Foreword

Fire protection systems are increasingly networked to Building Control Systems (BCS), Internet of Things (IoT), and other platforms that are, by design or oversight, exposed to the public-facing Internet. This emerging environment leads to unique and novel cyber vulnerabilities, and attacks on fire protection systems have the potential to have significant consequences. However, a thorough understanding of cybersecurity issues related to fire protection systems was lacking. The expansiveness of these vulnerabilities, the severity of the consequences, and the awareness of the fire protection community of these vulnerabilities was not well understood. Therefore, this project aimed to address these gaps by assessing the cybersecurity threats of built-in fire protection systems connected to BCS, IoT, and other potentially Internet-facing platforms.

The Fire Protection Research Foundation expresses gratitude to the report authors Jessica Chevreaux, Phil Owen, Ken Donaldson, Kyler Bright, Alexandra Largen, Daniel Meiselman, Kateryna Kirsanova, Michael Borinski, and Alejandro Uribe, who are with M.C. Dean, Inc. located in Tysons, Virginia. The Research Foundation appreciates the guidance provided by the Project Technical Panelists, the funding provided by the project sponsors, and all others that contributed to this research effort.

The content, opinions and conclusions contained in this report are solely those of the authors and do not necessarily represent the views of the Fire Protection Research Foundation, NFPA, Technical Panel or Sponsors. The Foundation makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

About the Fire Protection Research Foundation

The Fire Protection Research Foundation plans, manages, and communicates research on a broad range of fire safety issues in collaboration with scientists and laboratories around the world. The Foundation is an affiliate of NFPA.

About the National Fire Protection Association (NFPA)

Founded in 1896, NFPA is a global, nonprofit organization devoted to eliminating death, injury, property and economic loss due to fire, electrical and related hazards. The association delivers information and knowledge through more than 300 consensus codes and standards, research, training, education, outreach and advocacy; and by partnering with others who share an interest in furthering the NFPA mission.

All NFPA codes and standards can be viewed online for free.

NFPA's membership totals more than 65,000 individuals around the world.

Keywords: cybersecurity, vulnerabilities, insider-threats, fire protection systems, mass notification systems, two-way communication systems, two-way radio systems.

Report number: FPRF-2021-10

Project Manager: Victoria Hutchison
Project Technical Panel

Jens Alkemper, FM Global
Vincent Baroncini, Siemens (Alternate)
Krista Biaso, HGA Architects and Engineers
Lou Chaves, UL (alternate)
Dan Finnegan, Siemens
Joe Gittens, Security Industry Association
Joel Goergen, Cisco
Chad Jones, Cisco (alternate)
David Klien, Las Vegas Fire and Rescue
Peter Larrimer, Department of Veterans Affairs
Brian Marchionini, NEMA
Alan Manche, Schneider Electric
Mike Pallett, Telecor
Denise Pappas, Valcom/Keltron
Tyler Robinson, Dark Element
Richard Roux, NFPA
Larry Shudak, UL
Haritha Srinivasan, FM Global (alternate)
George Zimmerman, CME Consulting

Sponsor Representatives

Chad Beebe, American Society of Healthcare Engineering (ASHE)
Christina Francis, Procter and Gamble
Russ Leavitt, Telgian
Joseph Gochal, NFPA
Project Sponsors

ASHE  
Optimizing health care facilities  
Procter & Gamble  
telgian  
NFPA
# TABLE OF CONTENTS

1 TASK 1 – LITERATURE REVIEW ................................................................................. 2
  1.0 Introduction........................................................................................................ 2
  1.1 OVERVIEW OF APPLICABLE CODES, STANDARDS, BEST PRACTICES, GUIDES ETC.  2
     1.1.1 CYBERSECURITY BEST PRACTICES ......................................................... 4
  1.2 STAKEHOLDERS, THEIR ACTIVITIES AND ATTRIBUTES............................. 7
  1.3 CYBERSECURITY TERMINOLOGY APPLICABLE IN FIRE PROTECTION ........ 9
  1.4 FIRE PROTECTION VULNERABILITIES AND THREATS............................... 12
  1.5 PREVENTION AND INTERVENTION STRATEGIES ...................................... 15

2 TASK 2 – CASE STUDIES ......................................................................................... 17
  2.0 CASE 1 – [SOUTH CAROLINA FIRE DEPARTMENT SERVERS DISABLED BY HACKERS]  17
     2.1 CASE 2 – [WHEN PHYSICAL INTRUSIONS LEAD TO DIGITAL BREACHES] ........ 18
     2.2 CASE 3 – [RANSOMWARE ATTACK WIPES OUT RIVERSIDE POLICE AND FIRE DEPARTMENT DATA] ................................................................. 19
     2.3 CASE 4 – [MITIGATING INSIDER SABOTAGE] ............................................. 20
     2.4 CASE 5 – [INSIDE A PHISH] ........................................................................ 21

3 TASK 3 – WORKSHOP AND REFINEMENT OF BASELINE MATERIALS ......... 22

4 TASK 4 – GAP ANALYSIS ..................................................................................... 23
  4.0 KNOWLEDGE GAPS AND EXISTING GUIDANCE ANALYSIS .................... 23
  4.1 FUTURE RESEARCH NEEDS FOR CYBERSECURITY OF FIRE PROTECTION SYSTEMS ......................................................................................................................................................... 25
  4.2 ROADMAP TO ADDRESS CYBERSECURITY CHALLENGES IN FIRE PROTECTION SYSTEMS ......................................................................................................................................................... 27

5 INFORMATION REFERENCES ................................................................................. 28
1 TASK 1 – LITERATURE REVIEW

1.0 Introduction
Fire protection systems are increasingly networked to Building Control Systems (BCS), Internet of Things (IoT), and other platforms that are, by design or oversight, exposed to the public-facing Internet. This emerging environment could lead to unique and novel cyber vulnerabilities, and attacks on fire protection systems have the potential to have significant consequences. However, a thorough understanding of cybersecurity issues related to fire protection systems is lacking. The expansiveness of these vulnerabilities, the severity of the consequences, and the awareness of the fire protection community of these vulnerabilities is not well understood.

The goal of this project is to assess the cybersecurity threats of built-in fire protection systems connected to BCS, IoT, and other potentially Internet-facing platforms.

1.1 OVERVIEW OF APPLICABLE CODES, STANDARDS, BEST PRACTICES, GUIDES ETC.

One must identify various components comprising fire protection systems and the associated vulnerabilities to understand the relevant guides, codes, and best practices. This includes fire alarm systems, suppression systems, fire extinguishers, external systems linked to the fire alarm system (e.g., HVAC, elevator, physical access control, etc.), and sprinkler systems. The most vulnerable system components are the head-end units (typically servers), as these systems are often exposed to IT (Information Technology) and OT (Operational Technology) networks. The list below is a compilation of the most relevant codes related to cybersecurity of fire protection.

1. NFPA 72 – National Fire Alarm and Signaling Code
   • Includes guidance and requirements to address cybersecurity for equipment, software, firmware, tools, and installation, as well as physical access and security.

2. NFPA 70 – National Electrical Code
3. NFPA 92 – Standard for Smoke Control Systems
5. NFPA 110 – Standard for Emergency and Standby Power Systems
7. NFPA 731 – Standard for Installation of Electronic Premises
8. NFPA 1221 – Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems
10. IEC 62443 – Security for Industrial Automation and Control Systems
11. UL 864 – Standard for Safety of Control Units and Accessories for Fire Alarm Systems
12. UL 2572 – Standard for Mass Notification Systems

15. DoD Cyber Workforce – Starting point to learn about cyber frameworks, examples, and KPI’s

16. Cybersecurity Maturity Model Certification (CMMC) - consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the Defense Industrial Base (DIB) and Department of Defense (DoD) stakeholders.

17. DoD Cyber Workforce Framework - standardized workforce framework that DoD cybersecurity uses to categorize the full spectrum of cyber workforce roles.

Most of the life safety standards have been developed with fixed rules which will be a real challenge to be effective by the time they are published. Risk Assessments are also a challenge for code officials to work with, and do not seem to have been welcomed as an alternative approach. It will be important to coordinate where intersections may occur between traditional fire protection systems such as fire alarm systems, automatic sprinkler systems, and fire pumps among others and related systems such as medical equipment (NFPA 99) and backup generators (NFPA 110). Along with those, power over ethernet (NFPA 70) is another open channel that would be sensitive to cybersecurity risks.

Once interconnected systems have been evaluated, we can obtain a better understanding of system components, interdependencies, functions, and vulnerabilities.
1.1.1 CYBERSECURITY BEST PRACTICES

Cybersecurity strategies should protect assets deemed critical to a successful operation. To apply these practices, an organization must understand the relationship of threats and vulnerabilities to the standards and countermeasures put in place to protect the operations, personnel, and technologies that comprise a system. As the organization must continuously adjust and refine security countermeasures to ensure protection against emerging threats.

Workforce awareness and training are the most crucial aspects of protecting critical systems. Infrastructure systems are typically connected to other enterprise networks and systems. One must be aware of vulnerabilities introduced as systems become more interconnected. Many threats exploit human behaviors including:

- **Phishing** - The practice of sending fraudulent communications that appear to come from a reputable source. It is usually performed through email to induce individuals to activate automatic downloads or click through to malicious sites. Phishing attacks may also manipulate users into revealing personal information, such as passwords, or other sensitive information.

- **Piggybacking** - Unauthorized party gains access to some system in connection with an authorized party. This can happen in several ways, including piggybacking on public wireless networks, and piggybacking into a password-protected system.

- **Extortion** – By leveraging compromising information or financial gain, individuals may be coerced into releasing confidential information.

Providing information security training to staff is a crucial step to protecting systems. Training is paramount, and a well-trained workforce can implement and execute the following common cybersecurity best practices:

- **Risk Management and Cybersecurity Governance**
  - Identify threats to the system.
    - Perform vulnerability scans and penetration tests
  - Develop policies, procedures, and training
    - Strong passwords
    - Encryption
    - Limit privileges
    - Annual trainings to educate best practices and common cyber threats
    - Ensure tools used in performing any response, assessment, or remediation activity are themselves assessed, scanned, patched, and up-to-date on firmware upgrades.
  - Develop and practice incident response procedures.
    - Preparation – Creating checklist, recovery plans, monitoring tools, risk assessment
    - Identification – Investigate event, decide whether it’s a false positive or incident
    - Containment – Isolate the system, determine if the incident has propagated
    - Investigation – Systematic review, what data was accessed, who accessed the system, review logs
• Eradication – Cleanup and notify personnel
• Recovery – Service restoration and system validation
• Lessons Learned – Was the incident handled in an appropriate amount of time, and how can we prevent from happening again
  o Develop continuity of operations.
• Physical Security
  o Ensure only authorized personnel have access to controlled spaces that house the systems.
  o Use multi-factor authentication, guards, and barriers to control logical and physical access.
• Network Architecture
  o Utilize segmentation of networks.
    • Network is divided into multiple zones, with specific security protocols applied to each zone. The main goal of network segmentation is to have a better handle on managing security and compliance.
  o Develop Network Architecture Diagrams.
    • Shows how nodes, devices, and connections on your network are physically and logically arranged.
  o Employ reliable and secure network protocols and services where feasible.
    • IPSec
    • SSL
    • SSH
    • HTTPS
    • Kerberos
• Host Security
  o Patching and vulnerability management.
    • Patch management is the process of distributing and applying updates to operating systems, applications, and embedded systems. This is important for security, uptime, and compliance.
    • Vulnerability Management is identifying, prioritizing, and remediating vulnerabilities on systems and software.
  o Test all patches offline before implementation.
  o Implement device hardening measures available from manufacturer or third parties.
  o Replace out of date software and hardware.
  o Ports, protocols, and services identification and management.
  o Implement and test backups and recovery processes.
• Security Monitoring
  o Test against the baseline of normal operations.
• Establish a set of controls and standards that your system must be compliant to.

• Perform security assessments
  o Setup tools to monitor, analyze, and correlate logs to identify intrusion attempts.
  o Web Server, network, application, and database monitoring tools collect, and aggregates log data generated throughout the organization’s technology infrastructure, from host systems and applications to network and security devices
    • We can use these tools to setup alerts that can be reviewed by dedicated security personnel and escalated if needed
  o Deploy file monitoring methods that alert personnel if critical executable or configuration files are modified outside of maintenance windows.

• Perimeter Security
  o Configure firewalls to control traffic.
  o Prevent remote access.
  o Encrypt traffic in transit.

• Human Element
  o Train personnel to recognize the indicators of potential compromise and what steps they should take to ensure a cyber investigation succeeds.
1.2 STAKEHOLDERS, THEIR ACTIVITIES AND ATTRIBUTES

Identify the key stakeholders, their activities, and other attributes.

NFPA defines stakeholder as any individual, group, or organization that might affect, be affected by, or perceive itself to be affected by the risk (NFPA-72 3.3.276). Based on the level of involvement and affect the key stakeholders are as follows:

- **Standards Keeper (NFPA):** Develops standards that drive design, testing, operation, and security of fire protection systems at the minimum requirements necessary.

- **Manufacturers:** Design, manufacture, and sell fire protection devices and components that interface with the fire protection and other building systems. Devices might inherently have cyber security flaws, and prevention methods would either need to be built around this or to be corrected.

- **System Designers:** Design and plan fire alarm systems for detection coverage, notification coverage, and other related elements to the fire protection system.

- **System Installers:** Specialized companies and their staff responsible for actual installation of fire protection systems.

- **Service Personnel/Testing Personnel:** Staff employed by a variety of service providers who interact with system components including hardware and software within the duration of fire protection system life cycle.

- **Building Owners:** Property owners or operators responsible for fire protection system code compliance, maintenance, inspection, testing and security.

- **Occupants:** Primary users of the physical work areas and/or locations whose life is one of the main objects of fire protection systems. Provide last line of physical security to components residing within their work areas.

- **Authority Having Jurisdiction (AHJ):** An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, and installation, or a procedure.

- **Supervising Station:** Facility that receives signals from protected premises fire alarm systems and at which personnel are present at all times to respond to these signals.

- **First Responders:** Firefighters and service personnel who responds to calls for emergency support. They are the first to arrive and provide assistance at the scene.

- **Insurance Carriers:** Insurance companies who determine additional requirements and coverage for fire protection systems to assure maximum protection and mission continuity and covers losses in case of fire related accident.
• **Threat Actors**: a person or entity responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity.
1.3 CYBERSECURITY TERMINOLOGY APPLICABLE IN FIRE PROTECTION

Identify common terminology applicable to cybersecurity in fire protection applications.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Code Appears in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible</td>
<td>Admitting close approach, not guarded by locked doors, elevation, or other effective means</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Alarm Verification Feature</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Building System Information Unit (BSIU)</td>
<td>A computer-based electronic device that is intended to display building information and execute system control functions, including fire system information display and control.</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Channel (and sub definitions)</td>
<td>A path for voice or signal transmission that uses modulation of light or alternating current within a frequency band.</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Communications Cloud</td>
<td>The area in the communications path that is supported by providers of communication services not governed under the scope of NFPA 72 in which signals travel between a protected property and a monitoring station. Depending on the type of transmission that is used, signals can travel on a single defined route or through various routes depending on what is available when the signal is initiated.</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Control Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Alarm Communicator System (DACS)</td>
<td>A system in which signals are transmitted from a digital alarm communicator transmitter (DACT) located at the protected premises through a managed facilities-based voice network to</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>a digital alarm communicator receiver (DACR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electromechanical Releasing Device</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Emergency Communications System – Emergency Command Center Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net-Centric Alerting System (NCAS)</td>
<td>A net-centric alerting system incorporates web-based management and alert activation application through which all operators and administrators could gain access to the system’s capabilities based on the users’ permissions and the defined access policy. (SIG-ECS)</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Wireless Network</td>
<td>The method of communication used in a public emergency alarm reporting system that consists of two or more points that are not connected by physical wires.</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Network Architecture</td>
<td>The physical and logical design of a network and the inherent ability of design to carry data from one point to another</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Radio Alarm System (RAS)</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Signal(s)</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Executive Software</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Site Specific Software</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Transmitter</td>
<td></td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Unwanted Alarm</td>
<td>Any alarm that occurs that is not the result of a potentially hazardous condition</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Alarm Type</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Malicious Alarm</td>
<td>An unwanted activation of an alarm initiating device caused by a person acting with malice</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Nuisance Alarm</td>
<td>An unwanted activation of a signaling system or an alarm initiating device in response to a stimulus or condition that is not the result of a potentially hazardous condition.</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Unintentional Alarm</td>
<td>An unwanted activation of an alarm initiating device caused by a person acting without malice</td>
<td>NFPA 72</td>
</tr>
<tr>
<td>Unknown Alarm</td>
<td>An unwanted activation of an alarm initiating device or system output function where the cause has not been identified</td>
<td>NFPA 72</td>
</tr>
</tbody>
</table>
1.4 FIRE PROTECTION VULNERABILITIES AND THREATS

Define what fire protection systems or subsystems are vulnerable to cybersecurity threats (e.g. fire alarm systems, electrically monitored fire extinguishers, carbon monoxide detectors, etc.) and identify and categorize potential cybersecurity threats to these fire protection systems.

It is important to define and draw distinctions between the terms threat, vulnerability, and risk:

- **Threat** – anything that can cause a negative or adverse event or result.
- **Vulnerability** – a flaw or gap that can be exploited leading to a potentially negative or adverse event or result.
- **Risk** – the quantified impact and likelihood of a negative or adverse event.

Increased functionality or convenience leads to potential new vulnerabilities, which leads to increased attack surface. Attack surface are the parts of a system which are vulnerable to a malicious actor. As we interconnect our Life Safety control systems with outside networks, we increase our attack surface.

It is convenient to send a text message or an email in case of an alarm. However, it is necessary that a Fire and Life Safety system be connected to outside networks to send these notifications. Inherently, this poses additional risk. Moving forward, we must communicate to our customers that while a technology may be available, it may not be in the best interest of the customer’s security posture to implement that feature.

- **We must carefully consider if the risks of introducing additional vulnerabilities outweigh the value of the increased functionality.**
  - Internal IT networks should be accessible only to authenticated staff and contractors and should be physically or logically separated from controls networks.
  - External IT networks, including the Internet should only be accessible from systems that require internet connectivity.
  - Remote Access portals such as VPNs and software tools including VNC and TeamViewer are a common point of entry for threat actors into Operational Networks. These tools are designed to allow trusted outsiders inside your network. Access to these portals should be carefully monitored and controlled.
  - Wi-Fi is the primary wireless communication system used in IT networks. Some older wireless security protocols are readily bypassed and should be updated to newer protocols. Even if you physically secure your site, a threat actor may be able to access your wireless networks from outside your physical perimeter. Perform routine audits to detect rogue access points. Consider wireless access point placement and antenna design when deploying Wi-Fi networks.
  - Bluetooth presents significant security risks. Bluetooth should be disabled where possible and only used where necessary.
  - Some controls equipment communicates over Radio frequency (SWIFT, industrial, scientific, and medical (ISM)). These devices should be configured in such a way that their radio communications are encrypted, as a threat actor with commercially available equipment could intercept or falsify these communications.
  - Traditional controls protocols including BACnet/Modbus/RS232/RS485 may use unencrypted serial or ethernet-based communications which can be intercepted or interrupted by threat actors. Defense measures such as restricted physical & logical access, segmentation, OT based security monitoring should be considered for systems/devices using traditional control protocols.
  - Telephone lines connected to always-on modems. Additional protection measures should be considered for active dial-up modems such as call back setting to a designated phone number, caller ID filtering, disabling auto answer, etc.,
Potential Attack Surface

The network perimeter, specifically the areas where the fire alarm system connects to other networks, systems, or more generally exchanges data with anything else. These points can be considered “system interfaces or points of connection” and are often especially vulnerable (and targeted by threat actors).

Where the FA System touches IP pathways, or has any connection/port where an individual could connect into the system, such as a fire panel with a laptop or other device and cause harm. These points represent potential attack surface and need to be secured in hardware/firmware/software and/or with physical access controls.

While the presence of an IP network in and of itself is important to consider, it’s also critical to consider how that IP network is setup and what other devices (beyond the panels and cabling) may be present to provide connectivity.

- Cellular
- Physical access
Figure 1 shows a map of devices which may comprise a fire alarming and suppression system. Please note, not all installed systems will contain all components. The left side of this diagram shows inputs (sensors, power) to the fire system, the right shows outputs (annunciators, dialers).
1.5 PREVENTION AND INTERVENTION STRATEGIES

Identify and categorize existing prevention and intervention strategies to address identified threats.

In the world of Information Security and Cybersecurity, *security control* refers to the “application of specific safeguards or through the regulation of specific activities.” The need for these security controls is at an all-time high as cyber-attacks and cyber-crimes occur around the clock. Security controls and techniques are implemented to protect the cyber environment of a user or organization. The objective of this is to reduce attack surface. Below is a list of strategies that will facilitate in the prevention of cyber-attacks in a system.

- Implement an asset management program (maintain inventory of hardware, software, firmware, etc.,) to track device assignments for staff to and support asset replacement / refresh.
- Develop criticality rating of assets to determine appropriate security controls.
- Implementing physical access control and monitoring for alarms, prevents malicious actors from gaining physical access to the system.
- Implementing configuration change control to monitor for unauthorized activity.
- Employ network monitoring and audit firewall logs on a set frequency. Implement patch management program and develop measures to isolate systems that are obsolete.
- Develop incident playbooks and practice through tabletop exercises.
- Implementing network segmentation divides the network into smaller more isolated groups. This deters malicious actors and inquisitive personnel.
- With proper preventative training, organizations are more protected from malicious actors and prevent possible data breaches.
- Unused and insecure ports and protocols are potential attack vectors and should be disabled whenever possible.
- Perform scanning of portable devices such as USB, memory cards, contractor laptops, etc., before connecting to fire protection systems.
- Default Passwords are usually well known. If the default passwords are not changed, an actor with manufacturer documentation may be able to gain access.
- Guest Accounts allow anonymous access to a system. These should be disabled to properly monitor user activity.
- Implementing Role-Based Access Controls (RBAC) is a common security practice that creates separation of duties. (i.e. Preventing entry level personnel to access admin level controls)
- Firewalls monitor and filter network traffic and should be implemented as one of the first lines of defense to protect a system.
- Gathering a system baseline allows organizations to quickly identify anomalies that could be evidence of an attack or threat.
- By implementing policies of Least Privilege, we can reduce the likelihood of insider threat by limiting
user access to only authorized data sets and processes.

- A mindset of “this is the way we’ve always done things” can be very dangerous. The way we used to design and install these systems needs to be re-evaluated.

- Minimize network exposure for all devices and/or systems, and ensure that they are not accessible from the Internet.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that a VPN is only as secure as the connected device. Where possible, implement Multi-factor Authentication (MFA) for remote access connections.

- Identify potential trust boundaries, where data connections traverse from a “trusted” network (e.g. usually provisioned/managed by the fire alarm vendor or the system owner) to an “untrusted” network (e.g. a network that contains devices that aren’t fully vetted or over which the system owner has limited control). Trust boundaries are a critical concept in cybersecurity, as each boundary should be protected with a cyber control (usually a firewall) that limits the ability of the “untrusted” network to harm the “trusted” network and vice versa. In the most obvious case, anything connecting to the internet is traversing a trust boundary. However, a trust boundary can also exist between networks provided by two separate vendors or between a vendor-provided network and a system owner-provided network.
2 TASK 2 – CASE STUDIES

Conduct a case study review of cybersecurity incidents relevant to fire protection systems. Specifically analyze the vulnerabilities and challenges from each incident and assess the effectiveness of intervention strategies, where available.

2.0 CASE 1 – [SOUTH CAROLINA FIRE DEPARTMENT SERVERS DISABLED BY HACKERS]

Organization: Bluffton Township Fire District, South Carolina

Scenario: A note was discovered on the Fire District’s computer servers, March 15th, 2020. The computers were rendered inoperable by the hacker. Records, files, and email communications had been encrypted. The ransom note included an email address to write to, where the hacker would reply with “the cost of decrypting your files.” The hacker included assurances the files would be returned after payment. The Fire Department went to law enforcement, which is recommended by the FBI. 7 months of data has been recovered.

Attackers and motivation: The attacker targeted record, files, and email communications.

The attacker encrypted them and requested money in return for releasing them. The attacker’s motivation was to get money from the fire department.

Techniques used: Though the hacker’s methods were not identified because of an active investigation, common techniques could have been used. One most common technique being phishing. Phishing is when an attacker emails a potential victim a compromised website, where attackers can gather important credentials.

Prevention: Phishing can be prevented by not opening suspicious emails or clicking on suspicious links. Setup protocols in place for when an employee receives a suspicious email. Whitelisting email domains can further prevent phishing emails.

Business impact: District Captain Lee Levesque stated that no personal or sensitive information was taken, and the biggest impact was resorting to physical paperwork. The national state guard retrieved 7 months of the data back.
2.1 CASE 2 – [WHEN PHYSICAL INTRUSIONS LEAD TO DIGITAL BREACHES]

**Organization:** Health Care

**Scenario:** A recent joint report from Michigan State University and Johns Hopkins University researchers illustrates the scope of the issue. Their review of 1,150 electronic medical record cases between October 2009 and December 2017 that impacted more than 164 million patients found that more than half (53 percent) of data breach issues were internal to medical providers, such as unauthorized access or improper disposal, not due to hackers or other external actors.

“The perfect storm would be that you could get into a secured area, get onto someone’s computer because they didn’t log out, or their computer hasn’t timed out, and all of the sudden, you’re into a secured database with access to confidential information,”

**Techniques used:** Tailgating, an attacker lacking proper authentication gaining access to a secure area. An example of this attack is to follow an employee who is authorized to access a restricted area. Another example is an employee leaving their badge somewhere where an attacker can access it, thus giving access to the restricted area to the attacker.

**Prevention:** Proper ID management, training employees to keep track of their IDs. “You need to know where the ID is at all times. Don’t leave it on your desk or in your car… Themoment you notice your badge missing, file a report so the access can be shut off.”

Tailgating can be mitigated by training employees to politely deter potential bad actors. “How may I help you? I’m sorry, this is not a door open to the public. You’ll have to use Door A to come this way.” If you don’t know someone, ask them.

**Business impact:** Once an attacker has access to a restricted area, they can access sensitive information, drugs, or technology (laptops, phones, etc.).
2.2 CASE 3 – [RANSOMWARE ATTACK WIPES OUT RIVERSIDE POLICE AND FIRE DEPARTMENT DATA]

**Organization:** Riverside Police and Fire Department

**Scenario:** On May 3rd, 2018, Riverside Police and Fire departments were hit by a ransomware attack for the second time in three weeks. The attacker locked sensitive data including records containing information about ongoing investigations.

This attack was less damaging than the first, however eight hours of data was lost. The first attack caused one year’s worth of files to be lost. The City Manager Mark Carpenter is unclear how both attacks occurred, but he confirmed that was a malware attack leading to a ransomware infection. Mr. Carpenter stated, “Everything was backed-up, but we lost about eight hours’ worth of information we have to re-enter. It was our police and fire records, so we just re-enter the reports.”

**Attackers and motivation:** The attacker’s motivation was financial gain. Attackers demanded bitcoin due to its untraceable transaction system while demands in Monero cryptocurrency have also increased.

**Techniques used:** The U.S. Secret Service were investigating the attacks, but nothing has been released how both attacks were instigated. Common techniques are phishing, removable media, and Remote Desktop Protocol. Phishing is when an attacker sends emails with a malicious link. Attackers can drop USB drives in parking lots or outside of buildings. They expect you to plug it into your computer to either identify the owner or identify what is on the drive.

**Prevention:** Prevention starts with training employees to identify suspicious activity. Train employees not to click on any suspicious emails or links. Setup protocols in place for when an employee receives a suspicious email. Whitelisting email domains can further prevent phishing emails.

Train employees not to plug USB drives or any suspicious removable media into their computers. Any drive could be malicious.

**Business impact:** The first attack on the Riverside Police and Fire Department caused one year’s worth of data to be lost, the second attack only caused eight hours to go missing. Since the first attack backups were in place to prevent a mass data loss. For the eight hours that were lost, all were accounted for and manually entered.
2.3 CASE 4 – [MITIGATING INSIDER SABOTAGE]

**Organization:** General Hospital

**Scenario:** In 2009, “General Hospital” reported 21,000 of the hospital’s Accounts Payable bills were deleted from hospital computers without permission. There were no backups available. This cost the hospital $30,000 in data recovery fees, not to mention unspoken “man-hours” used by staff members.

Employees could work at the office on weekends, but they were to sign into the building log and call the guard ahead of time. The responding patrol officer would inspect the requesting employee’s identification card and if it were valid, the employee would then be granted access and the doors would be locked behind the employee. To exit the building, the dispatcher needed to be called again, a patrol officer would respond back, open the building and lock it immediately after an employee exited. Calls to the dispatcher were digitally recorded and archived daily. There was no Caller ID information available for the recorded line.

The security supervisor stated that he reviewed the dispatcher call archives for the Sunday in question and found three calls for the day. The first was a female requesting access to the building, which housed the Accounts Payable department. The second was the same female requesting to be given access to the building. Finally, the third call was a request from the same female, to be let out of the building. He interviewed the security officer who responded to the requests. The security officer stated that he knew the employee in question and knew she worked in the building, he gave her access into the building.

**Attackers and motivation:** The files were deleted by a disgruntled employee who was fired for belligerent behavior. The employee worked there for two years, during 2008 she had regular falling outs with one employee. They would fight and argue on a regular basis. Upon the supervisor confronting the employee, she became belligerent, started cursing at everyone and refusing to get back to work. She was fired later that day. The supervisor requested her badge, the employee insisted she left her badge at home. Her supervisor instructed she would not receive her final paycheck until it was returned.

**Techniques used:** Being an employee at the company for 2 years, the employee knew the procedures for working on the weekends and knew that the security guards would let her into the building.

**Prevention:** Since the building had no security cameras and didn’t check her badge, the employee was able to get inside easily. Physical security is the first countermeasure against threats. Badge checks, security cameras, and two factor authentication are common security practices.

**Business impact:** This cost the hospital $30,000 in data recovery fees, not to mention unspoken “man-hours” used by staff members.
2.4 CASE 5 – [INSIDE A PHISH]

Organization: GIAC Bank

Scenario: A phish is a fake email that convinces victims to click on a compromised website. The purpose of a phish is to acquire personal information from the victim to then use this information to get restricted access.

An attacker attempts to phish victims for bank account credentials. The attacker creates a dummy email with what look like legitimate information from the bank, the logo, their motto, and even signed by a bank manager. The attacker uses a compromised webserver to host their site. When a victim clicks on the link they will be brought to the site and asked to enter credentials. Those credentials are stored on the compromised server, where the attacker can access them.

The attack took place Sunday morning where banks were closed and would limit response time. After the emails were sent out, a couple of recipients of the phish forwards it to the bank. The bank has a response team in place in case of phishing attempts. The bank can get access to the compromised webserver and identify where the user’s credentials are being stored. They set up a team to look over the accounts and freeze every 30 mins. Their marketing team sent notices to compromised users and alerted current clientele about the phishing ploy.

Attackers and motivation: The attacker’s motivation in this instance were financial gain. However, attackers can target what seem like insignificant sites, but if you use the same credentials for an insignificant site as you do a significant site both are compromised.

Techniques used: There a couple of things an attacker needs to be able to send out a phish. The attacker needs email addresses of victims that could fall for clicking on the link. The attacker will set up a dummy email, a compromised web server, and the fake site. The attacker might use a sense of urgency to get victims to click on links, “You have one day to verify your account information before your account will be suspended.” The attacker could make the email and website look legitimate.

Preventions: Train employees not to click on any suspicious emails or links. Setup protocols in place for when an employee receives a suspicious email. Whitelisting email domains can further prevent phishing emails.

Business impact: The bank was able to close accounts that were compromised every 30 mins. However, the bank had to finance the team to work round the clock until the site was shutdown.
3  TASK 3 – WORKSHOP AND REFINEMENT OF BASELINE MATERIALS

Post-Workshop Refinement. Based on the workshop outcomes and respective feedback, update and refine the baseline materials developed in Tasks 1 and 2. Proceedings documenting the Stakeholder Workshop will be developed by FPRF and published on the FPRF website

Summary – A workshop was held online on 26 January 2021 and 02 February 2021 to review vulnerabilities and best practices with stakeholders.

Agenda for discussion:

- General speakers session / keynote
- Breakout rooms on threats and vulnerabilities
- Brief review of breakout room discussions

Workshop Goal and Objectives: The goal of the workshop was to engage with industry stakeholders to assess the cybersecurity threats of built-in fire protection systems connected to BCS, IoT, and other potentially Internet-facing platforms, and identify knowledge gaps and next steps.

The discussions in the workshops orbited the following central questions:

- What are some known vulnerabilities when it comes to life safety systems and how can they be mitigated?
- What are the insider threats when it comes to life safety systems and how can they be reduced?
- What should be added or corrected to improve the current codes and standards that would further benefit Fire Protection Systems with regards to cybersecurity?
- What additional knowledge and trainings gaps are there in terms of cybersecurity of life safety systems? How can these gaps be minimized?

The following organizations participated in the workshops. These groups represent a broad range of stakeholders as outlined in in section 1.2.

Manufacturers and Installers included:

Owners and Authorities included:
Ford Motor Company, USAF, Amazon, Marriott, Ikea, USACE, DLA, USACE, UL, Procter and Gamble, Office of Under Secretary of Defense, as well as representatives from dozens of state and local Fire and Life Safety organizations.

Also represented were health and property insurance companies, whose interests align with safer and more secure building operations.
4 TASK 4 – GAP ANALYSIS

4.0 KNOWLEDGE GAPS AND EXISTING GUIDANCE ANALYSIS

Identify knowledge gaps and assess the appropriateness of the existing provisions and guidance related to cybersecurity for fire protection systems.

Configuration –

- Interconnection of external systems (call centers, service providers) could allow for unauthorized activity if those external systems are not secure.
- Legacy systems (auto dialers, modems) connected to the public telephone network that can be discovered by war dialers.
- Interconnection with other building systems with no access/restriction to prevent unintended communications.
- If one interconnected system is compromised and life safety is connected, it would be safe to assume that all are compromised.

Implementation –

- Systems that have remote access for maintenance or monitoring could introduce vulnerabilities if not properly implemented.
- Using secure gateways and configuring devices with only the necessary communication mechanisms can reduce exposure.
- The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.

Physical –

- Lack of physical access controls to maintenance or configuration jacks/ports.
  - Use barriers (i.e. fences, walls, locks, etc.) to discourage an attack or to delay intruders. Make sure delay time is longer than response time.
  - Implement detection controls to identify an intrusion as quickly as possible.

Policy –

- Lack of device inventory, network drawings, and configuration.
- Lack of authentication / password management.
- Lack of training and maintenance responsibility.
- Failing to maintain an accurate hardware/software/interconnection documentation.
- Lack of supply chain and support requirements.
- Requirements to integrate with subsystems or 3rd party services.
- Need for authenticator (username/password) policy and sustainment processes.

Security –

- Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable to highly sophisticated arson (terrorist) attacks, industrial espionage, and insider threats. Because of this, it is becoming more difficult to defend against these attacks and new solutions need to be implemented in order to prevent.

Access –

- Weak logical and physical access to 3rd party networks and systems.
- Easy to implant hardware or software devices into environment.
Awareness/Training –

- Many people do not understand the risks associated with a lack of training and what the impacts truly are.
- Some people do not understand what the relevance of having a secure FACP provides.
- What is the true impact of an FACP compromise?

Pertaining to cybersecurity, the people that work in fire alarm and life safety are by no means cybersecurity people, however, the code is vague when it says that “qualified” personnel should operate and maintain fire alarm equipment. The concept of qualified should now universally include at least basics from the cybersecurity domain: usually qualified is satisfied by manufacturer certification, so a way to minimize this is to make part of manufacturer training curriculum the cybersecurity aspect.
4.1 FUTURE RESEARCH NEEDS FOR CYBERSECURITY OF FIRE PROTECTION SYSTEMS

Identify and prioritize future research/information needs for cybersecurity of fire protection systems.

Future research challenges must be assessed and addressed early in the cybersecurity space, fire protection, facilities management, code enforcement, and manufacturing fields. While not all cases are the same, some challenges can have an increased risk to the system in the long run, while others may require immediate attention to mitigate. Incorporating cybersecurity policies and procedures during a systems development phase can help reduce these risks and lead to a good life cycle development, as well as reduce cost, and improve the overall system performance and reliability.

Future Research Topics:

- Security, scalability, and usability must be accounted for during system design.
  - Wired vs Wireless
  - Closed systems versus systems exposed to the public internet or enterprise network segments unrelated to fire protection systems.
  - What type of equipment will be used?
    - How long will this equipment last/how often will it need to be maintained?
    - Impact of jurisdictional Approved Product Lists.
  - Restrictions on physical access prevent equipment tampering, data breaches, and deter malicious actors.
  - Remote access vulnerabilities leading to breach and exploitation.
  - Vendor Validation protects the organization from faulty equipment, fraudulent vendors, and validates existing vendors.

- Ports, Protocols, and Services Management should be implemented to secure enterprise network and systems.

- Implementing Role-Based Access Controls (RBAC) is a common security practice that creates separation of duties. (i.e. Preventing entry level personnel to access admin level controls)

- Security configuration guides should be used and followed to maintain and secure systems.

- Continuous Monitoring facilitates enterprise awareness of security events, incidents, and deviation from security baselines of networks and systems.
  - Threat detection allows organizations to identify and react to critical threats.
  - Vulnerability management identifies and remediates or mitigates high-risk vulnerabilities.
  - Patch Management provides updates to system security baselines.

- Enterprise Awareness & Training facilitates user behaviors that enhance organizational security policies and procedures.
  - Properly designed, implemented, and enforced roles and responsibilities prevent unauthorized access to privileged information or systems.
  - Policies and Procedures should exist to define requirements and operational activities to secure, protect, and monitor systems.
o Insider threat awareness training makes organizational personnel aware of key indicators of malicious activity.

- What are the impacts of cross-functional systems integration?
  
o Fire protection, life safety, physical access control, CCTV, HVAC, lighting, or other building automation systems (BAS).
  
o Can we implement multiple BAS? What policies need to be put in place? How will we integrate these systems?
  
o If one system is compromised, how can we reduce the risk to other connected systems?
4.2 ROADMAP TO ADDRESS CYBERSECURITY CHALLENGES IN FIRE PROTECTION SYSTEMS

*Develop a roadmap to address the cybersecurity challenges associated with fire protection systems.*

In order to further develop, additional workshops can be leveraged to identify more in-depth guidance, tools, codes and standards, and training for risk assessment and an integrated approach with cybersecurity guidance, collaboration, and engagement with stakeholders. During these workshops, we can also discuss how we can provide training to the workforce on cybersecurity basics and encourage stakeholders to create a standardized inventory of their system components. This will help identify and reduce risks as well as assist in developing proper policies and procedures that can be implemented into our best practices.

We can start by identifying the easiest victories and implementing changes to correct deficiencies. If a system is interconnected with enterprise networks, segregate those networks. If a system has internet connectivity, but does not need it, disable that internet connection. Alternatively, if a system does need internet connectivity, use the principle of least functionality to disable all communications features (ports/protocols/services) that are not required for system functionality, or use firewall rules to limit connectivity to specific time blocks.

Organizations can benefit from threat vulnerability risk analyses; these reports are provided by cybersecurity firms who evaluate the security posture of a network.
5 INFORMATION REFERENCES

“Siegeware and BAS Attacks, an Emerging Threat.” *MSSP Alert*, 3 Dec. 2019,

“Cyber Vulnerabilities in Fire Alarm Panels.” *AlphaGuardian Networks*, 3 July 2017,
https://www.alphaguardian.net/cyber-vulnerabilities-fire-alarm-panels/.


“Cybersecurity Capability Maturity Model (C2M2) Program.” *Energy.Gov*,

doi:https://doi.org/10.6028/NIST.SP.800-82r2.

*The State of Industrial Cybersecurity 2020 | Kaspersky ICS CERT*.

“Why Fire Safety Is Increasingly Reliant on Cybersecurity - Invicta Durasteel.” *Durasteel*,