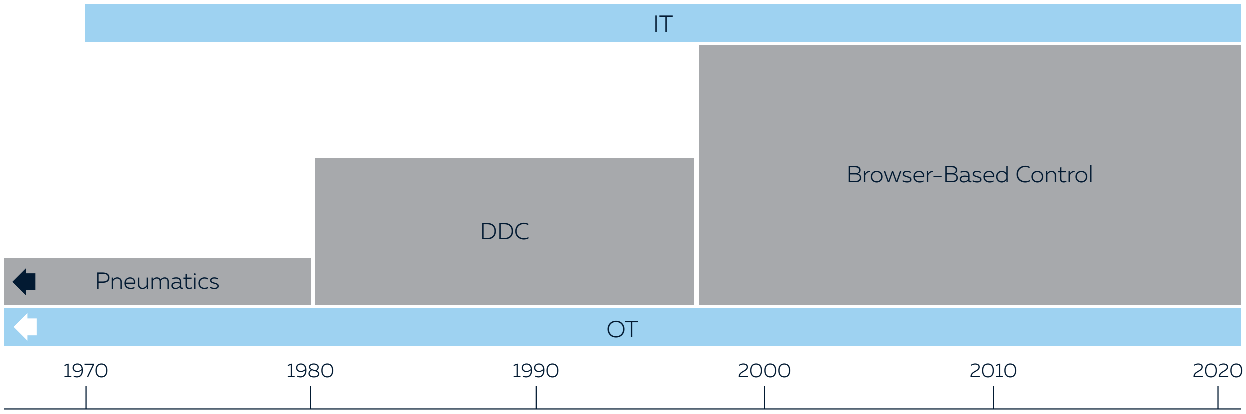


Image 1 – Timeline of operational technology (OT) beginning with pneumatics prior to 1970 to today's smart controllers overlayed with the progress of IT beginning in early 1970. The two technologies began to converge in the late 1990s with the advent of web-based controllers. The convergence ushered in the necessity for OT and IT to collaborate. However, collaboration is just now beginning to occur.

Four Critical Vulnerabilities Emerge

Vulnerability No. 1: Open protocols

During the mid-'90s, there was a movement to create open platforms. The goal was to give the end user flexibility to pick and choose manufacturers and create blended systems. Open protocols allowed for disparate manufacturer platforms to communicate easily with each other. This evolution began two distinct changes in the industry—skill sets of integrators needed to change and end users had more options for system design. However, this openness was the beginning of a vulnerability.

During this time, IT was evolving into what we know today, although IT and operational technology (OT) were independent of one another. Eventually, the paths of IT and OT would intersect.

In the early '70s, Robert Kahn and Vinton Cerf created the precursor of the internet. Kahn and Cerf developed the protocol necessary to create the "network of networks" starting in 1983.

Vulnerability No. 2: Lack of security foresight

With the advent of network-capable DDC and this new form of networking, OT integrators were required to connect these devices to the networks. This was a key moment for OT and IT. At the time, OT and IT did not intersect. If they had, the alignment could have significantly matured OT security, but because there had been no precedent for collaboration, aligning IT and OT wasn't a priority.

Vulnerability No. 3: Primary vendor control

Integrators by nature are service-oriented—it's why we continue to buy from certain vendors. In this sense, it allowed the vendors to fill a gap. IT departments already had their hands full with building and maintaining corporate networks, while IT departments were also grappling with a new invention: the internet.

Vendors began installing IT-type networks to facilitate the new network-based controllers, which worked well. Facilities had more control of their systems because they were not encumbered by IT policies and procedures. The vendor was happy to take care of all their network needs as opposed to being installed and maintained by IT departments.

Vulnerability No. 4: Open to the web

The next evolution for control systems was the introduction of controllers and control systems that could be accessed via a web browser in the late '90s. This eliminated the need for installing client software on the user machine/workstation. Through the use of a web browser, a user could view and control their system.

Despite this web access, the system could only be accessed via the vendor-supplied network because the networks were separated (or air-gapped) from any other networks. The next logical step would be to allow users on other networks (e.g., the corporate network) to access the system to see or control their environment. This allowed for several approaches, such as moving the devices to an IT-controlled network. However, the drawback to this solution was that IT departments did not understand that they would have to manage the devices. An alternative approach was having a PC serve as the front end joined to the corporate network and leave all the other devices on the original control network. IT departments only had to manage the PC, not the control devices. This was accomplished by adding a second network card to the front end, effectively bridging the networks.

Image 2

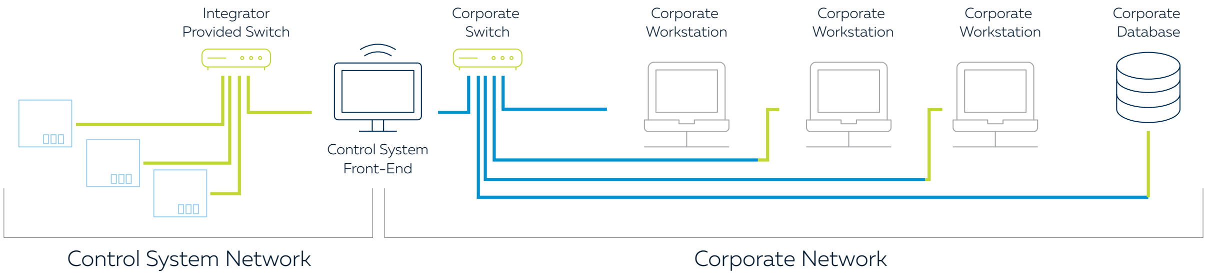


***Image 2** – This shows an OT network that has been bridged in the control system front end. The front end has two network interface cards (NICs). One NIC is connected to the OT network and the other NIC is connected to the corporate network, allowing corporate users access to the control system front end to control and/or view their environment.*

Image 3

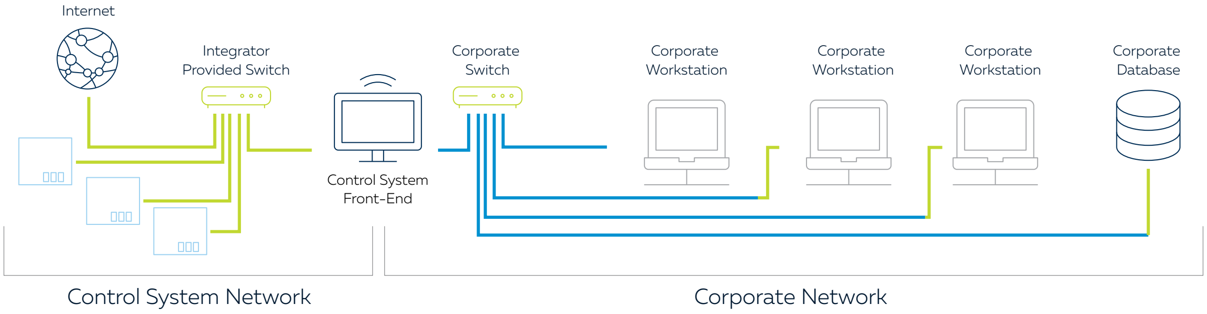


***Image 3** – Connecting to the internet allowed the outside world access to control systems. It also introduced a major risk to not only the control system, but also the corporate network. External users could theoretically pivot and gain unrestricted access to the corporate network.*

The bridged networks worked well for those inside the building, but what if facility engineers wanted to check on their building at night or weekends? If facility engineers had remote access to this information, it would eliminate the need to return to the building after hours, which would reduce costs and response time. Additionally, if costs and response time were reduced for facility engineers, the same could be done for the servicing vendor. Since the vendor was the original installer and IT departments were not typically involved, the vendor started taking on the responsibility of setting up and managing remote access.

Remote access was accomplished by exposing the front end to the web using a public IP address, meaning that there was nothing between the front end PC/server and the World Wide Web. The only available security feature was a login requirement for the front end. However, in some cases, either a password was not required to log in or a guest account was enabled, which required no login credentials at all. The front end's exposure to the World Wide Web allowed anyone to find the IP address and access the system. If it was also bridged to the corporate network, there would be a possibility that anyone could pivot and access the corporate network as well.

Image 4

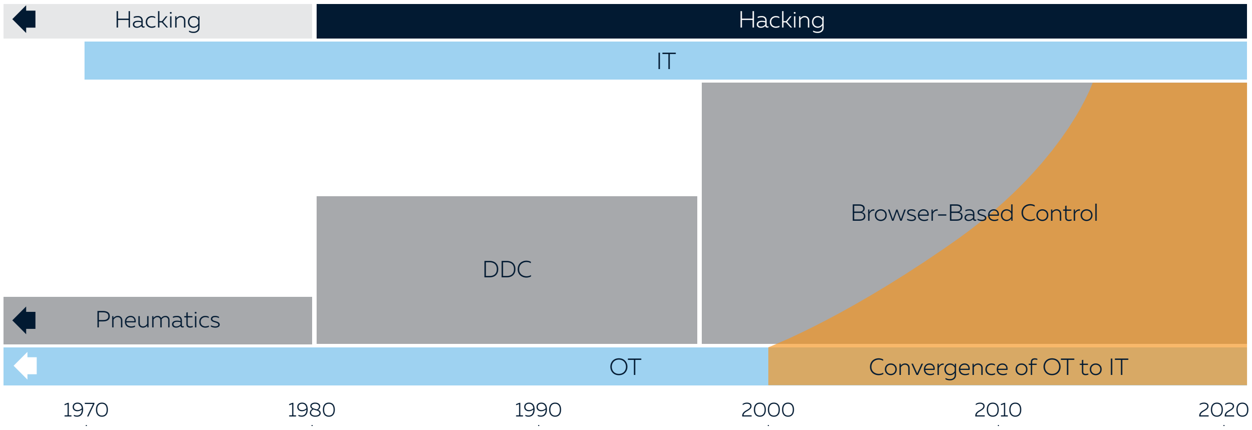


Image 4 – *IT and OT converge. Although OT devices were on the IT network before the mid-2010s, this represents the industry's movement from an OT-only network to an IT or IT/OT blended network.*

By the early 2000s, control systems were primed to be an easy attack vector. Control technology was an open platform, so anything or anybody with enough information could access and control a device. Information on how to do this, including default users and passwords, was readily available online from most manufacturers. With just a few keystrokes, anyone could use the web to download step-by-step manuals for accessing and controlling devices at the deepest levels. Vendors set up default credentials in the system so that anyone in their organization, past and present, could access thousands of systems.

For a time, no one noticed or cared that the security of these systems was so drastically compromised.

The History of OT Hacking

Hacking refers to gaining unauthorized access to data in a system or device. The motivations for hacking are simple: make a statement, cause mayhem and/or steal or destroy information. One of the earliest examples of hacking was in the '70s by a teenager named Kevin Mitnick, now considered the grandfather of hacking. He hacked phones (i.e., phreaking) to get free long distance calls for him and his college friends.

Hacking methods are as varied as the systems they attack. The most widely known method of hacking is Ransomware, which shuts down access to your data or system until a ransom is paid (typically in bitcoin). Hacking is all about the end goal; whatever means a hacker uses is immaterial, and they are unconcerned with the damage they may do. Hackers typically do not give up until they've achieved their goal—but they tend to take the path of least resistance to do it. This is referred to as the Path of Least Resistance Persistent Threat (POLRPT).

Image 5

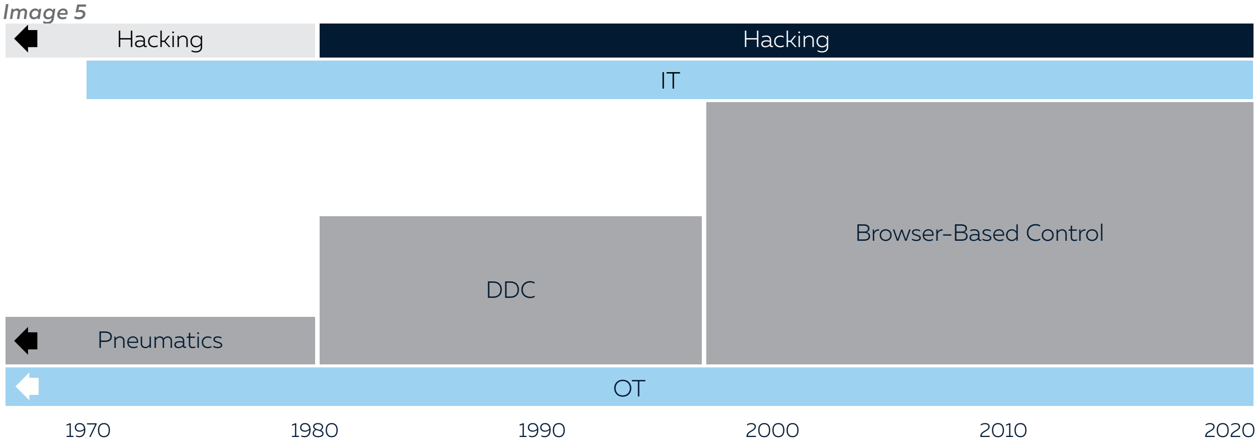


Image 5 – *In the '80s, hackers began turning their attention to IT networks. Image 5 depicts the timeline for when threat actors began hacking into IT and OT systems. The gray hacking bar is representative of other technology.*

The POLRPT mindset is part of the driving force that turned the attention of the hackers toward OT. Because OT offers a more vulnerable platform, it also offers a path of least resistance for hackers. Early trace evidence of OT hacking began around 2008 (see Image 6). These attacks were primarily focused on industrial control systems (ICS) that typically control oil and gas, power grids and production facilities.

Image 6

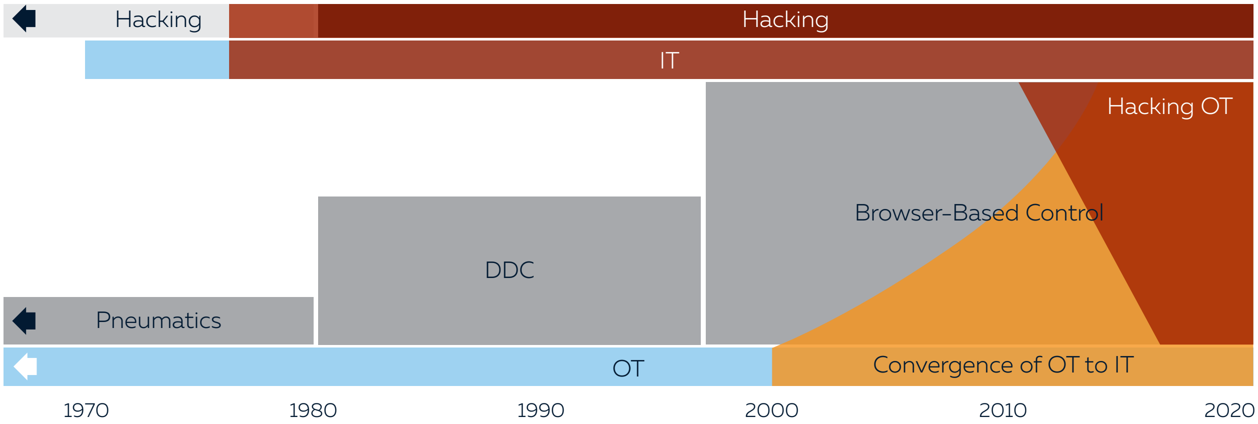
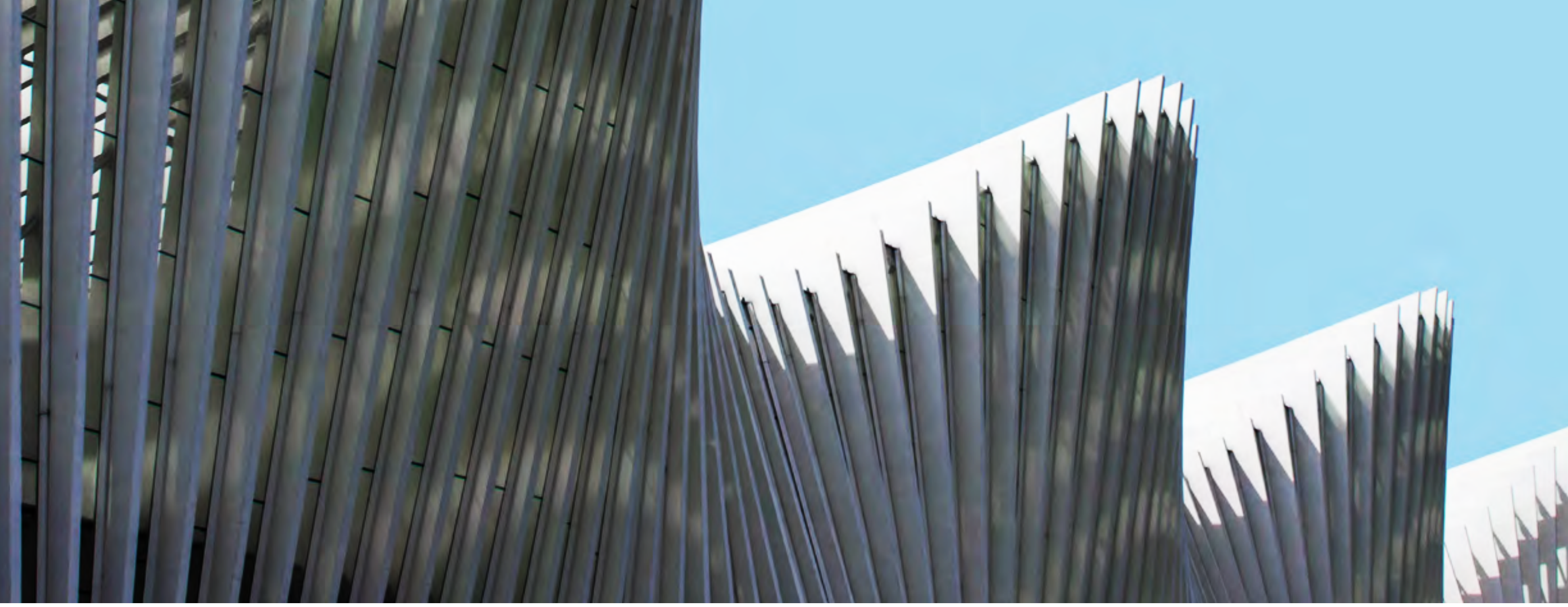


Image 6 – *The number of attacks on ICS has drastically increased since 2016. The top attack tactic has been ransomware, which can be avoided with proper knowledge and training.*

The Human Factor

Human behavior contributes to 80% of security risk to systems and devices. Ransomware, for example, requires human interaction to be enabled. It is typically delivered via email and requires the user to click or interact with an email. To date, all ransomware attacks have occurred on the front-end PC, which begs the question of why a person would access their email on the front end. A front end should be treated as a server, not a typical PC. We need to rethink and reclassify our front-end building control servers. The only function this PC/server should perform is controlling the building and serving up webpages so workstation operators can control the building.



How We Got Here ... and Where We Need to Go

Originally, control systems were not connected nor were they able to connect the DDC of valves and actuators that were controlled using compressed air. The brain of the system may have been a control board, and in some cases, there was even a computer, but the computer was not connected to any networks. These systems began to evolve to include browser-based control, which meant users without client software installed could use the system from any machine on the same network via a browser.

With open systems, one manufacturer system could communicate with another manufacturer system with little to no restriction. This openness-without-boundary defense created massive vulnerabilities in the systems.

The implementation of networks by integrators also influenced the vulnerability of control systems. Integrators weren't trained to follow basic security best practices. They installed off-the-shelf switches and exposed systems directly to the web via public IPs.

Facility management played a part as well. They relied heavily on the vendor to support the systems for remote access and system administration. This meant vendors had full-time access to the systems and theoretically could lock the company out of their control system. Integrators typically would install a single user that all past and present employees were aware of.

It is now up to the industry, through a collaborative effort between facility management, IT departments and the integrator, to secure control systems. There are several steps that can go a long way in increasing control system security:

1. **Inventory and assessment:** Most organizations don't know exactly what controls systems, contractors and connectivity exist in their portfolio, which makes even the most basic remediation cumbersome if not impossible. It is possible to get a low-cost, but comprehensive, inventory and assessment of risks.
2. **IT solutions:** Place publicly exposed devices behind a firewall or secure gateway device, with a facility management-owned and controlled remote access solution, and implement unique users with role-based access.
3. **Facility management solutions**: Create policy, not only for remote access but also importantly for system setup, configuration and backup of all control systems, and regularly audit and monitor compliance from contractors.

These three steps may not happen overnight but should be part of an immediate action plan that has a roadmap of progression and eventually incorporates all systems and connectivity (local and wide-area) into a proper IT process and controls environment.

Sources

Smart Building Automation Evolution, Ken Sinclair and Therese Sullivan.

About the Authors

Fred Gordy

Director of Cybersecurity, Intelligent Buildings

Fred Gordy is a smart building industry expert and thought leader with 20 years of experience in secure control system development and implementation for Fortune 500 companies. His control systems knowledge gives him insight on challenges of interlacing traditional IT environments with control systems for cohesive and security OT platforms. He has authored and participated in over 30 articles on building control cybersecurity with industry magazines as well as *The Wall Street Journal*, CNBC and healthcare publications. In the last decade, he has led control system cybersecurity workshops and has been a passionate speaker and teacher on the subject of building-control cybersecurity.

David Englebrick

Practice Manager, TEKsystems

With over 28 years in the telecommunications field, David Englebrick brings extensive experience in telecom design, operations and research and development. His focus has been serving clients in the higher education and government markets.

TEKsystems

Own change

We're partners in transformation. We help clients activate ideas and solutions to take advantage of a new world of opportunity. We are a team of 80,000 strong, working with over 6,000 clients, including 80% of the Fortune 500, across North America, Europe and Asia. As an industry leader in Full-Stack Technology Services, Talent Services and real-world application, we work with progressive leaders to drive change. That's the power of true partnership. TEKsystems is an Allegis Group company.

INTELLIGENT BUILDINGS™

IntelligentBuildings® is an nationally recognized Smart Building consulting and managed services company who leads the industry in operational technology cybersecurity and vendor risk management solutions. We help customers leverage solutions that enhance experience, increase productivity, lower costs and reduce risks for new building projects, existing portfolios and smart community development.