RESEARCH FOUNDATION

RESEARCH FOR THE NFPA MISSION

PROJECT PROSPECTUS

Cybersecurity for Fire Protection Systems

10 December 2019

Background: 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.

Research Goal: 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.

Project Tasks: The research goal shall be achieved through the following tasks, which will be conducted under the auspices of the Research Foundation in accordance with Foundation Policies and will be guided by a Project Technical Panel of industry stakeholders:

Task 1: Literature Review**.**

- Provide an overview of all applicable Codes, Standards, Best Practices, Guides, etc. that deal with subjects with potential cyber vulnerabilities.
- Identify the key stakeholders, their activities, and other attributes.
- Identify common terminology applicable to cybersecurity in fire protection applications.
- 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.
- Identify and categorize existing prevention and intervention strategies to address identified threats.

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.

Task 3: Workshop and refinement of baseline materials. The baseline materials developed in Tasks 1 and 2 will be further discussed, refined, and evaluated at three phases of the project: (1) Pre-Workshop, (2) During the Workshop, and (3) Post-Workshop.

a) Pre-Workshop Review. All baseline materials developed in Tasks 1 and 2 shall be documented and developed into a draft report and summarized in a PowerPoint presentation to be presented at

the Stakeholder Workshop. These baseline materials shall be reviewed by the Project Technical Panel (PTP) via conference call in preparation for the Stakeholder Workshop. Any feedback received from the PTP shall be modified or further refined prior to the stakeholder workshop.

b) Workshop Implementation. FPRF will plan and host a face-to-face workshop which will seek to clarify, confirm, add or refine detailed information and deep insight based on the field experience associated with cybersecurity issues within fire protection systems. The baseline materials developed in Tasks 1 and 2 will be further evaluated, discussed, and refined during the Stakeholder Workshop, in addition to key issues, challenges, or knowledge gaps regarding cybersecurity of fire protection systems.

   The logistical details for the workshop including identifying and coordinating attendees, the workshop venue, and overall workshop facilitation will be directly handled by FPRF. The project contractor shall present the findings from Task 2 at the Stakeholder Workshop and participate in Workshop discussion.

c) 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.

Task 4: Gap Analysis.

- Identify knowledge gaps and assess the appropriateness of the existing provisions and guidance related to cybersecurity for fire protection systems.
- Identify and prioritize future research/information needs for cybersecurity of fire protection systems.
- Develop a roadmap to address the cybersecurity challenges associated with fire protection systems.

Implementation: This eight-month research program will be conducted under the auspices of the Research Foundation in accordance with Foundation Policies and will be guided by a Project Technical Panel who will provide input to the project, recommend contractor selection, review periodic reports of progress and research results, and review the final project report.

About us:

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.