PNNL-29813

Challenges and Opportunities to Secure Buildings from Cyber Threats

March 2020

Hayden Reeve
Sri Nikhil Gupta Gourisetti
Penny McKenzie
Joe Hagerman (ORNL)
Andrew Nicholls
Michael Mylrea
Paul Ehrlich
Glenn Fink
Draguna Vrabie
Cliff Glantz
Ron Underhill

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express 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 any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-29813

Challenges and Opportunities to Secure Buildings from Cyber Threats

March 2020

Hayden Reeve
Sri Nikhil Gupta Gourisetti
Penny McKenzie
Joe Hagerman (ORNL)
Andrew Nicholls
Michael Mylrea
Paul Ehrlich
Glenn Fink
Draguna Vrabie
Cliff Glantz
Ron Underhill

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

Integrated and connected building control systems are becoming essential to provide a comfortable, safe, and efficient indoor environment. These systems have become more sophisticated and converged with commercial networks, as well as the internet. As a result, they are now being targeted for cyberattacks. This paper provides an overview of commercial control systems, potential cybersecurity risks to these systems, and discusses efforts underway in government and industry to protect these systems. It concludes with a discussion of the current challenges in deploying cybersecurity best practices and capabilities and presents existing gaps in capability and resources.

Summary

Buildings technology is increasingly digitized and connected to the internet, enabling new opportunities to improve occupant experience and energy efficiency, as well as to use renewable energy. The nation's 5.6 million commercial buildings use 19 percent of the nation's primary energy and 36 percent of its generated electric power. The Department of Energy's (DOE's) goal is to reduce this energy use per square foot in this sector by 30 percent by 2030, relative to 2010 levels. Achieving this goal, and other DOE goals—such as increased use of renewable energy and electric vehicles—that benefit from system-wide connectivity, interoperability, and control, will require the development and deployment at scale of advanced technology, including smart equipment, sensors, and controls that will increasingly be connected to the internet.

The national challenge to secure buildings from emerging cyber threats cannot be overstated. As the National Academies recently observed, however, "These systems provide critical services that allow a building to meet the functional and operational needs of building occupants, but they can also be easy targets for hackers and people with malicious intent…*As these systems are becoming more connected, so is their vulnerability to potential cyber-attacks*. [emphasis added]" Connectivity offers tremendous opportunity for realizing our energy efficiency and renewable energy goals but at the cost of increased cyber risk to our buildings. Cyber threats and vulnerabilities, or even the perception of increased risk, could hinder the adoption of smart, connected technology in commercial buildings and impede the realization of DOE's efficiency goals. For example, almost 50 percent of enterprise customers note security as their number one concern in the adoption of Internet-of-Things (IoT) technologies. Furthermore, half of commercial buildings typically have devices exposed to the internet, but 95 percent of sites do not have a disaster recovery plan; recent investigations suggest that nearly 40 percent of building management system servers have been targeted with malware, phishing scams, or ransomware. Even without intentional attacks, the increasing complexity of smart-building integrations increases the likelihood of disruptions and system failures from faulty patches, user errors, and poor maintenance. If not effectively addressed, these threats could significantly slow the deployment of high-value connected technologies and future energy efficiency gains.

Building control systems were once siloed and unconnected, limiting their exposure to cyber threats. However, increasing connectivity and growing complexity in smart buildings has increased the potential for vulnerabilities. These changes are driven by beneficial technologies such as remote monitoring, building-control applications, and grid services (such as OpenADR) which provide seamless occupant experiences. To combat this risk, the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) provides a structured framework to identify systems and vulnerabilities that should be addressed, define requirements to protect networks and devices, and to detect, respond to, and recover from attacks effectively. Various government and industry organizations have developed cybersecurity resources and activities for commercial buildings, and these are presented in Section 4.0.

Additional work is needed to ensure these resources adequately address the wide variety, maturity level, and risk profile of commercial building operators. The majority of best practices to date address only the "identify" and "protect" subdomains of the NIST CSF. Few resources exist for building operators to detect and respond to threats and to ensure rapid and cost-effective recovery. The need for a detection and response capability have clear analogues to the building communities' expertise in the research, development, and deployment of fault detection and diagnostics technologies and advanced adaptive controls.

Acknowledgments

This report is based, in part, on Pacific Northwest National Laboratory's (PNNL's) *Building Controls Cybersecurity Landscape* document, and the authors would like to thank Marina Sofos (APRA-E), Valerie Nubbe (GuideHouse), Stephanie Johnson (PNNL), Katheryn Farris (Microsoft), Teja Kuruganti (Oak Ridge National Laboratory), Ed Vineyard (US DOE), Alison Gotkin (Raytheon), and Paul Skare (PNNL) for the valuable input that they provided.

Acronyms and Abbreviations

ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigeration, and Air-conditioning Engineers
BACnet	Building Automation and Control Network
B-C2M2	Buildings Cybersecurity Capability Maturity Model
BAF	Blockchain Applicability Framework
BAS	Building Automation System
BCAP	Blockchain Cybersecurity Audit Platform
BCP	business continuity plan
BCF	Buildings Cybersecurity Framework
BCS	Blockchain-Based Cyber Security Solution
BTO	Building Technologies Office, Office of Energy Efficiency and Renewable Energy, DOE
C2M2	Cybersecurity Capability Maturity Model
CABA	Continental Automated Building Association
CEDS	Cybersecurity for Energy Delivery Systems
CI	Critical infrastructures
CPS	Cyber-Physical Systems
CRESt	Critical Infrastructure Resiliency, Efficiency, and Security
CRR	Cyber Resilience Review
CSF	Cybersecurity Framework
CyFEr	Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm
DHS	Department of Homeland Security
DMZ	demilitarized zone
DNS	Domain Name System
DOE	Department of Energy
EDS	energy delivery systems
EERE	Office of Energy Efficiency and Renewable Energy, DOE
EIA	Energy Information Administration, DOE
EO	Executive Order
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
EV	electric vehicle
F-C2M2	Facilities Cybersecurity Capability Maturity Model
FCF	Facility Cybersecurity Framework
FEDS	Facility Energy Decision System
FEMP	Federal Energy Management Program

FRisC	Framework to Analyze Cybersecurity Risks and Consequences for Critical Infrastructure
HVAC	heating ventilating, and air-conditioning
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team, Department of Homeland Security
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet-of-Things
IoT	Internet-of-Things
IoTCOE	IoT Common Operating Environment
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
MEEDS	Mitigation of Exposure of Energy Delivery Systems
NIST	National Institute of Standards and Technology
OE	Office of Electricity Delivery and Energy Reliability, DOE
OT	Operational Technology
PNNL	Pacific Northwest National Laboratory
RECC	Real Estate Cyber Consortium
Re-ISAC	Real Estate Information Sharing and Analysis Center
RMF	Risk Management Framework
SCADA	Supervisory Control and Data Acquisition
SD2-C2M2	Secure Design and Development Cybersecurity Capability Maturity Model
SHINE	Shodan Intelligence Extraction
TRL	Technology Readiness Level
UL	Underwriters Laboratory
VPN	Virtual Private Network

Contents

Abstract ii
Summary iii
Acknowledgments iv
Acronyms and Abbreviations v
Contents vii
1.0 Introduction 8
2.0 Background and Motivation 11
3.0 An Overview of Smart Building Systems, Vulnerabilities, and Cybersecurity Measures 16
3.1 Reference Architecture 16
3.2 Typical System Integrations 18
3.3 Example Vulnerabilities and Best Practices 19
4.0 Summary of Relevant Resources and Initiatives 25
4.1 Federal Agencies 25
National Institute for Standards and Technology 25
Department of Homeland Security 25
Department of Defense 26
Department of Energy 26
4.2 Industry Organizations 27
5.0 Deployment Challenges and Barriers 30
6.0 Conclusions 33
7.0 References 35
Appendix A – Overview of Commercial Building Systems A.1
Appendix B – Standards B.1
Appendix C – Communication Protocols C.1
Appendix D – Overview of Current Cybersecurity Buildings Efforts D.1

Figures

Figure 1. Commercial Building Reference Architecture 15
Figure 2. Secure Software Central services D.7
Figure 3. Microsoft's STRIDE model described D.8
Figure 4. VOLTTRON priorities. D.8

1.0 Introduction

Building control systems are essential to provide a comfortable, safe, and efficient indoor environment. These systems have become more sophisticated and have converged with commercial networks and the internet. The change to the network connectivity of these buildings has created a cyberattack vector that was not present before. This document provides an overview of the current cybersecurity landscape for commercial building technologies. It identifies relationships between buildings control systems and growing cybersecurity concerns and requirements, and introduces the existing tools, frameworks, and standards that are potentially relevant to the DOE's Office of Energy Efficiency and Renewable Energy Building Technologies Office's (BTO) goals and mission. It is intended for use by DOE's Energy Efficiency and Renewable Energy (EERE), BTO, and for industry stakeholders, including building owners and operators, suppliers, installers, Information Technology (IT)/Operational Technology (OT) professionals, and building managers.

There are 5.6 million commercial buildings in the United States, and this sector consumes 19 percent and 36 percent of the nation's primary energy and electricity use, respectively (EIA 2016); EERE's goal is to reduce, by 2030, commercial building energy use per square foot by 30 percent, relative to 2010 levels (EERE 2016). Achieving this goal, as well as other EERE goals that benefit from system-wide connectivity and optimization, will require the development and deployment of advanced technology, including advanced equipment, sensors, and controls, that will increasingly be digitized and connected to the internet. However, even the perception of risk or loss from a potential cyberattack hinders adoption of advanced connected buildings technologies and, thus, impedes attainment of EERE's efficiency goals for the nation.

A survey by Bain & Company showed that concern over cybersecurity is the number one barrier to the adoption of IoT technologies by enterprise customers. Of the executives surveyed, 45 percent listed security as their number one concern, with 60 percent of respondents stating they were very concerned about the risks (Bain & Company 2018). It is also important to remember that "cyber security must address not only deliberate attacks, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters (NIST 2010)." In this sense the impact of cyberattacks can often be indistinguishable from operational failures (for example, a hardware failure or faulty patch update taking out a key facility system). Maintaining a strong cyber posture increases an organization's resilience to increasing cyber issues, both from malicious intent and from operational failures.

Effective cyber resilience has similarities to risk management in other fields. For example, for human health, individuals understand the value of basic hygiene (like hand washing), healthy habits (diet and exercise), and response protocols (first aid techniques). In addition, citizens know who to call when additional expertise or care is required (primary care physicians and specialist); during a serious event (first responders), and when the risk of a catastrophic event needs to be underwritten (insurers). The cybersecurity resilience equivalent elements are not as well-established and understood, especially as it relates to building and facility stakeholders. Given the recent emergence of smart buildings and the rapidly changing cyber threat environment, many building operators are struggling to understand cyber risks, the value of proactive cybersecurity, and how to prioritize improving their cyber posture to achieve cyber resilience.

DOE has a critical role to play in educating the buildings community on the cyber resiliency of their systems. As the Quadrennial Energy Review states, "While the Department of Homeland

Security coordinates the overall Federal effort to promote the security and resilience of the nation's critical infrastructure, in accordance with Presidential Policy Directive-21, the Department of Energy serves as the day-to-day Federal interface *for sector-specific activities to improve security and resilience in the energy sector*. [emphasis added]" (Obama Administration 2015).

For these reasons, multiple DOE offices, including BTO and the Federal Energy Management Program (FEMP) have been evaluating cybersecurity from a holistic buildings-cyber-physical perspective. In 2020, EERE put forward a holistic cybersecurity strategy to enable its 13 offices to move toward cyber resilience and improve its ability to realize White House Executive Order 13800 goals to identify, detect, and respond to and protect and recover from cyber threats and vulnerabilities targeting critical systems and networks of its diverse stakeholders, all of which require secure buildings to function. In addition to the EERE cyber strategy and complementary strategies from the Departments of Defense, Energy, and Homeland Security, there are coordinated efforts underway to develop a cybersecurity capability and engage a wide range of industry and government stakeholders in a conversation about how best to enhance the cybersecurity of the nation's buildings. For example, in 2016, BTO and PNNL conducted an early stage investigation to evaluate the development of a buildings CSF document. Since 2018, FEMP and PNNL have been developing a wide range of cybersecurity tools, best practices, and frameworks to enhance awareness of the OT operators and owners of federal facilities and improve the cybersecurity posture of their buildings. In 2019, BTO hosted the Cybersecurity Roundtable meeting to understand the perspectives and best practices of commercial building operators and stakeholders. Beyond EERE's investments, DOE's Office of Electricity Delivery and Energy Reliability (DOE OE) and Cybersecurity, Energy Security, and Emergency Response (CESER) have been facilitating research and development to adopt and develop technologies improving cybersecurity and resiliency of industrial control systems (ICSs), especially energy delivery systems (EDSs).

Note that, while the buildings environment OT has similarities to ICS (e.g., long lifecycle with many legacy systems not designed for connectivity), there are also many differences, such as a lack of cyber security mandate and a fragmented delivery chain, especially for small facilities. Such legacy systems were originally designed for dedicated networks and often lack built-in security features to protect them from cyberattacks (Ranathunga et al. 2016). While the commercial building industry does recognize some protective practices, they are not as robust as best practices used in other industries, and not all installations comply.

In this context, it is important to understand that nearly 90 percent of all commercial buildings are small (under 25,000 square feet in floor area) and half are under 5,000 square feet (EIA 2012a). Many of these buildings do not have dedicated energy management staff, building automation systems, and other resources that some of the larger buildings possess. While increasing cybersecurity awareness and protection for all buildings is important, doing so for this sector of smaller buildings, and providing actionable and concise guidance, will be essential. Resource constraints, a complex, evolving cyber threat, and rapidly changing technology make these goals particularly challenging for resource constrained facilities.

This paper provides an overview of building control systems and potential cybersecurity risks to these systems, and it discusses efforts under way in government and industry to protect these systems. Section 2.0 describes examples of recent cyberattacks and potential threats that are the driving motivation for improved cybersecurity and presents trends on increased attack incidence. Section 3.0 outlines growth of connectivity and complexity in smart buildings, the increase in potential vulnerabilities, and role of cybersecurity in building controls. The

cybersecurity resources and activities of a number of government and industry organizations relevant to commercial buildings are presented in Section 4.0. Section 5.0 provides a summary of the challenges and barriers to developing and deploying cybersecurity best practices for building operators. Section 6.0 concludes with a summary of key gaps, in deployment and research, which are intended to catalyze a conversation about how best to continually increase the cybersecurity of the nation's buildings.

2.0 Background and Motivation

As the National Academies observes (Federal Facilities Council 2015), "The nation's buildings are increasingly relying on building control systems with embedded communications technology and many are enabled via the Internet.[1] These systems provide critical services that allow a building to meet the functional, operational, and energy efficiency needs of building occupants, but they can also be easy targets for hackers and people with malicious intent. These facilities contain building and access control systems, such as heating, ventilation, and air-conditioning; electronic card readers; and closed-circuit camera systems, that are increasingly being automated and connected to other information systems or networks and the Internet. *As these systems are becoming more connected, so is their vulnerability to potential cyber-attacks*. [emphasis added]"

In addition to the inherent vulnerabilities of increased connectiveness, the cyber-physical security threat to buildings is also complex, dynamic, and rapidly evolving as OT and IT continue to converge in buildings and their related critical infrastructures (CI; Mylrea 2014). These vulnerabilities continue to be exploited in critical cyber and physical systems and components. According to DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 56 percent of 257 recorded cyber incidents targeted critical energy infrastructure (up from 40 percent in 2012). Buildings are increasingly playing a role in critical energy infrastructure, with integrated and interconnected edge devices in buildings sending information back into critical electricity infrastructure that powers all other 15 CIs that support our nation's economy, national security, and livelihood (NCCIC 2015).

In a digital age of ubiquitous sensing and networked control systems, securing buildings from emerging cyber threats is increasingly necessary to secure CIs. Yet, while many cybersecurity policies, procedures, standards, and risk management frameworks exist for traditional IT systems and ICS, insufficient effort has been spent adapting and extending these resources for the building OT environment. This lack of tailored resources was a key gap identified by the BTO Building Cybersecurity Roundtable (Crowe et al. 2019). Moreover, the U.S. Government Accountability Office recognized additional gaps in a recent report (GAO 2014) that noted the U.S. government was not "addressing cyber risk to building and access control systems particularly at the nearly 9,000 federal facilities protected by the Federal Protective Service as of October 2014." The report also noted that the U.S. government "lacks a strategy that: (1) defines the problem, (2) identifies the roles and responsibilities, (3) analyzes the resources needed, and (4) identifies a methodology for assessing the cyber risk (GAO 2014)."

Malicious actors in cyberspace have identified these gaps and continue to exploit critical vulnerabilities, resulting in financial, reputational, and physical damage to private and public organizations. For example, cyberattacks targeting U.S. critical energy infrastructure are increasing. During fiscal year 2013–2014, DHS' United States Computer Emergency Readiness Team reported more than 200 hacking incidents at energy companies (NCCIC 2015). A detailed analysis of these attacks reveals a number of potential vulnerabilities that could enable hackers to exploit building systems, controls, and devices. DHS also reported that malicious actors in cyberspace are continuously probing U.S. CI networks to discover and exploit vulnerabilities. In addition, most of the attacks against controls systems that are found in buildings and energy

[1] Such networked systems are sometimes referred to as IoT or industrial IoT (IIoT), implying a network of interconnected devices, smart or otherwise.

infrastructure evaded the defenses deployed by operators. Many of the legacy control systems do not have the necessary cyber defenses to ward off attacks, and those that do are often times not configured properly. It is evident that, while traditional security policies, procedures, and defenses, such as authentication, access control, and encryption, are necessary, these defenses can be easily bypassed by cyberattacks that are both sophisticated (zero-day exploits)[2] and simple (phishing attacks). Clearly, our adversaries have the capability to disrupt commonly deployed buildings systems. They lack only a convenient occasion providing the motivation to do so. Hence, we need to design more comprehensive security architecture and risk management solutions that prevent, detect, and respond to cyber threats and proactively mitigate vulnerabilities.

Two sophisticated cyberattacks on electricity infrastructure in Ukraine in 2015 and 2016 led to physical damage to CI and OT. One attack even targeted the uninterruptible power supply in one of the utility's control room facility, leaving grid operators in the dark while they were trying to restore operations. Similar recent high profile and destructive attacks include Not Petya, which caused over 10 billion dollars of damage and shut down critical IT and OT in ports and other critical facilities globally. Industroyer was another malware with a pre-defined timer containing the date and time for a destructive attack on OT to take place (Cherepanov 2017).[3]. These highly targeted attacks may accidentally leak across the Internet to harm connected buildings systems, even if the political motivation to target them is lacking.

While buildings present a rich target, their building automation systems and control systems also lack the necessary defenses. To prove that point, a team of ethical hackers from IBM used simple scanning techniques to hack into a building management company that operated more than 20 buildings across the United States. Scanning helped highlight flaws in the firmware, which facilitated access to the management system in one building. They found a remote execution flaw that gave them access to the management company's central server and all the buildings the company controlled. With access and the ability to control the building automation systems in 20 different buildings, they could have easily caused damage to a data center in one building by turning up the heat and shutting off the air-conditioning. As building owners and operators increasingly connect their IT infrastructure with their Building Automation System (BAS), penetrating the building controls could open access to the entire IT enterprise network, increasing the amount of damage a hacker could do (Ionesco 2016).

The growth in the number of networked devices and control systems in buildings creates another major challenge that must be addressed (Hardin et al. 2015). Devices are often designed and deployed with functionality, price, and ease-of-use in mind, as highlighted by a study by HP that noted 70 percent of the most common IoT devices contained vulnerabilities, with an average of 25 vulnerabilities per device (HP 2014). This energy IoT environment

---

[2] As defined by Wikipedia at https://en.wikipedia.org/wiki/Zero-day_(computing), a zero-day (also known as zero-hour or 0-day) vulnerability is an undisclosed computer-software vulnerability that hackers can exploit to adversely affect computer programs, data, additional computers, or a network. It is known as a "zero-day" because once the flaw becomes known, the software's author has zero days in which to plan and advise any mitigation against its exploitation (for example, by advising workarounds or by issuing patches).

[3] Industroyer brief: The first part of the malware included a denial-of-service tool that targeted protection relays, rendering them unresponsive. The second was a wiper tool that honed in on Microsoft Windows workstations used to administer, control, and configure protection relays though ABB MicroScada software. The data wiper scanned workstation hard drives for specific file extensions belonging to the software. If these files were detected, the wiper removed them all, preventing recovery unless a backup was available. The malware then crashed the system.

expands the attack landscape, making traditional security mitigation procedures and mitigations like secure configuration, white listing, patch management, and inventory a herculean task. In contrast, this increasing digital footprint makes a hacker's job easier.

The vulnerability of IoT devices was highlighted when the Mirai Botnet attack used a virus to infect over 600,000 IoT devices (mostly video cameras, many of which are installed in building IT networks), by gaining access using factory default usernames and passwords. These infected devices could then be remotely triggered to launch a massive distributed denial of service attack on more critical systems. Attacks launched against several sites impacted businesses and shut down portions of the internet. Widespread world-wide-web outages resulted when the Domain Name System (DNS) was knocked offline (Fruhlinger 2018; Antonakakis et al. 2017). Variations of this approach continue to be developed and deployed.

Beyond the headlines, cyberattacks on commercial building OT systems are increasing: building control systems are being attacked with ransomware and remote access control gained directly over building equipment. Data published by Intelligent Buildings shows that half of the sites they assessed in 2018 had devices directly exposed to the internet and could be accessed remotely, and 95 percent of the sites had no disaster recovery plan or had not changed default configurations and ports (Gordy 2019). Research has also shown that BAS operators struggle to differentiate the criticality of various vulnerabilities and associated mitigations (Brooks, Coole, and Haskell-Dowland 2019). Survey results from over 300 practitioners showed that "*23 BACS vulnerabilities were found to be equally critical with limited variance. Mitigation strategies were no better, with respondents indicating poor threat diagnosis*." This was in contrast to security professionals who showed an ability to differentiate and prioritize vulnerabilities and mitigation strategies.

Another study, Project SHINE (Shodan Intelligence Extraction), was conducted using Shodan, an easy-to-use scanning tool that can identify devices with routable IP addresses, including computers, building automation controls, webcams, and industrial control devices. Shodan crawls the internet, indexing devices and interrogating available services along the way. The study found over 500,000 Internet-facing control systems' assets, such as remote terminal units and programmable logic controllers. Of the assets found, 13,475 devices were heating ventilating, and air-conditioning (HVAC) and BASs from popular vendors. The study suggests that these systems provide an indirect avenue of attack and allow attackers to penetrate networks and scan other vulnerable systems. Most of these systems did not include adequate encryption or firewalls to prevent threat actors' entry into the buildings and IT networks (Radvanovsky 2013). Of the sample set, researchers found 204,416 serial-to-Ethernet devices that bypass traditional firewalls and can be accessed directly, in part, because system integrators prioritize functionality and ease-of-use before security controls (O'Harrow 2012). Shodan was originally intended only as an illustration of vulnerability, but it has been used to attack the systems it finds. Shodan is a simple scanner; many other purpose-built tools exist and are in use by adversaries.

More recently, an analysis by Kaspersky Labs of 40,000 servers used by building automation servers showed that 37.8 percent of these computers had been targeted by a mix of malware, phishing scams, and ransomware (Memoori 2019). "The majority of threats came from the internet … with 26% of infection attempts being web-born. Removable media including flash sticks and external hard drives were only responsible for 10% of cases, the same percentage that faced threats from email links or attachments. While just 1.5% of smart building computers were found to have been attacked from sources within the organization network, such as shared folders."

In small- and medium-sized commercial buildings that typically do not have a BAS, many of the functions are performed by individual IoT devices with varying levels of security. A recent analysis (Kumar et al. 2019) of 83M IoT devices across 16M global homes showed that the cybersecurity posture of these devices varied greatly by vendor and geographic region. For example, for some vendors and regions, nearly half of the devices have easy-to-guess or well-known hard-coded passwords. While this study focused on residential data, many of the devices (e.g., printers, security cameras, thermostats) are also used in small-to-medium-sized commercial buildings. Collectively, these studies illustrate a lack of cybersecurity awareness and implementation of best practices by building operators.

A Symantec study (Osborne 2015) highlights that vendors often prioritize ease of use and interoperability above cybersecurity, inducing the following vulnerabilities:

- devices lack encryption
- devices allow for simple or hard -coded passwords
- devices send sensitive information over open networks
- threat actors can intercept information, manipulate and take control of devices, and use that foothold to break into corporate networks.

Based on the above attack surface and threat landscape analysis, it is evident that there is a strong need for cybersecurity research and outreach. In collaborative efforts between DOE and the national laboratories, the development of cyber tools and processes can help building owners and operators identify their critical systems and processes, protect their OT networks against malicious and non-malicious actors, defend their building control systems from cyber threat actors, and effectively respond to and recover from cyber intrusions.

Cybersecurity is a continuous process. Cyber threat actors have many open source tools at their disposal to achieve their goals. Therefore, it is almost impossible to achieve a zero-risk state with 100 percent security. Vigilance requires not only to train the building owners and operators but also to provide them with needed research-supported processes to effectively meet their organizational goals in a secure fashion.

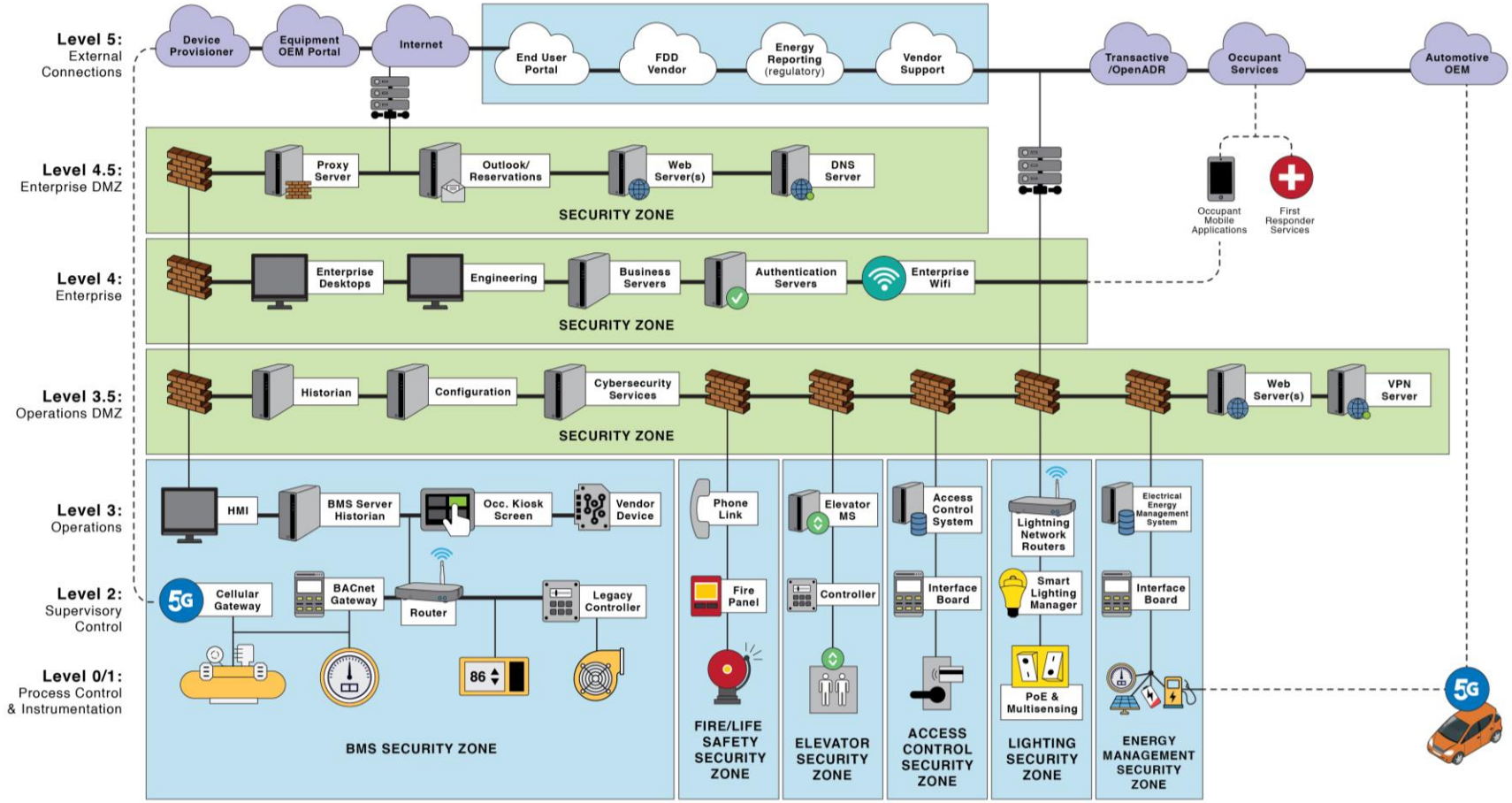

Figure 1. Commercial Building Reference Architecture

3.0 An Overview of Smart Building Systems, Vulnerabilities, and Cybersecurity Measures

Historically, building control systems and building equipment were unconnected, independent, and analog. Even digital building control systems frequently relied on proprietary operating systems, logic, and algorithms and fundamentally lacked external connections with other systems. However, many of today's buildings have digitally evolved—building control systems are increasingly automated, connected, and available on internal and external networks. In a recent Building Operating Management survey, 84 percent of respondents said that their BASs were connected to the internet (Snyder 2015). In addition, systems within a building are being integrated to enable additional functionality to occupants and operators. However, these integrations can increase the vulnerability of the building. This section presents a representative building system architecture (Figure 1) to support discussion of example cross system integrations and external connections, the potential resulting vulnerabilities, and example cybersecurity practices that can minimize these.

3.1 Reference Architecture

The reference architecture (Figure 1) is not intended to be prescriptive, complete, or representative of every commercial building but to represent a superset of features commonly seen in smart buildings. It is based on the Purdue enterprise reference architecture and parallels the architecture defined by PNNL for ICS and Supervisory Control and Data Acquisition (SCADA) systems with a focus on the utility industry (Mahan et al. 2011).

- Level 0: At the lowest level of the reference architecture are the actual physical processes and associated devices required to run the building. Those devices include basic sensors and actuators, smart sensors and smart actuators, process-specific automation machinery, other field instrumentation devices, and fieldbus networks communication gateways. Level 0 essentially encompasses field devices and the functions involved in communicating between cyber and physical systems.
- Level 1: Directly coupled with the level 0 processes and devices are the site-specific control devices. These control devices commonly include devices such as the distributed control system, programmable logic controllers, dedicated building operator workstations, control processors, and process-specific microcontrollers. Other buildings-related, process-specific systems at level 1 include (left to right in Figure 1) chillers, thermostat controller, and ventilation fans (HVAC system); smoke detector and sprinkler (fire protection system) controller; elevator controller connected to the call buttons and hoist motors (vertical transportation system); security controls related to the door locks and security badge readers (access control system); lighting and switching controls including presence detector processes and controls (lighting system); and backup power supplies, on-site power generators, and control systems related to the electric vehicle chargers (energy management system).
- Level 2: These devices may have embedded controllers and receive inputs from supervisory controllers that are coordinating multiple devices within a system, for example, supervisory control of an Air Handler Unit, and its variable air volume terminal units (dampers) and thermostats in each building zone. Unlike the level 1 systems, which are related to local control processes, at level 2 reside the supervisory processes that control collections of local processes. Level 2 wide-area systems include operations alarm servers, process analytic

systems, security event collectors, communication frontends, data historians (potentially in large buildings), network and application administrator workstations, and dedicated workstations specific to each process, or particular OT network segment.

- Level 3: These systems are often similar to the level 2 systems except their scope is building-wide, whereas the level 2 systems are associated with a segment in a building. In buildings, level 2 and 3 may overlap to some extent if the building is small enough and does not justify a need to have multiple segments and process lines. As a general set of best practices, level 3 systems should be divided into multiple separately secured subnets. Subnets can be based on system functions and role. Common systems in level 3 include master servers that are managing processes for the whole building, building-wide alarm servers, aggregate historians and databases that can be replicated to read-only historians in the network's demilitarized zone (DMZ), operations simulation modeling and tracking tools, and others. In some cases, level 3 may also have operations-specific IT services including Dynamic Host Configuration Protocol, Lightweight Directory Access Protocol, Active directory, DNS, and file servers. However, such services, if configured correctly, are separate from the enterprise IT network and are only dedicated to the OT network. Level 3 controls and systems related to cybersecurity may include OT-related Security Information and Event Management, patch management servers, or host-based protection software servers.
- Level 3.5: Between the operations layer (level 3) that enables operators to monitor OT systems building-wide and reprogram them if required, and external systems or the enterprise IT system (level 4) there should be what is called a "demilitarized zone (DMZ)". A DMZ typically sits between internal and external systems and is separated from both by firewalls. Only servers that provide services to both layers live in the DMZ, and the services they offer are very limited and restricted. Nothing else is allowed in the DMZ to make monitoring the DMZ systems and writing the firewall rules protecting them simpler. Intrusion detection systems (both signature and anomaly based), access control lists, logging, and recording, and cyber-attack incident response capabilities are in the DMZ layer. In large buildings, multiple DMZs may be required to provide sufficient segmentation. All communications between level 3 and the enterprise network (level 4 and 5) should be intercepted and regulated by the DMZ. Direct connections between level 3 and enterprise network devices are eliminated and no level 3 system may talk to an external host unless the carefully controlled DMZ VNC server is configured to allow it. To establish these one-way communications, devices known as "data diodes" and "unidirectional gateways" can be used.
- Level 4: The IT network contains traditional IT assets such as employee person computers and workstations, databases containing customer, employee, and intellectual property data, and other traditional IT systems. There is typically an IT DMZ (level 4.5) that contains servers hosting externally facing services (e.g., email, web hosting, etc.) and associated firewalls that also mediates level 4 connection to the internet.
- Level 5: The fifth conceptual level encapsulates the idea of external devices, services, and connections, many of which may be cloud-based. Level 5 systems also include internet access points, email servers, external stakeholder-facing web servers, internal web servers, Human Resources systems, corporate directory architectures, remote access VPN endpoints, enterprise document management systems, and partner and service provider portals.

An overview of individual building systems is provided in Appendix A, and a summary of building communication protocols is provided in 7.0Appendix C.

3.2 Typical System Integrations

A growing number of deployed smart building integrations are interconnecting traditionally siloed (and often disconnected) building systems. For example, proxies for occupancy presence, such as badge swipes at access readers, and security video footage, are being used by other systems to improve performance. Security footage has been used to not only determine crowd size to improve HVAC control, but also for improved dispatch of elevators (Romano, Rusert, and Reeve 2015). These integrations also extend to life safety applications, including the commandeering of the HVAC ventilation system by the fire protection system to manage smoke propagation and, more recently, the fire system using the occupant evacuation operation response protocol to automatically dispatch elevators to floors where smoke has been detected to expedite the egress of occupants in tall buildings (NEII 2016). These integrations are also extending into the IT system, with conference room calendars and hotel reservation systems used to predict future occupancy and, thereby, dynamically schedule HVAC systems. The growing capability and deployment of smart, sensor-rich, connected lighting systems will continue to drive the number and sophistication of these integrations. Beyond interconnectivity within the building and enterprise, there are an increasing number of connections to external systems, including a rapid increase in cloud connectivity. This has traditionally supported the remote access of building systems for operators and service providers. More recent examples include enabling the BAS to 1) receive grid signals (such as OpenADR) to provide demand response and other grid services; 2) integrate with cloud-based services providing energy monitoring (including regulatory energy reporting), fault detection and diagnostics capabilities, and control optimization; and 3) providing occupant services (such as comfort control, keyless access, and indoor location-based services) through their personal mobile devices. In addition, legacy systems are often being connected directly to cloud portals. Energy monitoring and fault detection and diagnostics providers may install a single board computer (such as a Raspberry Pi) on the OT network to support the integration of legacy BAS devices to a remote monitoring cloud platform. Maintenance service providers and original equipment manufacturers are also using cellular gateway devices to connect new and existing HVAC equipment directly to their own cloud portals for remote monitoring and diagnostics. Cellular gateway devices are popular, as they avoid the often expensive and time-consuming process of understanding and complying with the cybersecurity requirements of a customer's OT network and address the need for connectivity when none exists (as is often the case in small- and medium-sized commercial buildings). It is expected that the number and type of building connections will only continue to grow. For example, cellular connectivity is also a growing trend in automobiles, including electric vehicles (EVs) that connect to building smart chargers, offering another connectivity path. Also, it is expected that, in the future, buildings systems such as the fire protection system, security system, and elevator systems will provide information directly to first responders to improve situational awareness during emergency events such as fires and active shooters.

While every such integration enhances the services and capabilities of the overall building and improves communication between systems, one should note that these connections also form back doors that may bypass security controls normally enforced by DMZ systems. These integrations can make for porous security with multiple, seldom documented and often intermittent points of connectivity. Usually these connections are made for convenience of operation, but such connections make inventorying access points and diagnosing intrusions extremely difficult. Best practice dictates minimizing these connections and documenting them where elimination is not possible. Every such connection point greatly increases the difficulty of writing a safe set of access control rules and adds complexity to security at a rate that grows exponentially with the number of such connections.

3.3 Example Vulnerabilities and Best Practices

This increasing level of connectivity and automation, (from the simplest deployments in a connected, programmable thermostat to a complex network of building automation and building control systems that operate in smart buildings) can enable increased efficiencies and grid and occupant services and achieve substantial cost savings as compared to closed analog or digital systems. Yet, to an individual or group with malicious intent, this IT/OT convergence of connectivity and automation provides an attack surface that compromises the building's confidentiality, integrity, and availability, as well as potentially business sensitive information, if the building controls share the same network infrastructure. The degree of automation deployed in buildings will likely amplify the impact of operator error and system misconfiguration events—whether unintentional or deliberate. The end result is an increased level of complexity and brittleness that can raise the vulnerability of the system and decrease cyber resilience if not properly identified and addressed.

The NIST (2018) CSF provides a structure to systematically improve an organization's cybersecurity posture. The first step 'Identify' involves understanding the systems, devices, and data within a facility, who has access to these, and the corresponding risks. Often, buildings owners and operators do not have an inventory of what devices are connected, what systems they are connected to, and who has access (both on-site and remotely). As described above, vendors may have installed devices with cellular connections to support data exfiltration to enable monitoring and this provides undocumented and possibly vulnerable access to the networks to which these devices are connected. Detecting these shadow networks is notoriously difficult. Legacy systems may also contain undocumented devices and connections. New systems may collect data that is considered personally identifiable information requiring an increased level of protection. In other words, you cannot secure devices you do not know are connected and potentially vulnerable. This challenge has been exacerbated by virtualization and today's IoT environment characterized by ubiquitous deployments of mobile and networked devices.[4]

Another key part of the identify step is to determine the cybersecurity risks associated with the site. This is often a function of the motivations of the threat actor. Threat actors include:

- Disgruntled employees, or any person who simply want to create disruptions
- Blackhat "researchers"
- Competitors and their agents
- Terrorists, "hacktivists," or state-sponsored actors with political agendas

The objectives and motivation of those who might wish to compromise building systems and equipment include, but are not limited to:

- denial of service, potentially as part of a ransom scheme
- trying to demonstrate system weakness
- theft of intellectual property

[4] Networked devices span a wide range of control systems such as lighting systems, HVAC-related controls and sensors, occupancy- and safety-related autonomous and data acquisition systems, etc. Publications related to networked systems and protocols pertaining to smart buildings include Minoli, Sohraby, and Occhiogrosso 2017; Zafari, Papapanagiotou, and Christidis 2016; and Plageras et al. 2018.

- negatively affecting the public image of a company and, thereby, taking advantage of a predictable drop in its share price
- compromising a building system to expose the other networks comingled with the control system
- inferring national security strategic information from building occupancy
- disrupting critical energy services through malware that affects the connected energy infrastructure.

Building systems can also be compromised when well-intentioned but inadequately trained building operators or vendors misconfigure sophisticated control systems—everything can be set correctly to protect a complex system, but there may be too many entry points or option points to cost-effectively secure against all potential cyberattacks. Therefore, the cybersecurity plan must be tailored to the building, the building's intended use, and the owners, occupants, and equipment within the facility. Additionally, the building operators may not understand how the building networks are structured, shared by tenants, or exposed to the internet. Uncertainty may be caused by the dynamic nature of network development or simply be undocumented components that were added without application of appropriate network controls.

Once the systems and associated risks have been identified, the second step is "Protection." The most prominent form of protection is network protection, including access control. Examples include (but are not limited to):

- Implementing appropriate access controls, including removal of default or guest accounts, preventing concurrent logins, use of strong passwords following NIST guidelines, and ensuring that people do not have access or permission levels that they do not need (the concept of least privileges).
- Ensuring that devices and systems are securely configured and consistently maintained. Part of this security hardening includes closing any transmission control protocol ports that are not strictly necessary for operation and reducing to a minimum the number of services a given endpoint offers. Connectivity to the outside world should be eliminated or mediated entirely through the building's controlled network. Insecure default configurations such as open telnet or ftp ports or non-individualized factory passwords should be hardened. Sensitive data should be identified and encrypted both at rest and in transit, and software updates (patches) should be implemented. Maintaining up-to-date software on building devices can be challenging, as vendors may not support updates for the entirety of the typically long life of the equipment, resulting in the need for a planned end-of-life and obsolesce strategy.
- Implement need-to-know, least-privilege, and job rotation to eliminate problems like single points of failure or privilege escalation and aggregation. In addition, implement access controls (either mandatory access controls, discretionary access controls, role-based access controls, or some combination of these), to support the confidentiality, integrity, and availability requirements of OT networks and systems.
- The IT and various OT networks should be segregated to prevent threat actors who gain access to the HVAC OT network from by default obtaining access to other building systems or the enterprise IT system. Because IT and OT systems have different functions and different users, they should not be on one common network. Network segregation enables a "defense-in-depth" strategy where layers of controls must be breached to gain illicit access. Isolating building controls traffic using either a dedicated controls network or the use of a protected local area network subnet, virtual local area network, or via software-defined networking all

provide for an added level of cyber protection. Isolating devices into segmented subnetworks allows security rules to better describe acceptable behavior and identify anomalous behavior. For instance, only traffic from approved devices is allowed to transfer between heterogenous networks (known as whitelisting). In certain rare situations where there may be a need for certain type of data or information to be requested from the non-OT network, unidirectional gateways (data diodes) should be employed. Those devices, in addition to firewalls and intrusion detection systems, can help mitigate inadvertent and malicious access attempts to access the OT systems from the non-OT networks and vice-versa.

- If remote access is required, practitioners often employ a commercial VPN that provides access control into the enterprise OT network. VPNs are only armored pipes into the enterprise, but they cannot ensure the endpoints provide security controls. Thus, VPNs must be configured with appropriate access controls. Multi-factor authentication is recommended, because physical tokens can be issued and controlled better than passwords alone. Finally, wherever possible, use of end-to-end encryption should be enforced.

It is important to emphasize that protection is not limited to an IT/OT function for connected devices. Physical security vulnerabilities can pose significant risks to an organization when devices that are sufficiently protected from remote access can readily be physically accessed on-site. Examples include distributed energy resources (e.g., EV charging stations, photovoltaic inverters, backup generators) that may be located outside the physical security boundary of a site and communicate with unencrypted protocols. Occupant information kiosks can also present vulnerabilities if not configured correctly. In fact, devices do not need to be connected to present cyber risk and warrant inclusion in a risk assessment. For example, hotel card key card readers have been hacked for monetary gain, despite not being externally connected (Greenberg n.d.).

The following protections should be enacted to reduce the threat of malicious physical access:

- Limit physical access to equipment to qualified and authorized personnel (e.g., example: need-to-know and least-privilege). This generally means locating equipment in locked mechanical rooms, with doors that close automatically and are regularly monitored. Further security can be provided by locking electrical and control panels. Special consideration must be taken to restrict physical access to equipment that is located on the roof or outside the building.
- Local human-machine interface displays (including thermostats, status panels, and annunciators) should require passwords to make any programming or configuration changes or be located in a secure environment.

An equally important element to protection is addressing human factors through training and development of a cybersecurity culture. One of the greatest security risks for any computer-controlled system, whether IT or OT, is having users be fooled into providing their credentials. This is most typically done with a social engineering form of attack called *phishing, spear phishing, Vishing, and Whaling*. Phishing attacks usually come as e-mails with malicious web links or attachments that look trustworthy. Simply clicking on the fake content may make it possible to compromise the system and give the threat actor a foothold in the organization. Spear phishing is a highly targeted form of phishing that exploits trust relationships and personal information. For this reason, personnel in charge of critical systems must take care what personal information they share on the internet and via social media. Highly personal details can be collected and used to gain the trust needed to get a specific person to make a security mistake. Even innocuous-seeming information like travel schedules and names of associates

can be used maliciously. For example, if a company vice president is known by the threat actors to be on foreign travel, they could contact the IT department, posing as this highly ranked person and insist on immediate remote access to internal systems. Attackers use plausible intimidation, schedule pressure, and knowledge of internal activities and points of contact to get defenders to give them unwarranted access.

Preventing these attacks can be done through both improved filtering of email, as well as through education of users to be more aware of potential risks and know what to avoid. Implementation of a user training and awareness program can make great strides toward protecting an organization. Testing users by attempting social engineering attacks can be a useful way to ensure proper training is occurring but care must be taken not to abuse users with excessive testing or imposing high costs for errors. Once users become aware of testing, especially if there are punitive results for failing a test, experience shows that user preparedness against actual attacks decreases. Overdoing internal phish-testing or applying punitive measures for failure can create the impression that management is a greater threat than external attackers producing negative morale effects that outweigh the potential cybersecurity gains.

The third step in the NIST CSF is “Detection.” It is important to know when a smart building control system has been compromised or when attempts have been made. However, OT systems and building operators do not typically have detection systems in place. While IT systems (like servers) have anti-virus and anti-malware software, availability of such solutions is very limited for supervisory and field controllers. Especially legacy systems may be unable to monitor their own security state at all. Such limitations exist for multiple reasons.

- In some cases, OT systems are custom designed for the customer, and typically, there may not have been enough penetration testing performed to discover vulnerabilities. OT systems traditionally were not networked until the recent spike in the affinity toward networked systems. In most of the IT systems, there are several tools that can be used to discover/detect vulnerabilities and address them. Existing IT security intelligence tools have limited applicability in the OT space because of issues such as architectural differences or protocol uniqueness. In addition, NIST maintains an open-to-all vulnerabilities database (NIST 2020), but it is evident that the IT systems vulnerabilities portion of the database is much more mature compared to the very limited discovered vulnerabilities of OT systems. Because OT networks are very operations-driven, it is extremely risky to perform aggressive penetration testing to identity/detect vulnerabilities. Such vulnerability testing may produce adverse physical effects such as setting off sprinklers that may damage the building. It may also completely disable OT devices making them permanently unusable.
- Typical anti-virus and anti-malware software are signature-based, with minimal level of pattern-based analytics. Because of this, there are limited OT systems signatures discovered to date, limiting the usability of those detection software systems.

These challenges should make it clear why it is crucial that all external or IT access to these systems must be mediated via a DMZ where effective detection and traffic analysis capabilities may be emplaced. These challenges also imply that the OT network operators should understand the fundamentals of the attack surface, threat landscape, possible malwares, and their potential impact on their network. Knowing the types of malware—such as virus, worm, ransomware, botnet, dropper, Trojan, rootkit, and spyware—their standard behavior, and common malware delivery mechanisms, can not only help with the design of effective OT discovery tools but also help the OT network operators to potentially detect anomalous behavior at early stages. In addition, network traffic logs are typically not analyzed to identify abnormal

volumes of data flow or unusual or inappropriate external destinations. In fact, operators often do not have a well-documented understanding of typical baseline network activity. Regular virus scanning and system log reviews are necessary in IT systems, but that detection software may not be as matured in regard to OT systems. However, it is always possible to monitor network traffic, especially between OT and non-OT systems. There will always be some traffic, but security analysts must be able to recognize when a communication pattern is aberrant. In general, there is a need for better intrusion detection systems for OT systems (Peacock and Johnstone 2014).

The fourth step is "Response." By far the largest deficiency here is the lack of a defined and practiced response plan. Creating a detailed, documented response plan and regularly enacting it through read-through tests, structured walk-through tests or table-top exercises, simulation tests, parallel tests, full-interruption tests,[5] or other review events is critical to ensuring clear roles and responsibilities. It is crucial for owners and operators to know when to escalate intrusion detections, which external stakeholders (such as law enforcement) to communicate with and when, and how to preserve information for forensic purposes. The response plan should dictate how threats are investigated, contained, and mitigated. This step also includes incorporating lessons learned into an updated response strategy and the voluntary sharing of information on threats and intrusions with external organizations (such as Real Estate Cyber Consortium [RECC] and Real Estate Information Sharing and Analysis Center [RE-ISAC]; see Section 4.2) to achieve improved situational awareness in the boarder community.

The fifth and final step is "Recovery." A recovery plan should include a system backup (securely stored on a separate server on a different network) to enable the recovery of critical data and restore OT equipment and associated systems back to operational capability. Another critical component is a communication and engagement plan to address any reputational and legal repercussions. This may include a communication plan to engage customers (e.g., tenants and occupants), as well as understand legal responsibilities if personal information was accessed. A solid recovery plan must be continuously tested and updated for evolving threats, vulnerabilities, and potential impacts of a cyber event. One of the effective means to perform a smooth recovery is to have a well-established business continuity plan (BCP), disaster recovery plan, and business impact analysis, which may also incorporate maximum allowable downtime of the building controls and processes. When a cyber event happens, the responsible parties should be expected to implement those plans following the organizational policies and standards. Here are some of the recommendations to achieve effective recovery processes:

- Perform risk analysis and use the information to perform a business impact analysis, which includes assessment of known vulnerability and impact.
- Periodically test the BCP and incorporate lessons learned.
- Ensure that the BCP encompasses the overall building-related processes and dependencies, steps related to the recovery of systems, and personnel backup.
- Have an updated list of prioritized critical process in order to recover systems in order of their criticality to business operations.
- Streamlined communication between the teams is important.

[5] Note that the listed tests/exercises are often used in the disaster recovery planning/practice processes. However, some or all of those similar tests may be developed for cyber event response processes.

- Based on the building's size and mission, perform cost-benefit analysis to select insurance options, cold, warm or hot backup site for operations and data, or mutual assistance agreements.
- Always have a point of contact and a lead to initiate the BCP and disaster recovery plan in case of a cyber event.

4.0 Summary of Relevant Resources and Initiatives

This section summarizes relevant cybersecurity resources and activities in the building domain, as well as adjacent fields across federal agencies, industry organizations, and vendor and IoT best practices.

4.1 Federal Agencies

National Institute for Standards and Technology

NIST has a number of foundational resources for cybersecurity, including the Cybersecurity Risk Management Framework (NIST 2018) that has been adopted by many organizations and approaches. NIST also published the *Security and Privacy Controls for Information Systems and Organizations* report (Joint Task Force 2020), which provides a comprehensive listing of controls for general information systems. Both documents are general, comprehensive, and require time and expertise adapting them to a particular domain. The domain application publications most applicable to smart building applications are NIST's *Guide to Industrial Control Systems (ICS) Security* (Stouffer et al. 2015) and *Cybersecurity Framework Manufacturing Profile* (Stouffer et al. 2017). NIST is also developing a project related to the cybersecurity of distributed energy resources (NCCoE n.d.). The authors of this report are not aware of any NIST resources specifically tailored for the security of building systems.
A summary of relevant NIST standards is provided in Appendix B.

Department of Homeland Security

One of DHS's roles is to promote and improve the cybersecurity of federal and private-sector computer systems and networks. Many programs and activities are implemented by DHS to mitigate cybersecurity risk and vulnerabilities on computer systems and networks that support federal operations and the nation's critical infrastructure. DHS coordinates and cooperates with partners within the department and other federal agencies, and with state and municipal administrations, first responders, private-sector companies in a wide range of industries, internet security researchers around the world, universities, and national laboratories. DHS is the lead agency for coordinating government and industry efforts for the reestablishment and provision of critical communications infrastructure, facilitates the stabilization of systems and applications from malicious cyber activity, and coordinates communications support to response efforts. Utilizing the National Response Framework, DHS supports and facilitates multi-agency planning and coordination for operations involving incidents requiring federal coordination, including information collection, analysis, and dissemination.

DHS cybersecurity coordinating functions include coordinating with telecommunications and information technology; reestablishment and provision of critical communications infrastructure; protection, reestablishment, and sustainment of cybersecurity and IT resources; oversight of federal response structures; and the stabilization of systems and applications from cyber incidents.

The Cybersecurity and Infrastructure Security Agency, which operates under DHS oversight, provides alerts and advisories of vulnerabilities for ICSs, including building automation systems (CISA n.d.). This is a key resource for identifying known vulnerabilities for building system equipment and associated mitigations (typically through patches).

Cyber Resilience Review: The Cyber Resilience Review (CRR) is a voluntary, non-technical assessment of an organization's operational resilience and cybersecurity best practices. The CRR relates closely to the Cybersecurity Framework (CSF) used by an organization to assess their relative capabilities. The CRR assessment maps to the NIST CSF, although the NIST CSF is based on a different underlying framework. When an organization uses the CRR for a self-assessment, some capabilities may fall short or exceed practices and capabilities in the CSF.

Cyber Security Evaluation Tool (NCCIC n.d.): The Cyber Security Evaluation Tool is a disciplined, systematic, and repeatable approach for evaluating an organization's cybersecurity posture. This software tool guides operators and asset owners using step-by-step instructions to evaluate their ICS and IT network security posture. The tool is aligned with many recognized government and industry standards and recommendations. A series of detailed questions about system components and architectures and operational policies and procedures generates a dashboard of charts showing areas of cybersecurity strength and weakness. The information gathered also provides a prioritized list of recommendations to increase the organization's cybersecurity posture.

Department of Defense

The DoD, through its *Unified Facilities Criteria (UFC): Cybersecurity of Facility-Related Control Systems* (DoD 2017) and *Unified Facilities Guide Specifications* (USACE 2017) describes the requirements for incorporating cybersecurity in the design of all facility-related control systems. While these documents are focused on the specification and design for new systems, the *Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DOD Installations* (OSD 2012) is a useful resource for best practices on assessing existing systems. DoD's Environmental Security Technology Certification Program also provides resources for the cybersecurity of facility-related control systems (SERDP and ESTCP n.d.). In 2020, DoD released the cybersecurity maturity model certification (OUSD A&S n.d.; OUSD A&S 2020) for DoD stakeholders and critical infrastructure facilities, in general.

Department of Energy

The bulk of DOE's work in cybersecurity is performed under the **CESER** office. CESER leads DOE's emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyberattacks, natural disasters, and man-made events. CESER divisions include the Infrastructure Security and Energy Restoration and Cybersecurity for Energy Delivery Systems (CEDS). CEDS (n.d.; Thomas et al. 2013; CESER n.d.) advances the research and development of innovative technologies, tools, and techniques to help reduce cybersecurity risks and threats to the nation's critical energy infrastructure. To ensure the success of grid modernization and transformation, the CEDS program includes ongoing support of research, development, and the demonstration of advanced cybersecurity solutions, the sharing of information, enhancement of situational awareness, technical assistance, and the development and adoption of best practices in the energy sector.

FEMP is part of EERE and advances the development and deployment of tools for assessing the cybersecurity vulnerabilities in federal buildings. FEMP has developed a factsheet for the cybersecurity of facility systems (EERE 2017). Additional examples include the Facilities Cybersecurity Capability Maturity Model (F-C2M2) tool that provides a methodology to self-assess and improve cybersecurity capabilities for building IT and OT systems. It includes a toolkit that can be deployed in a single day or scaled to a more comprehensive evaluation effort.

F-C2M2 helps organizations express their capabilities through four maturity indicator levels across 10 domains of cybersecurity practice.

FEMP has also funded development of the Facility Cybersecurity Framework (FCF) to provide easy to follow general guidance, drawn from the NIST CSF and a wide variety of industry best practices and guidance documents (i.e., NIST 800 series and DoD United Facilities Criteria). The FCF facilitates implementation of the May 2017 Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which calls on federal agencies and critical infrastructure owners and operators to manage their cyber risk through adoption of the NIST-developed *Framework for Improving Critical Infrastructure Cybersecurity* (EO 13636; EO 13800).

The FCF Primer provides a voluntary, risk-based set of industry standards and best practices to help facility owners and operators better manage cybersecurity risks. FCF provides a common taxonomy and mechanism for facility stakeholders to describe their current cybersecurity posture, describe their target state for cybersecurity, identify and prioritize opportunities for improvement within the context of a continuous and repeatable process, assess progress toward the target state, and communicate among internal and external stakeholders about cybersecurity risk.

In addition, FEMP's cybersecurity tool development investments resulted in the FCF-RMF (Risk Management Framework) Hybrid tool. RMF is largely used in DoD-related facilities, and because of EOs 13800 and 13686, it is non-trivial for the federal facilities to perform two independent assessments. Through the FCF-RMF hybrid tool, the facilities can perform a standard RMF assessment and learn about their compliance with the FCF. Other cybersecurity resources developed under FEMP are the cybersecurity training game, network enumeration, and discovery tools. All of the FEMP tools are open to everyone to use. More details about FEMP's cybersecurity tools are discussed in Appendix D.

BTO has funded several projects and initiatives related to cybersecurity. These include the development and publication of a lighting cybersecurity factsheet (EERE 2018) and the evaluation of cybersecurity maturity of connected lighting systems (Poplawski, 2020). BTO funded the Cybersecurity Roundtable, held in May 2019, which convened 21 organizations identified as early adopters of smart building technologies from the commercial real estate, higher education, hospitality, grocery, utility, and government sectors, as well as representatives from industry associations. This workshop sought to understand 1) the range of building cybersecurity risks and possible mitigation strategies, 2) current cybersecurity management practices in the commercial sector, and 3) insights to inform publicly funded building technology research that takes into account cybersecurity risks and current practices/constraints within the commercial building sector. In addition, BTO is funding research into the cybersecurity of adaptive building controls through Buildings Energy Efficiency Frontiers & Innovation Technologies funding awards.

A summary of pertinent DOE-funded tools and research is provided in Appendix D.

4.2 Industry Organizations

This section profiles the various industry groups and companies undertaking initiatives relevant to building cybersecurity.

The **Real Estate Cyber Consortium (RECC)** mission is to "elevate awareness across the real estate community in order to improve cyber security preparedness for buildings and facilities." RECC members include operators of large commercial building portfolios such as CBRE, Oxford Properties, Wells Fargo, Oracle, and ExxonMobil. Collectively, the RECC has developed best practices for OT security, self-assessments, vendor sourcing, and contract language. The RECC is tightly aligned with the RealComm Conference Group, who is a leader in highlighting the need and current best practices for cybersecurity in the commercial real-estate domain. RealComm hosts webinars and an annual cybersecurity forum where operator best practices and vendor solutions are profiled. In addition, CBRE has hosted building technology cybersecurity roundtable events.

The Building Owners and Managers Association International has developed cybersecurity guidance for practitioners including self-assessment checklists as a function of an organization's or site's risk level (BOMA International n.d.).

The Continental Automated Building Association (CABA) has funded research activities in the field of cybersecurity for intelligent buildings, including industry surveys to assess cybersecurity trends, risks, and market trends (King 2016). Of more practical relevance to commercial building practitioners is the CABA whitepaper *Cybersecurity in Smart Buildings: Preventing Vulnerability while Increasing Connectivity* (Dribble, Imhof, and Drafz 2015). A recent CABA whitepaper has also identified that there is no "*recognized international IoT cybersecurity standard to which IoT device manufacturers can conform"* (Khan and Rogers 2019). This whitepaper also reviews and contrasts leading potential IoT cybersecurity standards such as NIST, the International Organization for Standardization (ISO), the International Society of Automation (ISA), and the CSA Group (formerly the Canadian Standards Association).

The American Society of Heating, Refrigeration, and Air-conditioning Engineers (ASHRAE) has several notable efforts related to both developing resources as well as educating practitioners. ASHRAE's primary activity in this area is the development of BACnet Secure Connect, an updated version of the Building Automation and Control Network (BACnet) communication protocol that achieves increased security through implementing established IT best practices. In addition, ASHRAE's Technical Committee 1.5 cybersecurity subcommittee (ASHRAE n.d.) coordinates efforts in this area. Finally, ASHRAE promotes increased understanding of smart building cybersecurity issues through seminars and ASHRAE journal articles (for example in the July 2019 issue; McGowan 2019).

SANS is a private organization with a board of subject matter experts from private and government organization. Over the years, SANS has produced very efficient and detailed cyberattack forensics and analysis white papers that are related to both IT and OT systems. In addition, SANS has periodic OT/ICS training programs for the practitioners and decision-makers to understand and develop a security-in-the-loop operations implementation path for their building. SANS has active forums of security practitioners and live feed on security updates related to the OT/ICS systems.

The Real Estate Information Sharing and Analysis Center Group (RE-ISAC; RE-ISAC n.d.) "*is a public-private information sharing partnership between the U.S. commercial facilities sector and federal homeland security officials organized and managed by The Real Estate Roundtable.*"

The National Electrical Manufacturers Association, in collaboration with ISA and DoD advisors, plans to roll-out a building system cybersecurity certification program (Anderson

2019). Its goal is to "*create easy-to-understand tiers for end users to apply industry-accepted Standards to products, processes, and technology to allow end users to market cyber protections and consumers to understand the level of security present.*"

The **Institute of Electrical and Electronics Engineers (IEEE)** has created several cybersecurity standards that are applicable to building systems:

- *An Adaptive Control Architecture for Mitigating Sensor and Actuator Attacks in Cyber-Physical Systems* (Yucelen et al. 2016)
- *IoT Security Framework for Smart Cyber Infrastructures* (Pacheko and Hariri 2016)
- *Forensic Readiness of Smart Buildings: Preconditions for Subsequent Cybersecurity Tests* (Bajramovic et al. 2016)
- *Cybersecurity and Privacy Solutions in Smart Cities* (Khatoun and Zeadally 2017).

The Thread Group, inc., started in 2014, is an alliance that includes Google, Arm Holdings, Haiku Home, NXP, Samsung Electronics, Silicon Labs, and Yale Security and has over 230 member organizations. Together, they developed "Thread," a low-power mesh networking technology for residential IoT products. The protocol is available at no cost but requires membership in the Thread Group (2015). This network technology is specifically designed to be secure and interoperable and is intended to support a variety of IoT products.

Underwriters Laboratory (UL) offers services for product testing, primarily for electrical safety. They are in the process of developing their 2900 series of test and certification standards for cyber-testing of products called the "Cyber Assurance Program" (UL 2017). The new program will be applied to building controls, fire alarms, and security systems and is being rolled out in phases.

Other Industry Resources: Participants at the BTO Cybersecurity Roundtable also identified other resources relevant to the building space. Both the first and second editions of *Navigating the Digital Age*, published by Palo Alto Networks and NYSE, contain essays from leading cybersecurity practitioners and relate to the organizational, technical, and process best practices and lessons learned in addressing cybersecurity in enterprises (Palo Alto Networks, Inc. 2018). In addition, both Google (n.d.) and Microsoft (Hunt, Letey, and Nightingale 2017) have published security best practices for IoT devices.

5.0 Deployment Challenges and Barriers

The challenges associated with the broad deployment of resources, training, tools, and testing capability to address the vulnerabilities and best practices detailed in Section 3.0 have similarities to the challenges in deploying other building technologies. Many of these challenges have been summarized by the *DOE Cybersecurity Roundtable Report* (Crowe et al. 2019).

Cybersecurity Value Proposition is Hard to Quantify

There is a well-established return on investment for networking, digitizing, and automating smart building technology, from reduction in greenhouse gas emissions, to cost saving and comfort from improved energy management. However, it can be difficult in cybersecurity—like other forms of risk management—to identify a clear return on investment, especially in a new area like OT cybersecurity, where the threats are rapidly evolving. Cybersecurity can reduce interoperability, functionality, ease of use, and increase costs. Furthermore, increased cyber investment may stop hundreds of thousands of attacks daily, but it does not guarantee protection from all threats. Finally, unlike the bulk power grid that has North American Electric Reliability Corporation Critical Infrastructure Protection cybersecurity requirements, there are very few external incentives or regulatory requirements for deploying cybersecurity for commercial building operators.

Within the federal government, where a clear cybersecurity mandate exists, the focus has been on securing facility-related control systems. Agencies, including the General Services Administration, DoD, DOE, and DHS, are working to complete assessments and move to improve security for these systems. But progress has been slower in other sectors of the built environment. For example, many commercial owners have a lower awareness of cyberattacks on building systems and may not perceive this as a large risk. Diligent owners are establishing connections between IT and facility operations that follow best practices. Demand for more secure products and solutions is starting to emerge from entities such as RECC. This is most prominent among the owners and operators of large building portfolios who typically have the experience and resources to assess and manage building OT cybersecurity, often pulling from IT and other corporate risk management best practices. However, better education and awareness are needed to get the vast majority of owners and operators to understand the needs in this area and determine the appropriate level of investment. In particular, there is a need to support operators of small commercial buildings to assess risk and the value in implementing training and best practices.

Cybersecurity Must Address a Variety of Requirements

One important characteristic of connected buildings that is particular to the breadth of the 5.6 million buildings across the nation is that the equipment and devices span the range of complexity and cost, just as the building users and tenants range in degrees of sophistication, criticality, and income. For example, an acute-care inpatient hospital is very different from a neighborhood restaurant in its risk profile and tolerance. Thus, as buildings and physical infrastructure are increasing their connectivity and the potential points by which attacks to the cyber-physical architecture are likely to occur, we need to understand the appropriateness of cybersecurity to these buildings and facilities and the related impacts to the owners, tenants, and users of the buildings, including both the risks and the costs of “appropriate” cybersecurity measures.

There is no “one-size-fits-all” cybersecurity solution for buildings. The cybersecurity requirements vary from building to building and system to system, as well as from owner to occupant to tenant. For example, temperatures in larger buildings change relatively slowly, so a building’s HVAC system could hypothetically be offline for a period of time without significant impact to the building occupants and tenants (depending on the function of the building). Therefore, the availability requirements for the HVAC system may be moderate. On the other hand, if critical temperature and humidity requirements exist for buildings, such as for hospitals, their HVAC cybersecurity risk profile and requirements are substantially higher.

Legacy Systems

Building control systems are often used for 10 to 20 years before they are updated or replaced. This is much longer than the lifespan for most IT systems and IoT devices. Control systems utilize embedded hardware and have a very limited amount of processing and storage capacity. Furthermore, older systems may not be able to be updated to operate using new standards for secure communications without the expense of a hardware update. Servers and desktop computers used for automation systems may be managed by the facilities group and not by IT and, as a result, they may not be getting properly scanned, patched, and updated as new vulnerabilities are discovered. This presents a unique set of challenges for ensuring the security of such systems. While building OT systems share similarities with ICSs and are benefiting from adapting traditional IT security practices, it is important to remember that building systems have distinct needs requiring customized solutions.

Workforce and End-User Education and Training

The building operators must be aware of risks and be properly trained to ensure existing systems are secure against cyberattack. Building system designers, commercial control contractors, and facility managers often have limited knowledge of how to protect against cyberattacks. However, in many commercial and government organizations, cooperation between IT and facility management groups is slowly emerging. IT groups are often well aware of cyber risks and have experience in applying best practices. As building owners obtain greater knowledge about cybersecurity threats and best practices, these will be increasingly specified during procurement for new systems. Awareness and appreciation of security aspects for the stakeholders and participants in the building-operations-related value chain will strengthen the pull for secure products, lower the inertia to technology transformation, and drive wide adoption.

System users must also be trained in basic cybersecurity hygiene, including being made aware of potential dangers, such as spear phishing e-mails, malware spread vectors, and the risks of infected media (such as USB drives), all of which can introduce malware into a system. This need is particularly apparent for users of IoT devices, which are often installed and configured by homeowners or small building operators with little cybersecurity education. The resulting poor password hygiene and lack of two-factor authentication has resulted in IoT devices (such as security cameras) being compromised.

Validation

No system is secured until it is tested. For federal operators, system testing may include adherence to checklists like those mandated by the Federal Information Security Management Act and active penetration testing by red teams. Building cybersecurity commissioning and testing capability is needed for commercial sites with sufficiently high-risk profiles. However, care is needed when performing cybersecurity testing, particularly scanning of legacy OT

systems. Penetration testing should be done by an independent organization and only under highly controlled conditions. OT systems are notoriously sensitive and often cannot withstand normal cybersecurity testing. Red teams may unintentionally permanently damage the OT systems they test unless they know what they are doing.

Control systems consist of both standard IT equipment, such as servers, workstations, laptops, and tablets, and numerous controllers, which are typically embedded systems with real-time operating systems or application-specific integrated circuits. Verifying that there is no issue with malicious code introduced in manufacturing and installation of the IT devices is very difficult without employing trusted suppliers. Verifying that there are no issues with embedded devices is nearly impossible. The supplier must be trusted, and verification testing should be conducted in a cyber lab or testing range. UL is in the process of developing independent, third-party cyber-testing, which may become a good option in the near future. Trusted suppliers must be open to periodic inspection and independent third-party verification. There is no guarantee that supply chain compromises have not occurred, and continually vigilant monitoring of systems is the best defense.

Since most IoT products are relatively new to the market, they may be designed to accommodate some level of cyber protection. However, there are few standards in place for these products and little way for consumers to know if a product is properly protected or not. The development and dissemination of clear best practices (or better standards) would help the industry to continue to grow and assure a certain level of cyber protection. One option is the work started by UL on the Cyber Assurance Program. Requiring compliance and testing could be a baseline for selling network-connected devices.

6.0 Conclusions

Sophisticated monitoring and control systems in a smart building can deliver significant value. First and foremost, they can operate the building more efficiently and keep occupants safer and more comfortable. Current systems have naturally evolved from simple pneumatic, mechanical, and electrical controls, replacing “siloed” controls with integrated data acquisition and analysis systems that feed operational data back into the control system. These technologies are a core element in continuing to advance energy efficiency in buildings and providing future grid interactive services. However, these systems are vulnerable to cyberattacks and are increasingly being targeted. As discussed in Section 2.0, typically half of commercial buildings have devices exposed to the internet, and 95 percent of sites do not have a disaster recovery plan. Recent investigations suggest that nearly 40 percent of building management system servers have been targeted with malware, phishing scams, or ransomware. Even without malicious attacks, the increasing complexity of smart building integrations increases the likelihood of disruptions and system failures due to faulty patches, user errors, and poor maintenance. If not effectively addressed, these threats could significantly slow the deployment of high-value connected technologies and future energy efficiency gains.

Therefore, cybersecurity and resiliency can no longer afford to be an afterthought or a “band aid” in response to attacks and operational issues. A comprehensive approach is needed to enhance the cybersecurity of commercial and government buildings that also takes into account their great diversity in terms of systems, size, criticality, complexity, function, and financial and personnel resources. The goal is to strike the right balance between building security and functionality, reliability and resilience, opportunity, and cost. That is, the approach to security must cost-effectively support critical building functionality, such as energy optimization and data analytics, while ensuring critical OT/IT components are secured from threats.

Cybersecurity must be part of the core building design and operational criteria and should be conceived as a foundational platform that minimizes risks to its users and IT systems. Securing these smart systems and providing cybersecurity for buildings is not an end state, nor is it solely a technology solution, but rather a process of fostering a culture of cybersecurity awareness and holistic cybersecurity. Effort in three areas will provide considerable value to this cause:

1. Curation and development of tailored cybersecurity resources and tools for the building community.
2. Continued education and engagement of the building community to establish clear expectations, roles, and responsibilities.
3. The continued research and development in tools and technologies to increase cybersecurity, particularly when it comes to the detection and response to attacks.

The building community needs tailored cybersecurity resources suitable for their systems and workforce that are distinct from the foundational (but often generic and dense) NIST and ICS resources. Fortunately, many resources exist for the building sector, including industry best practices and federal specifications and assessment tools (see Section 4.0). Considerable value would be obtained by curating these tools and resources into a centralized cybersecurity “toolkit.” This would aid in enabling commercial operators to understand and leverage government tools and learnings. Also, given the diversity of buildings in the marketplace (e.g., function, size, and degree of automation), various “appropriate” levels of cybersecurity risk management need to be defined so that building owners and operators can specify and deploy the necessary mitigations based on their maturity level and risk level. Finally, while many

resources and tools exist, these are heavily weighted toward the identify and protect domains of the CSF. More comprehensive best practices and resources are needed in the area of detecting an attack in building systems and responding to and recovering from such an attack.

Continued engagement and education are required with all stakeholders throughout the lifecycle of connected building systems, including the development, acquisition, implementation, operation, maintenance, and decommissioning of building control systems. Clearer responsibility for cybersecurity will need to be allocated over the fragmented delivery chain (original equipment manufacturers, system integrators, commissioning agents, maintainers and operators). Developed resources can be used to ensure operators understand risks and can prioritize vulnerabilities and cybersecurity needs. Stakeholders also need to understand appropriate cybersecurity best practices and how best to specify them, ensure they are implemented and commissioned correctly, and maintain them. This will require continued collaboration between building OT and IT stakeholders. As buildings become increasingly networked and, thus, exposed to cyber threats, additional qualifications will likely be desired by building operations and IT managers, integrators, and service providers to protect buildings and building assets. Given that cyber threats and countermeasures are rapidly evolving, this engagement and education will need to be ongoing and agile. The ultimate goal is to foster a culture of cybersecurity among commercial building stakeholders.

There is also a continued need for additional tools and technology to ensure cybersecurity is delivered and maintained in an efficient, comprehensive, and cost-effective manner. FEMP has funded assessment tools such as the FCF and work is underway on tools that support the automated identification of devices exposed to the internet (such as Mitigation of Exposure of Energy Delivery Systems [MEEDS]) and inventory system devices. However, substantially less capability exists to enable the detection of intrusion within building systems and technology to appropriately respond and recover from such events. The complexity of converging cyber and physical systems exacerbates the challenge of identifying whether building system anomalies and failures are the result of human error, malicious cyber or physical attacks, computational errors, or a combination of these failure points. Such areas present the opportunity for natural extensions of building technology initiatives in the area of fault detection and diagnostics (i.e., detecting, determining, and dispositioning anomalous behavior in a way that elicits both trust and appropriate action from building operators) and advanced adaptive and robust control (i.e., ensuring that control systems are resilient to disturbances and ensure safe and acceptable operation during extreme events). Appropriate data sets and metrics are needed by developers and building operators to evaluate the adequacy and performance of technologies and systems. Such tools need to be developed in the context of increasing the overall value proposition and ensuring that costs associated with “appropriate” levels of protection are minimized. These capabilities would need to cover a continuum of users, processes, and existing technologies and readily adapt to the rapidly changing cybersecurity threats.

7.0 References

Anderson, Kirk. 2019. “NEMA, ISA Announce New Building Systems Cybersecurity Program.” *Electroindustry* 24(4):19. https://www.nema.org/news/EI%20PDF/EI_JulAug19.pdf.

Antonakakis, Manos, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, et al. 2017. “Understanding the Mirai Botnet.” In *Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, August 16–18, 2017*, 1093–1110. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf.

ASHRAE. n.d. “Computer Ap[plications: ASHRAE Technical Committee 1.5.” American Society of Heating and Air-Conditioning Engineers. Accessed November 2019. https://tc0105.ashraetcs.org/functions.php.

BACnet International. January 23, 2018. “Research Study Indicates Global Market Share.” Accessed March 2020. https://www.bacnetinternational.org/page/BACnetStandard

Bain & Company. June 13, 2018. “Cybersecurity Is the Key to Unlocking Demand in the Internet of Things.” https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things.

Bajramovic, Edita, Karl Waedt, Antonio Ciriello, and Deeksha Gupta. 2016. "Forensic Readiness of Smart Buildings: Preconditions for Subsequent Cybersecurity Tests." In *2016 IEEE International Smart Cities Conference (ISC2), Trento, Italy, September 12–15, 2016*, 1–6. https://doi.org/10.1109/ISC2.2016.7580754.

BOMA International. n.d. “Cybersecurity.” Building Owners and Managers Association International. Accessed November 2019. https://www.boma.org/BOMA/Research-Resources/Trends/Cybersecurity.aspx.

Brooks, David J, Michael Coole, and Paul Haskell-Dowland. “Intelligent Building Systems: Security and Facility Professionals’ Understanding of System Threats, Vulnerabilities and Mitigation Practice.” *Security Journal*. https://doi.org/10.1057/s41284-019-00183-9.

CESER. n.d. “Game-Changing RD&D to Develop Resilient Energy Systems.” *Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems*. U.S. Department of Energy, Office of Cybersecurity, Energy, Security, and Emergency Response. Accessed February 2020. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and.

Cherepanov, Anton. 2017. *WIN32/INDUSTROYER: A New Threat for Industrial Control Systems*. ESET. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

CISA. n.d. “Industrial Control Systems.” U.S. Department of Homeland Security, Cyber Infrastructure Security Agency. Accessed November 2019. https://www.us-cert.gov/ics.

Crowe, Eliot, Claire Curtin, Hannah Kramer, Jessica Granderson, Cindy Zhu, Hayden Reeve, and Glenn Fink. 2019. *Summary of Outcomes of the 2019 Cybersecurity Roundtable*. U.S. Department of Energy.

https://buildings.lbl.gov/sites/default/files/Cyber%20Roundtable%20Summary%20Report%202019%2011%2019%20%282%29.pdf.

DoD. 2017. *Unified Facilities Criteria (UFC): Cybersecurity of Facility-Related Control Systems*. U.S. Department of Defense, UFC-4-010-06, Change 1. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06.

Dribble, Pramod E.F., Raphael Imhof, and Udo Drafz. 2015. *Cybersecurity in Smart Buildings: Preventing Vulnerability While Increasing Connectivity*. Continental Automated Buildings Association Intelligent & Integrated Buildings Council (IIBC). https://www.caba.org/CABA/DocumentLibrary/Public/CybersecuritySmartBuildings.aspx.

EERE. 2018. *Cyber Security for Lighting Systems*. Department of Energy, Office of Energy Efficiency & Renewable Energy. https://www.energy.gov/sites/prod/files/2018/06/f52/cyber_security_lighting.pdf.

EERE. 2017. *Cyber-Securing Facility Related Control Systems*. U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. https://www.energy.gov/sites/prod/files/2018/01/f46/cyber_securing_facilities.pdf.

EERE. 2016. *Building Technologies Office Multi-Year Program Plan Fiscal Years 2016-2020*. Department of Energy, Office of Energy Efficiency and Renewable Energy. http://energy.gov/eere/buildings/downloads/multi-year-program-plan.

EERE. 2014. *Building Energy Codes: ANSI/ASHRAE/IES Standard 90.1-2013 Power and Lighting*. U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. https://www.energycodes.gov/sites/default/files/becu/90.1-2013_Lighting_BECU.ppt.

EERE. n.d. "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)." U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. Accessed July 5, 2016. http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.

EIA. 2016. "2012 Commercial Buildings Energy Consumption Survey: Energy Usage Summary," U.S. Energy Information Administration. https://www.eia.gov/consumption/commercial/reports/2012/energyusage/.

EIA. 2012a. "Commercial Buildings Energy Consumption Survey (CBECS)." U.S. Energy Information Administration. https://www.eia.gov/consumption/commercial/.

EIA. 2012b. "Table B40, Cooling Equipment, Number of Buildings, 2012." *Commercial Buildings Energy Consumption Survey (CBECS)*. https://www.eia.gov/consumption/commercial/data/2012/bc/cfm/b40.php.

Federal Facilities Council. 2015. "Cybersecurity Building Control Systems." The National Academies of Sciences, Engineering, and Medicine, Federal Facilities Council. http://sites.nationalacademies.org/DEPS/FFC/DEPS_160507.

Fruhlinger, Josh. March 9, 2018. "The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet."

https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

GAO. 2014. *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*. United States Government Accountability Office. www.gao.gov/assets/670/667512.pdf.

Google. n.d. "Application Security Requirements for IoT Devices." Accessed November 2019. https://partner-security.withgoogle.com/docs/iot_requirements.

Gordy, Fred. April 2019. "The State of BAS Cybersecurity." AutomatedBuildings.com. http://automatedbuildings.com/news/apr19/articles/ib/190318022808ib.html.

Greenberg, Andy. n.d. "The Hotel Room Hacker." *Wired*. Accessed November 2019. https://www.wired.com/2017/08/the-hotel-hacker/.

Griffor, Edward R, Christopher Greer, David A. Wollman, and Martin J. Burns. 2017. *Framework for Cyber-Physical Systems: Volume 1, Overview*. U.S. Department of Commerce, National Institute of Standards and Technology, Cyber-Physical Systems Program Office Engineering Laboratory, NIST Special Publication 1500-201, Version 1.0. https://doi.org/10.6028/NIST.SP.1500-201.

Hardin, DB, CD Corbin, EG Stephan, SE Widergren, and W Wang. 2015. *Buildings Interoperability Landscape*. Richland: Pacific Northwest National Laboratory, PNNL-25124. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-25124.pdf.

HP. July 29, 2014. "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack." http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.V41Wm01f3X6.

Huergo, Jennifer. April 16, 2018. "NIST Releases Version 1.1 of its Popular Cybersecurity Framework." U.S. Department of Commerce, National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

Hunt, Galen, George Letey, and Edmund B. Nightingale. 2017. *Seven Properties of Highly Secure Devices*. Microsoft Research NExT Operating Systems Technologies Group. https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf.

Ionesco, Paul. February 3, 2016. "Is Your Smart Office Creating Backdoors for Hackers?" Security Intelligence. Accessed April 30, 2016. https://securityintelligence.com/is-your-smart-office-creating-backdoors-for-cybercriminals/.

ISA. 2009. Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. International Society of Automation, ISA–62443-2-1–2009. https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731.

Joint Task Force. 2020. *Security and Privacy Controls for Information Systems and Organizations*. U.S. Department of Commerce, National Institute of Standards and Technology,

Information Technology Laboratory, NIST Special Publication 800-53, Rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft.

Khan, Faud, and David Rogers. 2019. *IoT Cybersecurity Guidelines, Standards and Verification Systems*. Continental Automated Buildings Association. https://www.researchgate.net/publication/334947831_IoT_cybersecurity_guidelines_standards_and_verification_systems_A_CABA_WHITE_PAPER.

Khatoun, Rida, and Sherali Zeadally. 2017. "Cybersecurity and Privacy Solutions in Smart Cities." *IEEE Communications Magazine* 55(3):51–59. https://doi.org/10.1109/MCOM.2017.1600297CM.

King, Rawison O'Neil. 2016. "Cyber Security for Intelligent Buildings." *Engineering & Technology Reference*. https://doi.org/10.1049/etr.2015.0115.

Kumar, Deepak, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dimitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. 2019. "All Things Considered: An Analysis of IoT Devices on Home Networks." In *Proceedings of the 28th Usenix Security Symposium, Santa Clara, California, August 14–16, 2019*, 1169–1185. https://zakird.com/papers/state_of_iot.pdf.

Lee, Robert M., Michael J. Assante, and Tim Conway. 2016. *Analysis of the Cyber Attack on the Ukranian Power Grid*. Electricity Information Sharing and Analysis Center. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Mahan, RE, JR Burnette, JD Fluckiger, CA Goranson, SL Clements, H Kirkham, and C Tews. 2011. Richland: Pacific Northwest National Laboratory. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf.

McGowan, Mary Kate. 2019. "Building Automation Systems: Addressing the Cybersecurity Threat." *ASHRAE Journal* 61(7):28–36. http://www.nxtbook.com/nxtbooks/ashrae/ashraejournal_201907/index.php#/30.

Memoori. September 24, 2019. "37.8% of Smart Building Automation Systems Were Attacked in H1 2019, Kaspersky Reports." https://memoori.com/37-8-of-smart-building-automation-systems-were-attacked-in-h1-2019-kaspersky-reports/.

Minoli, Daniel, Kazem Sohraby, and Benedict Occhiogrooso. 2017. "IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems." *IEEE Internet of Things Journal* 4(1):269–283. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7805265.

Mylrea, Michael. 2014. "Cyber Security and Optimization in Smart Autonomous Buildings." *AAI Symposium.* Palo Alto: Stanford University.

NCCIC. 2015. "Incident Response Activity." *ICS-CERT Monitor*. Department of Homeland Security, National Cybersecurity and Communications Integration Center. Accessed July 25, 2016. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

NCCIC. n.d. *NCCIC ICS Cyber Security Evaluation Tool*. Department of Homeland Security, National Cybersecurity and Communications Integration Center. Accessed November 2019.

https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf.

NCCoE. n.d. “Securing the Industrial Internet of Things.” U.S. Department of Commerce, National Institute of Standards and Technology, National Cybersecurity Center of Excellence. Accessed November 2019. https://www.nccoe.nist.gov/projects/use-cases/energy-sector/iiot.

NEII. 2016. “How Occupant Evacuation Operation Works.” *The Insider*. National Elevator Industry, Inc. http://www.neii.org/insider/editions/20160712.pdf.

NIST. 2020. “National Vulnerability Database.” U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory. Last modified March 22, 2020. https://nvd.nist.gov/.

NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity*. U.S. Department of Commerce, National Institute of Standards and Technology, Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018.

NIST. 2014a. “Cybersecurity Framework.” U.S. Department of Commerce, National Institute of Standards and Technology. Accessed July 10, 2016. http://www.nist.gov/cyberframework/index.cfm.

NIST. 2014b. “Framework for Improving Critical Infrastructure Cybersecurity.” U.S. Department of Commerce, National Institute of Standards and Technology. Version 1.0. Accessed July 10, 2016. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST. 2010. *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. U.S. Department of Commerce, National Institute of Standards and Technology, Smart Grid Interoperability Panel Cyber Security Working Group. https://www.nist.gov/system/files/documents/smartgrid/nistir-7628_total.pdf.

O’Harrow, Robert. June 3, 2012. “Cyber Search Engine Shodan Exposes Industrial Control Systems to New Risks.” *The Washington Post*. Accessed July 25, 2016. https://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html.

Obama Administration. 2015. *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure.* White House, 2–37. https://www.hsdl.org/?view&did=764791

OSD. 2012. Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DOD Installations. U.S. Department of Defense, Office of the Secretary of Defense. http://www.wbdg.org/files/pdfs/ics_handbook.pdf.

OUSD A&S. 2020. *Cybersecurity Maturity Model Certification (CMMC): CMMC Model v.1.0*. Office of the Under Secretary of Defense for Acquisition & Sustainment. https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf.

OUSD A&S. n.d. “CMMC Model.” Office of the Under Secretary of Defense for Acquisition & Sustainment. Accessed November 2019. https://www.acq.osd.mil/cmmc/draft.html.

Pacheko, Jesus, and Salim A. Hariri. 2016. "IoT Security Framework for Smart Cyber Infrastructures." In *Proceedings of IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 2016, Augsburg, Germany, September 12–16, 2016*, 242–247. https://doi.org/10.1109/FAS-W.2016.58.

Palo Alto Networks, Inc. 2018. Navigating the Digital Age: The Definitive Cybersecurity Guide. 2nd ed. Palo Alto: Palo Alto Networks, Inc. https://www.securityroundtable.org/navigating-the-digital-age-2nd-edition/.

Peacock, Matthew, and Michael N. Johnstone. *An Analysis of Security Issues in Building Automation Systems*. Edith Cowan University. https://doi.org/10.4225/75/57b691dfd9386.

Plageras, Andreas, Kostas E. Psannis, Christos Stergiou, Haoxiang Wang, and B.B. Gupta. 2018. "Efficient IoT-Based Sensor BIG Data Collection—Processing and Analysis in Smart Buildings." *Future Generation Computer Systems* 82:349–357. https://doi.org/10.1016/j.future.2017.09.082.

Poplawski, Michael, St. Lawrence, Adam, and Ngo, Hung. 2020. "An Authentication Vulnerability Assessment of Connected Lighting" Prepared by Pacific Northwest National Laboratory for U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy, PNNL-28782. https://www.energy.gov/sites/prod/files/2020/04/f73/ssl-cls-authentication-vulnerability-mar2020.pdf

PNNL. 2020. "FEDS: Facility Energy Decision System." Last modified March 2020. http://www.pnl.gov/feds/.

Radvanovsky, Bob. September 19, 2013. "Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting." Tofino Security Blog. Accessed April 30, 2016. https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting.

Ranathunga, Dinesha, Matthew Roughan, Hung Nguyen, Phil Kemick, and Nickolas Falkner. 2016. "Case Studies of SCADA Firewall Configurations and the Implications for Best Practices." *IEEE Transactions on Network and Service Management* 13 (4): 871-884.

RE-ISAC. n.d. Home Page. Accessed November 2019. https://www.reisac.org/.

Romano, Kelly, Mead Rusert, and Hayden Reeve. 2015. *Integrated and Intelligent Buildings: An Imperative to People, the Planet, and the Bottom Line*. http://global.ctbuh.org/resources/papers/download/2404-integrated-and-intelligent-buildings-an-imperative-to-people-the-planet-and-the-bottom-line.pdf.

Rubinstein, Francis, Stephen Treado, and Peter Pettler. 2003. "Standardizing Communication Between Lighting Control Devices: A Role for IEEE P1451." In *38th IAS Annual Meeting on Conference Record of the Industry Applications Conference, Salt Lake City, UT, October 12–16, 2003*, 805–811, Vol. 2. https://doi.org/10.1109/IAS.2003.1257619.

SERDP and ESTCP. n.d. "Cybersecurity Facility-Related Control Systems (FRCS)." Strategic Environmental Research and Development Program, and Environmental Security Technology Certification Program. Accessed November 2019. https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity.

Snyder, Loren. 2015. "Why Building Management Systems Are at Risk of Cyberattack." FacilitiesNet. http://www.facilitiesnet.com/buildingautomation/article/Why-Building-Management-Systems-Are-At-Risk-Of-Cyberattack-Facilities-Management-Building-Automation-Feature--15558#.

Stouffer, Keith, Timothy Zimmerman, CheeYee Tang, Joshua Lubell, Jeffrey Cichonski, and John McCarthy. 2017. *Cybersecurity Framework Manufacturing Profile*. U.S. Department of Commerce, National Institute of Standards and Technology, NISTIR.8183. https://doi.org/10.6028/NIST.IR.8183.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 2015. *Guide to Industrial Control Systems (ICS) Security*. U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory, NIST Special Publication 800-82, Rev. 2. http://dx.doi.org/10.6028/NIST.SP.800-82r2.

Thomas, Russell Cameron, Marcin Antkiewicz, Patrick Florer, Suzanne Widup, and Matthew Woodyard. 2013. "How bad is it? – A Branching Activity Model to Estimate the Impact of Information Security Breaches." Paper accepted by *12th Workshop on the Economics of Information Security, v. 2.0., Georgetown University, Washington, D.C., June 11–13, 2013.*

Thread Group, Inc. 2015. *Thread Commissioning*. https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=658.

Tuenge, Jason, and Michael Poplawski. 2017. *PoE Lighting System Energy Reporting Study Part 1*. Prepared by Pacific Northwest National Laboratory for U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. https://www.energy.gov/sites/prod/files/2017/04/f34/2017-02%20ssl-poe_part1_0r.pdf.

UL. 2017. *UL Global Cybersecurity Services and Standards*. Underwriters Laboratory. https://industries.ul.com/wp-content/uploads/sites/2/2017/04/UL_CAP_Overview.pdf.

USACE. 2017. *Unified Facilities Guide Specifications (UFGS): Cybersecurity of Facility-Related Control Systems*. U.S. Department of Defense, United States Army Corps of Engineers, UFGS-25 05 11. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11.

Wueest, Candid. 2015. "Symantec research highlights security failures in the connected home" ZDNet. https://www.zdnet.com/article/symantec-research-highlights-security-failures-in-the-connected-home/

Yucelen, Tansel, Wassim M. Haddad, and Eric M. Feron. 2016. "Adaptive Control Architectures for Mitigating Sensor Attacks in Cyber-Physical Systems." In *American Control Conference (ACC), Boston Marriott Copley Place, Boston, MA, July 6–8, 2016*, 1165–1170. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7525075&tag=1.

Zafari, Faheem, Ioannis Papapanagiotou, and Konstantinos Christidis. 2016. "Microlocation for Internet-of-Things-Equipped Smart Buildings." *IEEE Internet of Things Journal. 3(1):96–112.* https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7120085.

Appendix A – Overview of Commercial Building Systems

Building control systems have historically been designed with operational efficiency and service availability in mind and under the assumption they will not be connected to the internet. Their configuration can change over time as more devices are added to the system. Little to no security has been included in the communication protocols. The threat and business risk are not well quantified, and there is limited understanding of the consequences should a system fail in a specific way. Although most building systems are considered non-critical, failures to the operation of these physical systems could be exceptionally costly. The challenges associated with the current technological state of building systems manifest when the security limitations are not well understood, and they are unintentionally or unknowingly exposed to the broader cyber threat of the internet.

A.1 Heating Ventilation and Air-Conditioning Systems

Most commercial buildings that are over 30,000 square feet have some form of BAS for controlling their HVAC systems (EIA 2012b). Smaller commercial buildings generally rely on packaged systems that are similar, in terms of controls, to residential systems. The stock of large commercial buildings varies widely in age and condition of equipment and controls. It is not uncommon to see 20-year-old control systems that are a mix of pneumatics and proprietary digital controls. These systems have relatively little capability, may not be network-connected, and are somewhat obscure and likely to have relatively low risk in terms of cyberattack. Buildings with newer state-of-the-art control systems are at higher risk. Most of these newer systems utilize open standard protocols, such as the ASHRAE/American National Standards Institute (ANSI) BACnet that are unencrypted and allow for ready discovery of devices and easy reading and writing of data points. On the physical networking layer, most systems use a mix of dedicated field bus (RS-485/MSTP) and Ethernet (IP) networks, although new systems are providing additional options to connect controllers over IP. The user interface for these systems is through a workstation-based client or a server that provides web pages (HTML5 or Asynchronous Java and XML [AJAX]). HVAC control systems are often connected to an owner's enterprise network and may also be connected to the internet for remote operation and monitoring. While there are a series of best practices to provide protection for these systems they are not always implemented.

A.2 Lighting Control Systems

Networked and integrated lighting control is not as common as HVAC control for commercial buildings (EIA 2012). However, it is required under current codes (EERE 2014) and is becoming a common feature for new buildings and retrofits. While a few lighting control systems utilize open protocols, such as BACnet or Digital Addressable Lighting Interface (Rubinstein, Treado, and Pettler 2003), the vast majority are based on proprietary field bus protocols. Lighting control systems can be configured to be stand-alone or can be integrated into a BAS along with the HVAC control. New lighting control technologies include the use of “connected lighting” with smart sensors and controls in each fixture. These are connected using either wireless communications (often IEEE 802.15.4) or wired communication with Power over Ethernet, where the network cable provides both communications and power for the fixture (Tuenge and Poplawski 2017). Proprietary lighting control systems may employ some form of encryption. More advanced lighting control systems, including connected lighting, Power over Ethernet, and integrated systems are likely at higher risk of cyberattack.

A.3 Metering

In addition to utility-provided meters for electricity, natural gas, and water, many facilities are also installing their own building- or system-level sub-meters. Some of these sub-meters are not networked but are manually read on a monthly basis. Others are network-integrated for remote reading using either wired or wireless connection. Sub-meters often support open protocols, such as BACnet or Modbus, either directly from the meter or through a gateway. Since meters generally do not have the ability to issue control commands, the cyber risk is somewhat lessened. However, if the meter's firmware is overwritten, they can be employed to issue an attacker's commands on the sensitive building networks. They may also be blocked or forced to create false readings, deceiving the operators into perceiving problems where there are none or missing problems caused by attackers elsewhere in the system.

A.4 Fire Protection Systems

Fire protection, including alarm and extinguishing systems (sprinklers), is tightly controlled by codes and regulations. These systems are critical for life safety of the occupants in the building. These systems have transitioned to largely networked and digital communications, with all of the field bus wiring and protocols dedicated and proprietary. Proprietary protocols provide “security through obscurity,” relying on the lack of general knowledge about the protocol as protection. Such reliance is unwise. There are situations where a fire alarm system may be integrated into a BAS through a gateway, often using a protocol such as BACnet. These interfaces are considered “secondary annunciators” and have their functionality restricted to the status of alarm zones and potentially the ability to silence an alarm. Fire alarm systems are also moving to the ability to be able to notify a central monitoring service (or fire department) via an internet connection, in place of a traditional dial-up or dedicated phone line. In general, these systems are at fairly low risk for cyberattack, unless the attacker's aim is to increase damage by preventing these systems from notifying fire authorities in a timely manner. But the use of network connection and integration opens potential paths for attack.

A.5 Access Control Systems

Security systems, including motion detection and door-access controls, are highly coveted targets for attackers. They are generally well protected by being highly proprietary and through their use of encrypted communications. These systems are rarely integrated with other building control systems and are typically monitored full-time by security professionals. However, these systems are not without cyber risk. Currently, the industry is most concerned about the security of access control tokens (e.g., smart cards, etc.). Magnetic stripe card technologies may be easily copied and replicated, providing the ability to access a building using a cloned card.

A.6 Video Surveillance Systems

The use of video cameras is common in commercial buildings for monitoring and security. These systems have evolved from the use of analog cameras and monitors to the use of IP-enabled cameras that are on a wired or wireless network and connect logically to a digital or network video recorder for storage, viewing, and analysis. These systems are often on enterprise networks and may also be utilizing internet connections. Video cameras have long been an attractive cyberattack target. The paths for protecting these systems are similar to other building systems and include the use of firewalls, segmentation, encryption, and supplier management. Attackers may exploit human confidence in video surveillance to take advantage.

Because they stream pictures as network packets, video systems may be susceptible to replay attacks that show the same video stream of an empty room while a thief is actually at work.

A.7 Vertical Transport

Building vertical transport typically refers to elevators, escalators, and other people movers such as moving walkways. The controls for these systems have become more sophisticated and digital over the years. The high level of required safety in vertical transport means the controls systems are generally highly proprietary, with very limited external connectivity and ability to integrate. When these systems are integrated (which is fairly rare) the data exchanged is limited to status and alarms. There is little control ability through these interfaces unless their controllers can be overwritten or used as part of a deception campaign. The criticality of these systems creates high interest for a cyber attacker in certain scenarios, but they may be relatively protected through isolation.

A.8 Facility Management Systems

Facility Management Systems focus on controlling the operational management of buildings. Such systems aid in management of workflows, space scheduling, asset inventory, timely procurement, and maintenance scheduling to enable seamless building operations.

Appendix B – Standards

This section describes the current applicable standards from NIST and ANSI.

B.1 National Institutes of Standards

Standards from NIST described in this section include several frameworks and guides.

NIST SP 1500-201 Framework for Cyber-Physical Systems (CPS; Griffor et al. 2017)

This framework is focused on the protection of CPSs and was developed by the NIST Cyber-Physical Working Group. This group gathered experts to help define and shape the key aspects of CPS to accelerate the development and implementation of cybersecurity and physical security within multiple sectors of the economy.

NIST SP 800-37 Rev 1

Guide for Applying the RMF to Federal Information Systems (Feb 2010). This document provides guidance for applying the RMF to federal information systems. The six-step process includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The implementation of the RMF provides the necessary information to organizational leaders to make the most cost-effective and risk-based decisions regarding their information systems.

NIST Framework for Improving Critical Infrastructure Cybersecurity

This framework (Huergo 2018), often referred to as the Cybersecurity Framework (CSF), is required under EOs 13636 and 13800. It focuses on using business drivers to guide cybersecurity activities and the processes for considering the cybersecurity risks as part of an organization's risk management processes. There are three parts: the core, implementation, and profiles to help the organization with the prioritization of their cybersecurity activities. This framework describes the way cybersecurity is implemented, including its effectiveness on physical, cybernetic, and human systems. It can assist organizations in addressing cybersecurity in IT, ICS, CPS, and connected devices, including IoT. Organizations will have differing cyber risks, and the framework is aimed at reducing and better managing those risks.

NIST SP 800-53 Rev 4

This special publication provides a more holistic approach to information security and risk management by describing the breadth and depth of security controls designed to strengthen an organization's cybersecurity environment. The publication describes a variety of controls for continuous monitoring that supplies near-real-time information. This provides senior leaders with better information for risk-based decision-making.

NIST SP 800-82 Rev 2

Guide to Industrial Control Systems Security (May 2015) 800-82 provides guidance on securing ICS, including SCADA systems, Distributed Control Systems, and other control system configurations such as programmable logic controllers, while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS

and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

NIST SP 800-115

Technical Guide to Information Security Testing and Assessment (Sept 2008). The purpose of this guide is to assist organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies.

NIST SP 800-184

Guide for Cybersecurity Event Recovery (Dec. 2016). This document provides tactical and strategic guidance regarding planning, playbook development, testing, and improvement of cybersecurity event recovery.

B.2 American National Standards Institute

This section describes the current materials available from ANSI.

ANSI/ISA-62443-2-1 (99.02.01)-2009: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program (ISA 2009)

The business rationale for this standard is to identify what is at risk in the event of a cyberattack. Identifying and communicating these points helps strengthen a relationship with the organization and create perspective as to the importance of control system cybersecurity hardening. The steps include risk analysis; risk identification, classification, and assessment; selection of an assessment methodology; data collection; and performance of a high-level risk assessment. This standard recommends development of the following risk assessment strategy:

- Security policy, organization, and awareness, including defining control system scope, organizing for security, staff training and awareness, business continuity plan, policies, and procedures
- Security countermeasures and risk management including a summary of countermeasures in place, a plan to develop and maintain them, and a document management process
- Incident planning and response including a strategy to detect and respond to various incidents and a plan to conduct drills
- Implementation of system controls
- Ongoing monitoring and maintenance of the system and its security controls.

Appendix C – Communication Protocols

This section discusses communication protocols, including BACnet, Modbus, LanWorks, and ZigBee.

C.1 BACnet

BACnet (ASHRAE/ANSI standard 135, ISO 16484-5) was developed to provide an open standard for commercial building control systems communication and was originally approved in 1995. BACnet is an open standard control protocol that defines standard objects and services for interoperability. BACnet operates over various physical media options, including dedicated control field buses (such as RS-485) and shared networks using User Datagram Protocol or IP. BACnet has gained broad acceptance for use in commercial control systems, with recent market research estimating that 60 percent of new control shipments are BACnet compatible (BACnet International 2018).

The original release of BACnet had little support for either IP communications or security. Systems were initially deployed on dedicated networks using RS-485 (called MSTP in BACnet), ARCNET, and Ethernet. In 2008, a secured version of BACnet (ANSI 135 Addendum G) was approved. This solution was optional but proved difficult to implement. As a result, very few commercial products were introduced.

The BACnet Secure Communications working group is developing a new solution for secure communication using BACnet on IP networks. The approach is to communicate using TCP/IP sessions with Transport Layer Security. The document is completed and is in the process of being reviewed prior to approval in 2018 or 2019. This new approach uses encrypted communications and private keys. Several vendors have announced their intent to release products that will comply with the proposed standard; however, upgrading an existing system to encrypted communications may require updating system hardware, as well as firmware.

C.2 Modbus

Modbus was originally developed by Modicon (now part of Schneider Electric) in 1979. Since then, it has become a *de facto* standard for controller communications. Modbus is an easy protocol to implement and is often used for communications for electrical devices such as meters and drives. In common usage, the protocol is transmitted without encryption and all devices are required to respond to proper read or write requests. Modbus provides no security against data interception and command injection, making it suitable for perpetrating unauthorized command execution attacks, command reply attacks, denial-of-service attacks, and man-in-the-middle attacks.

C.3 LonWorks

The LonWorks standard was originally developed by Echelon corporation and is currently standardized as ISO/IEC 14908. LonWorks is being used as a field bus in many new and existing commercial buildings. Like BACnet and Modbus, LonWorks messages are sent without encryption. LonWorks does include the ability to utilize a 48-bit authentication key; however, this must be configured during installation and may not be used on many projects.

C.4 Zigbee Guidelines

The Zigbee Alliance has created a series of guidelines for wireless mesh networking implementing the IEEE 802.15.4 standard. Zigbee products are often used in home and small commercial building applications. Zigbee guidelines include both authentication, as well as encryption. A security analysis of Zigbee is available on the Massachusetts Institute of Technology's website.

Appendix D – Overview of Current Cybersecurity Buildings Efforts

Over the last few years, PNNL and other national laboratories have conducted cybersecurity research that ranges from basic research to development and deployment. A handful of those research initiatives and projects were developed under DOE, DHS, DOD, and others, while some of them have been field-tested and even deployed in multiple critical infrastructure facilities. This Appendix provides an overview of significant research projects and products that potentially fall under BTO's purview. Although not all of the discussed projects and products could be directly used with BTO's stakeholders in a plug-and-play fashion, the research to-date provides a foundation upon which BTO can consider tailoring and expanding the research and the products to fit the needs of BTO's stakeholders. In other words, all of the discussed projects and products can be potentially tailored towards BTO's stakeholders in a non-intrusive fashion. This listing should not be considered exhaustive or complete, merely a listing of relevant projects known to the authors.

D.1 OT Cybersecurity Tools for Buildings: High Maturity

D.1.1 The Buildings Cybersecurity Capability Maturity Model

One way to characterize the cybersecurity of a building is by using a maturity model. A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline, such as cybersecurity. A maturity model provides a benchmark against which an organization can evaluate the current level of capability of its cybersecurity practices, processes, and methods. Results can be used to set goals and priorities for improvement and to track over time the building's cyber-secure readiness status. Assessing the maturity of an organization's or a facility's cybersecurity program and readiness could potentially be a complex undertaking, as it includes all the facility's building control systems, appliances, and equipment. Conceptually, this complexity is similar to that encountered when utilities developed their cybersecurity methodologies and criteria within the National Framework for Improving Critical Infrastructure Security (EO 13636, Improving Critical Infrastructure Cybersecurity, February 2013).

The National Framework for Improving Critical Infrastructure Security borrowed heavily from the Electricity Sector's experience in applying the cybersecurity capability maturity model C2M2 (NIST 2014a), so the same fundamental principles of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), developed by DOE's Office of Electricity Delivery and Energy Reliability, are now being used across a wide array of critical infrastructure sectors (EERE n.d.). It addresses issues similar to those that buildings and facilities face, such as:

- How does my cybersecurity program compare with that of my peers?
- What are the relative strengths and weaknesses of my cybersecurity program?
- Are we appropriately allocating cybersecurity resources in a balanced and effective manner?
- Are we doing too much or too little?
- Where can I invest additional cybersecurity resources to get the "biggest bang for my buck?"

With this in mind, DOE directed PNNL to develop the Buildings Cybersecurity Capability Maturity Model (B-C2M2), drawing directly from the ES-C2M2. It is a first of its kind

cybersecurity tool developed to evaluate the cybersecurity maturity of buildings and to help building owners and operators respond to related cyber and physical threats. B-C2M2 provides a high-level view of cybersecurity situational awareness and risk, focusing on 10 critical cyber domains, including risk management, asset management, and workforce management. The B-C2M2 is, by design, completely voluntary, and provides descriptive and flexible guidance to building owners; it can be administered in one to two hours, an important consideration in the buildings sector. It is also important to note what the B-C2M2 does not do: 1) it is not an audit, controls assessment, or penetration test; 2) it does not provide specific guidance for implementing specific security controls; and 3) it is not intended to replace other cybersecurity-related activities, programs, processes, or approaches.

Five B-C2M2 demonstration pilots on government and commercial buildings, conducted from November 2015 to April 2016, reaffirmed the need for increased cybersecurity for buildings. Building operations and IT managers often are not clear regarding roles and responsibilities for securing critical cyber assets in buildings, especially for Internet-facing operational assets. Pilot studies suggest buildings managers and IT staff rarely have an updated or comprehensive inventory of critical building cyber assets. As a result, cyber-situational awareness on what assets are networked and internet-facing is often lacking. Managing BASs is often a time-intensive, ad-hoc exercise that relies on the expertise of a handful of people, rather than a systematic process. Initial data from B-C2M2 pilots suggests that contingency planning, cyber risk management, password management, and patching building controls for vulnerabilities does not appear to be an accepted norm in building operations.

D.1.2 Buildings Cybersecurity Framework

BCF was developed in 2016 to help buildings stakeholders identify, protect, detect, respond, and recover from cyber-physical threats, as well as mitigate cyber-physical vulnerabilities in buildings (NIST 2014b).[6] BCF is designed to deliver actionable guidance to key stakeholders in industry and government as well as building owners and operators, improve the cybersecurity situational awareness and security posture in buildings, and develop insight on how to build and maintain end-to-end cybersecurity in buildings. The core of BCF consists of five concurrent and continuous functions—Identify, Protect, Detect, Respond, and Recover—to help mitigate cybersecurity threats. Specific elements include:

- a user-friendly checklist to facilitate buildings security assessments, procurement, inventory, and cyber-situational awareness
- a threat vulnerability risk assessment matrix to determine threats and vulnerabilities of critical cyber assets in buildings and assess the risk of each critical asset in the risk assessment matrix.

D.1.3 CS-FEDS

At the direction of DOE, PNNL is exploring the potential integration of B-C2M2 into an existing federal building energy software tool developed at PNNL, known as the Facility Energy Decision System (FEDS; PNNL 2020). FEDS is an easy-to-use building energy efficiency software tool that quickly and objectively identifies energy efficiency improvements that maximize lifecycle savings; it has been extensively used to conduct energy efficiency and renewable assessments at DoD installations, including air force and army bases. The combined tool, Cyber-Secure–

[6] These five functions—Identify, Protect, Detect, Respond, Recover—are drawn directly from NIST's (2014b) "Framework for Improving Critical Infrastructure Cybersecurity."

FEDS, would provide a scalable approach for DOE to release for public use and an easy-to-use building energy efficiency and cybersecurity training and assessment tool that identifies energy efficiency and cybersecurity improvements that maximize lifecycle savings and optimize the security of building automation and controls systems.

D.1.4 Facility Cybersecurity Tool Suite

The development of the facility cybersecurity tool suite has been performed as part of the multi-year projects funded by FEMP. The OT cybersecurity tools are developed to help federal facilities to understand their cybersecurity posture and stay in compliance with the EOs 13686 and 13800. In addition, all of the tools under the facility cybersecurity tool suite have been field-tested at multiple federal facilities. Below are the six critical tools that are part of this tool suite:

1. Facility Cyber Framework (FCF) – While primarily designed for the OT networks in federal facilities, FCF can be used in non-federal facilities, as well. FCF was designed based on NIST CSF. The FCF tool equips organizations to better manage cyber risk, continuously improve their cybersecurity posture, and train OT and IT staff on cybersecurity standards and best practices. The easy-to-use, repeatable, holistic approach builds a culture that addresses the dynamic nature of cybersecurity risk. The FCF tool facilitates implementation of the May 2017 Presidential EO on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which calls on federal agencies and critical infrastructure owners and operators to manage their cyber risk through adoption of the Framework for improving Critical Infrastructure Cybersecurity developed by NIST (EO 13636 and EO 13800).
2. F-C2M2 Lite – Designed for OT networks with detailed emphasis on management requirements, in addition to technical constraints. F-C2M2 Lite was designed based on DOE's C2M2 architecture. The tool is adaptable and automatically re-adjusts throughout the assessment process based on the user responses.
3. Training Game – A real OT cybersecurity game designed to train facility owners and operators in regard to effectively responding to cyberattacks. The Cyber Security Training Game Simulator can be used to train staff and equip them to train others within their organizations, based on interactive scenarios that incorporate major U.S. cyberattacks experienced in the last 10 years.
4. FCF-Checklist – Tracking tool to evaluate "things to do" to improve the overall cybersecurity posture.
5. Qualitative Risk Assessment – A risk-informed inventory management tool that can be used by the facility owners and operators to qualitatively annotate and track the vulnerability, impact, and risk pertaining to their OT systems.
6. FCF-RMF – Primarily designed for DoD facilities and stakeholders. This can be used by the facilities that are most comfortable with NIST's RMF (e.g., DoD facilities may be recommended to be in compliance with RMF) and get two maturity scores: FCF and RMF scores. By doing this, the facility can stay in compliance with EO 13686, EO 13800, and DoD's RMF compliance requirements with a single assessment.

D.1.5 Mitigation of Exposure of Energy Delivery Systems (MEEDS)

Operations technologies, industrial control systems, IoT devices, and energy delivery systems are often inadvertently exposed to the public-facing internet, where threat actors can exploit them to gain control of critical networks and systems. MEEDS provides an effective, affordable, and easy-to-use cyber-risk management system designed specifically for energy utilities. The

advanced cyber defense technology offers a holistic defense-in-depth solution to mitigating potential cyber risks without degradation or disruption of energy delivery systems. It can distill data from Shodan, one of the world's largest vulnerability databases, which is used by over 50 percent of Fortune 1000 companies. It provides advanced identification and monitoring for important operations technologies, industrial control systems, and other systems that can be protected in no other way. Currently, MEEDS is in the process of advancements to adapt and use it for federal facilities such as buildings. The federal-facilities-specific MEEDS is scheduled to be released for field-testing in late 2020.

D.2 Grid Cybersecurity Tools with Potential Buildings Adaptability: Medium Maturity

D.2.1 Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2)

A key challenge in creating resilient systems is factoring in cybersecurity needs throughout the development process. SD2-C2M2 is an integrated tool that enables developers to design hardware and software for critical infrastructure against designated cybersecurity maturity levels. The tool can compare maturity levels against a set of management-derived requirements to determine hardware and software improvements as the devices are being developed. The easy-to-use framework features a graphical user interface that allows a user to select a subset of best practices for evaluating the technology's cybersecurity maturity. SD2-C2M2 is the only approach that intertwines management priorities with technical and security controls.

D.2.2 Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm (CyFEr)

In a typical hardware-centric organization, such as a power utility, IT and OT networks are equally important and are designed with firewalls between them that only a network administrator can navigate. If a cyberattack compromises administrator credentials, the attacker can bring down the entire system, potentially resulting in loss of power, infrastructure damage, and loss of life. CyFEr identifies critical vulnerabilities and gaps between IT and OT and prioritizes requirements to reach the desired cybersecurity maturity. CyFEr's built-in, optimized threat filters can be used to not only tailor the discovered vulnerabilities in relation to the business policies but also precisely identify the most critical threats in relation to those vulnerabilities. CyFEr can ingest various organizational bounds, such as cost and time limitations, to generate ideal mitigation paths to achieve the desired cybersecurity maturity.

D.2.3 Operations Technology Cyber Security Visualization Tool

Providing cybersecurity in control rooms for operations technologies is challenged by a lack of common taxonomy among control room operators and cybersecurity professionals. The Operations Technology Cyber Security Visualization Tool bridges the communication gap and improves situational assessment and awareness for operators and cyber experts. The tool allows them to work together to assess a situation and determine the best outcomes. It has been tested in an operational setting and enabled adequate communications for cybersecurity issues to be addressed. Because the tool is HTML-based, it can be used by any control center and cybersecurity operations center.

D.2.4 Integration of Green Renewable Energy Sources Securely

Control systems may issue messages alerting building and grid owners and operators about cybersecurity problems, but nothing defines whether those problems could result in unsafe or unstable conditions or shorten equipment lifetimes dramatically. Integration of Green Renewable Energy Sources Securely is an advanced attack detection and resiliency-enabling cybersecurity platform for behind-the-meter distributed energy resources. It can be deployed within legacy and emerging energy system environments to establish and verify the behaviors of devices, information, and command sequences. The platform builds and continuously improves models of the equipment that it protects, and it automatically prevents malicious control commands or operations in real-time. The platform also supports secure communication with other systems and utilities.

D.2.5 Threat Model-Based Response

Malware can extract a heavy toll on systems, but fighting it means determining how to defend against each piece of malware and ultimately attributing the source to prevent future incursions. Both approaches can prove challenging for most organizations. Threat Model-Based Response reduces these challenges by linking behaviors of particular types of malware to known threats, as well as successful defensive techniques. The technology uses hierarchical data clustering to identify common patterns and distinguish behavioral characteristics. This approach is particularly useful when confronted by malware that has unique features that may be otherwise difficult to predict.

D.2.6 Kritikos/Caddy

Cyber defenders in an industry are often unaware of dependencies between various IT assets. Kritikos/Caddy automatically discovers the relationships among assets using pattern recognition of network monitoring data. The technology uses an artificial neural network that groups and labels patterns to pinpoint dependencies. Understanding dependencies gives an organization better situational awareness and the ability to assess, triage, and recover from cyberattacks. Such knowledge also supports planning for business continuity, disaster recovery, and development of infrastructure investment strategies.

D.2.7 Framework to Analyze Cybersecurity Risks and Consequences for Critical Infrastructure (FRisC)

Current cybersecurity vulnerability assessments are missing a critical piece: the ability to analyze risks and consequences. Without information derived from such analysis, organizations cannot design programs that reach a desired security posture. FRisC identifies critical assets and their relationships to business processes, then analyzes the consequences of a disruption of those processes. Designed specifically for the power industry, the framework takes a multi-dimensional approach that enables FRisC to be used as a stand-alone system or in line with existing systems to analyze risks and consequences for decision-makers. FRisC's unique means of connecting business functions with engineering processes to identify the value-at-risk and consequences makes the technology scalable and applicable to other CI beyond the power industry.

D.2.8 Risk Model for Autonomous Adaptive Cyber Controllers

To help OT systems prevent, mitigate, and respond to cyber threats and events, some utilities are considering using adaptive cyber controllers that detect incursions and trigger defenses. What is often missing is a risk assessment. PNNL's risk model interfaces with cyber controllers to determine the expected impact of a cyber incursion on operational functions based on a list of potential cyber network reconfiguration alternatives. The model then characterizes trade-offs so that operators can take informed actions to prevent progression of an attack and minimize business disruption.

D.2.9 The Cymbiote

Embedded field devices that sense and control physical processes in critical infrastructure are soft targets for cyberattack because they lack the fundamental features for cybersecurity monitoring and control. A combination of hardware and software, and the only device of its kind, the Cymbiote collects data from multiple sources, synthesizes them to detect events of importance, and enables dynamic and real-time device reconfiguration for event recovery. It includes hardware to replace the Y cable to allow data to flow between pieces of equipment without disrupting normal operations or communications.

D.2.10 Shadow Figments

Deception is an approach to cybersecurity defense that slows attackers by diverting their attention and increases detection when attackers interact with the deceptive systems. Because control systems rely on physical rather than data processes, this approach is difficult for those systems to mimic, allowing attackers to easily reengage and penetrate the real system. Shadow Figments generates and runs high-fidelity deceptions of control systems. Using a model of the real process, the software generates controllers and sensors that respond to an attack in realistic ways to deceive intelligent attackers targeting control systems.

D.2.11 End-to-End Segmentation Via Containerization and Network Labeling

Critical business systems are often protected by the defense-in-depth approach—use of layers of defensive controls to prevent unauthorized access. However, in trying to retain the efficiency of less critical systems, industry may strip away these layers and leave a path through which adversaries can access more important systems. End-to-End Segmentation Via Containerization and Network Labeling creates containers around processes and allows each process to communicate with the others via labels that provide important contextual information. When an incursion is detected, the technology can dynamically alter network behavior to prevent any damage. This technology enables a level of segmentation never before possible, while providing strong protections that prevent threats to one business process from impacting other processes. All the while, the technology keeps processes agile and efficient.

D.3 VOLTRON Threat Profile

VOLTTRON™ is an open-source and secure execution and communications platform, what today would be called an IoT platform. Although VOLTTRON has been used in a number of buildings, grid, and buildings-to-grid applications, the core platform is application neutral. Developed and maintained by PNNL, VOLTTRON is now part of Eclipse Foundation's suite of IoT projects.

VOLTTRON is, essentially, a small operating system built on top of Linux and Python. This minimal software stack is able to run on small cheap computing platforms such as Raspberry Pis. VOLTTRON runs specially crafted programs called "agents." Agents communicate with one another and the outside world using tagged messages in a pub-sub (publish-subscribe) model. Agents post messages onto a message bus (essentially a queue); when the message reaches the head of the queue, agents that subscribe to the relevant tags are "woken up" and executed. The VOLTTRON messaging infrastructure supports federation (aggregation) of multiple VOLTTRON instances such that agents in different VOLTTRON instances (e.g., two different Raspberry Pis) within the same network can communicate as if they are executing in the same instance.

VOLTTRON's core functionality is complemented by a library of agents that perform both general and building-specific functions. Building-specific agents include driver agents for protocols such as BACnet, MODBUS, and OpenADR, and an agent that encapsulates EnergyPlus for testing other agents against simulated buildings. General purpose agents include a cloud communication agent, a "historian" for batching data, and an agent for downloading data from online weather services.

These common "utility" agents can be combined with custom agents to implement a range of applications. In the buildings space, VOLTTRON was initially conceived as a platform on which to build low-cost "software only" BASs for small and medium commercial buildings that cannot bear the cost of traditional BAS. However, other use cases have also emerged. These include:

- A side-car or data-bridge to a traditional BAS for performing custom analytics.
- Communications and control for building components and subsystems such as refrigeration systems, RTUs, and water heaters.
- Federation and aggregation of monitoring and control across multiple buildings.

VOLTTRON also has a number of non-building applications in utility scale solar installations, EV charging, and battery management. DOE laboratories continue to use VOLTTRON in research and development of building sensing and control infrastructure and to support use of VOLTTRON by third parties.

The VOLTTRON team has engaged with Pacific Northwest National Laboratory's PNNL's ***Secure Software Central (SSC)*** Team to provide cybersecurity analyses of the VOLTTRON software. SSC offers both threat-based analysis services and secure software development services, as defined in Figure 2. These services are used to document, understand, and mitigate software threats and vulnerabilities based on categorized and prioritized threats as well as secure software life-cycle principles.

Threat-Based Software Analysis **–** determines and prioritizes threats against the software system and recommends mitigations. The result is a Threat Profile that contains a threat model, threat findings, and mitigations.
Secure Software Development **–** applies security best practices to the software development life cycle. This includes secure design, secure code review, vulnerability scanning, and security testing.

Figure 2. Secure Software Central services

Purpose of the Threat Profile. The Threat Profile establishes security requirements, justifies security measures, yields actionable controls, and effectively communicates risk. To that end, it can be effectively used by development teams, software architects, managers, and stakeholders. For stakeholders and managers, the Threat Profile shows what has been mitigated and what has not been mitigated, thus enabling decision makers to assess priorities

based on the actual system and the threats against it. For development teams and software architects, the Threat Profile provides direct and actionable tasking that boosts the cybersecurity of the software product. The format of the Threat Profile maps mitigations to threats and threats to a system diagram, making it clear where and how the controls are affecting and benefiting the system.

Categorizing and Prioritizing Threats. Categorizing threats helps identify, organize, and prioritize threats in any system—this holds true for the VOLTTRON software. To optimize the analysis process, streamline the engagements, and aid in mitigation implementations, SSC utilizes Microsoft's STRIDE model (see Figure 3).

Spoofing **–** when a process, file, website, network address, etc. is not what it claims to be
Tampering – the act of altering the bits in a running process, data in storage, or data in transit
Repudiation – involves an adversary denying that something happened
Information Disclosure – when the information can be read by an unauthorized party
Denial of Service – when the process or data store is unable to service incoming requests
Elevation of Privilege – when an adversary gains increased capability on a system or network

Figure 3. Microsoft's STRIDE model described

Prioritizing threats is also critical in developing a Threat Profile. With mitigations unique cost, level of effort, and consequences, so it is critical to prioritize. The SSC basis for prioritizing is the standard CIA (Confidentiality, Integrity, and Availability) Triad. Stakeholders must rank ***Confidentiality*** (keep the data secret), ***Integrity*** (make sure the data is correct), and Availability (make the data available). VOLTTRON's ranking is show in Figure 4.

Figure 4. VOLTTRON priorities.

Value. The VOLTTRON Threat Profile provides the foundation for a thorough understanding of threats for VOLTTRON users. It enables decision makers at all levels to improve the security posture of VOLTTRON. This effort leads to more secure software and better-understood security; the VOLTTRON team is to be commended for their rigorous approach to employing cybersecurity throughout the software development life cycle.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov