Protection against Modern Hazards and Threats to our Safety Systems

Victoria Hutchison
Fire Protection Research Foundation, Quincy, MA, USA

Abstract

The Fire Protection Research Foundation conducts a variety of research projects relating to fire protection systems. This paper covers findings of two distinct hazards in our modern world: 1) the impact of material changes on modern vehicle hazards in parking structures and 2) the cyber vulnerabilities of fire protection systems.

Vehicles have changed significantly over the years. Modern vehicles present new hazards due to the incorporation of larger quantities of combustible materials (e.g., fuels, plastics, synthetic materials, etc.) into their designs. As alternative fuel vehicles are popularized, concerns regarding their unique hazards, burn characteristics, and typical burn duration have been raised. Compared to older vehicles, modern vehicles burn differently. Modern parking structures have optimized space requirements for vehicle parking and storage and often implement automated retrieval features and car stacking, which presents unique hazards as well. Thus, it raises the question if the safety infrastructure of these parking structures and vehicle carriers have kept pace.

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.

Keywords: modern vehicles, parking garages, sprinkler protection, cybersecurity, vulnerabilities, fire protection systems

Part 1: Modern Vehicle Hazards in Parking Structures

Introduction

Fires in vehicles are not uncommon. In fact, 17 % of the 1.3 million fires reported to US fire departments involve vehicles, with most of these incidents occurring along the roadway or following a collision [1, 2]. While parking structures developing into large, out of control events have historically been rare, they are on the uptick, as evidenced by the recent fires at Liverpool's Echo Arena (UK) and at the Stavanger Airport (Norway) which involved hundreds of vehicles and resulted in severe structural damage. These incidents have raised concern regarding the probability of a single vehicle fire developing into conflagrations in a parking garage setting.

This study details the current state of knowledge of the hazards posed by modern vehicles in parking structures and marine vessels to inform and evaluate the appropriate protection requirements.

Changes in parking garage and vehicle design

The parking industry is undergoing change due to the sheer volume of vehicles today and the resultant demand for parking solutions. Since land is immensely value in densely populated areas, the area afforded to each vehicle has, on average, been reduced from approximately 30 m^2 (322 ft^2) to 18.5 m^2 (200 ft^2), with the width being around 3 m (~10 ft) [4]. Stackable garage configurations are now experiencing rapid advancement and cost reductions. As a result, these automated and mechanized garages continue to gain popularity. Beyond construction changes, many garages are also integrating electric charging stations and photovoltaic systems into their designs – which presents additional hazards.

Global efficiency goals have pushed automotive manufacturers to make vehicles more affordable, safer, lighter, and more fuel efficient [5]. As a result, the amount of plastics by weight used in vehicle construction, for both external and internal materials has increased by 91 % since 1970 [3]. Many parts that were historically metal, cast-iron, or aluminum, are now made of plastics or fiberglass. Modern vehicles today are generally larger than legacy vehicles and have experienced an overall increase in average curb weight over the years, despite the large increase in plastics. The impact of the quantity of plastics is most apparent in the total fuel load of the average vehicle.

Impact on Fire Behavior and Hazard

Despite the increase in fuel load, available literature and fire testing indicates relatively constant heat release rates (HRR) and burn durations for vehicle fires over the past few decades (a HRR in excess 7 MW was found among every decade of vehicles examined) [3]. Alternative fuel vehicles now account for a growing portion of the world's vehicle fleet.

From the limited testing available, these vehicles do not necessarily yield larger fires when compared to traditional internal combustion engine vehicles, however, they do present different burn characteristics and unique hazards [3].

The changes in materials and vehicle design are driving easier ignition and faster flame spread within the vehicle and to neighboring vehicles.

Although there is limited test data available on fire spread between multiple new vehicles, older tests of multiple vehicles have shown fire spread from one vehicle to another on the order of 10 to 20 minutes in a parking garage configuration. Plastic fuel tanks, popular in most vehicles today, can be another contributor to rapid fire spread, as a two-to-five-minute fire exposure can initiate a fuel leak, creating a flammable liquids fire [3].

As more vehicles become involved, the prolonged high-temperature exposures on the load-bearing structural elements can threaten the integrity of the structure. Concrete can begin to spall when its internal temperature exceeds 374 °C (705 °F). This can create large penetrations in the floor, and enable vertical fire spread throughout the garage. The ceiling level temperatures experienced from a large quantity of modern vehicles burning, can also cause structural steel to fail, once its critical thermal threshold of 538 °C (1000 °F) is exceeded. This thermal exposure can reduce the load bearing capacity of the steel to approximately 50 %, increasing the probability of structural collapse [3].

Regulatory requirements

The existing regulatory provisions for open and enclosed garages were assessed with respect to the hazards posed by modern vehicles.

For enclosed parking garages, the existing sprinkler protection requirements appear adequate for controlling a vehicle fire until the fire service arrives on-scene. This is based on fire loss data for enclosed garages where a sprinkler was present and activated, and limited.

This study found open parking structures to be the main area of concern for fires involving modern vehicles - due to their high probability of rapid fire spread. Fire and building codes have historically not required active protection systems in open parking structures. But since the trends indicate that devastating fires in parking structures could become more common, some regulatory bodies now require sprinklers protection in open garages, under certain conditions. Design and installation standards, however, are still lacking guidance on what the appropriate protection should be.

Conclusion

While the total energy released from fires has not changed dramatically over the years, there has been significant change in fire behavior. The time for a single vehicle fire to spread to adjacent vehicles continues to lessen. Understanding fire spread between vehicles in a parking garage setting is critically important. Fire spread from the first to the second and third vehicles are critical for determining the extent of fire spread, timeline, and the ability of the fire service to control and extinguish it. Full-scale testing with a range of configurations is needed to evaluate the spread dynamics and critical parameters [3]. Data on vehicles that are representative of what is on the roads today is necessary to provide regulatory bodies with the information needed to develop guidance to protect against this hazard.

Acknowledgements

Special thanks go to NFPA and SFPE Foundation and all the project technical panelists. Without their financial and technical support, the project would not have been possible.

References

[1] Ahrens, M. (2020). *Vehicle Fires.* Quincy: National Fire Protection Association.

[2] Ahrens, M., & Evarts, B. (2020). *Fire Loss in the United States During 2019.* Quincy: Naitonal Fire Protection Association.

[3] Boehmer, H., Klassen, M., & Olenick, S. (2020). *Modern Vehicle Hazards in Parking Structures and Vehicle Carriers.* Quincy: Fire Protection Research Foundation.

[4] Ison, S., & Mulley, C. (2014). Parking Issues and Policies. *Transport and Sustainability, Volume 5*.

[5] NHTSA. (2020). Corporate Average Fuel Economy Standards. Washington, DC , United States.

Part 2: Cybersecurity for Fire Protection Systems

Introduction

As a result of the digital transformation underway today, cyber criminals have stepped up their efforts to steal valuable information or threaten the delivery of essential services. While fire and life safety systems used to be standalone systems, today, Building Control Systems (BCS) are connected to other systems like double-interlock pre-action, special hazards, smoke control, bi-directional amplification, building automation, access, CCTV security systems, and other internet-connected devices.

As fire protection systems are increasingly networked to platforms that are, by design or oversight, exposed to the public-facing internet, they are exposed to more cyber risks. This emerging environment leads to unique and novel cyber vulnerabilities, and attacks on fire protection systems have the potential to have significant consequences. Vulnerabilities, defined as a hole or weakness in an application, hardware component, or network that allows an attacker to cause harm or command a system or component to act in an unauthorized manner [1].

Attack Surfaces for Fire, Life Safety, and other connected systems

With an increase in functionality and connectivity comes an increase in cyber risks. All the available aspects of the system which are vulnerable to an attacker are known as the threat surface. As fire and life safety control systems are interconnected with outside networks, the threat surface is increased. The most vulnerable system components are the head-end units (typically servers), as these systems are often exposed to both IT (Information Technology) and OT (Operational Technology) networks [1].

The network perimeter is where the fire alarm system connects to other networks, systems, or more generally shares data with another system. These points, known as “points of connection” and are often particularly vulnerable, and as a result are commonly targeted by threat actors. The areas where the fire alarm system touches IP pathways, or has any connection or port where an individual could connect into the system with a laptop or other device and cause harm, need to be secured in their respective hardware, firmware, software and/or with physical access controls [1].

To expose software, hardware, connectivity, security or human vulnerabilities, attacks on fire safety systems can be categorized into three types of cross-domain hazards: cyber-physical hazards, socio-cyber hazards, and socio-physical hazards [5].

A few examples of these hazards and attack methods include:

- **Radio frequency jamming** – a type of denial of service (DoS) attack when an adversary can introduce a powerful radio frequency signal to overwhelm the system and block the wireless communication between different components to interfere with data transmission. In the case of fire, this attack could cause the sensor to be unable to communicate the detection of the fire [6].
- **Remote code execution (RCE)** is when an adversary is able to gain access to a computing device remotely, execute malicious code, make changes, and take control with administrative privileges [4].
- **Theft** is when an adversary performs a theft operation, digitial or physical, to gain access to a building system.

- **Man-in-the-middle** attack is when an adversary intercepts the exchange between systems, pretends to be the original sender and implements an attack while tricking the recipient into believing they are still receiving a legitimate message from the original sender [2].

- **Physical Infestation** is physically accessing the building (e.g., such as by tailgating another person into the building. Once inside, they can execute the attack.

- **Social Engineering** is when an attacker utilizes human interaction or social skills to obtain confidential information about an organization or its systems. By the attacker pretending to be someone else and asking the right questions, they can often obtain enough information to infiltrate the organization's networks [3].

Cyber-attacks directly on fire safety systems or indirectly through connected systems can result in loss of communications, false alarms, denial of service, and overheating of equipment which may cause distrust of fire protection systems, cause systems to not operating as intended, or to prevent sensors from detecting fires or recognizing ignition in physical pieces of equipment.

Protection

In the presence of all these threats to our fire and life safety systems, it is important to implement security controls and mitigation strategies to reduce the attack surface by applying safeguards. Below is a partial list of strategies that will reduce the probability of cyberattacks in fire and life safety systems [1]:

1) **Network segmentation** - Segmentation divides a computer network into smaller parts. While the purpose is to improve network performance and security, segmentation improves cybersecurity by limiting how far an attack can spread. For example, segmentation keeps a malware outbreak in one section from affecting systems in another.

2) **Update Malware/virus protection** - Keeping technology up to date with appropriate protection against malware and viruses is critical for reducing cyber risks. A disadvantage of stand-alone fire, life safety, and building systems is that the software security, virus, and malware protection is rarely updated unless there is a software maintenance agreement in place. Therefore, these systems are more vulnerable to attack from new viruses and malware. Since, most fire, life safety, and building systems personnel are not IT technicians, these systems are often excluded from the updates that occur on other IT systems.

3) **Training –** To protect critical systems, workforce awareness and training is crucial. The key stakeholders must be aware of vulnerabilities introduced as systems become more interconnected and their role in reducing the threats. Many threats, such as phishing, piggybacking, and data theft, exploit human behaviors. But a well-trained workforce can implement and execute common cybersecurity best practices.

4) **Disabling insecure and unused protocols** reduces the attack surface and in-turn the cyber risks.

5) **Change Default Passwords -** Cyber criminals use passwords to prey on weaknesses. To slow or deter cyber-attacks on fire alarm systems, change the admin level password. Out-of-the-box admin passwords are commonly used, but not changing it creates one of the easiest points of entry for an attack.

6) **Manage Permissions**

   - **Disable guest accounts** – By disabling guest accounts, permissions can be better managed, reducing the attack surface.

   - **Manage permissions for programming changes** - Updating passwords also increases system security and forces technicians to request permission for programming changes. This ensures all programming requests and functions impacted by the changes are tested, verified, and documented through a change management process, as required in NFPA 72.

   - **Manage access -** Another way to reduce cyber risks in a facility is through proactive access management. When employees or vendors' employees leave a company, terminate their access to systems.

7) **Firewalls** – Firewalls provide enhanced IT security to protect your technology from attack, blocking unauthorized access while still allowing legitimate users access to the systems and data necessary to perform their jobs.

8) **Baselining** – Creating a baseline of network behavior can help improve the security stance of the organization or network, by being able to identify abnormal behavior.

9) **The principle of least privilege** recommends that users, systems, and processes only have access to resources (networks, systems, and files) that are necessary to perform their assigned function. This reduces the attack surface.

10) **Threat, Vulnerability and Risk Assessments** – can be conducted to assess an organization's need to protect their respective assets and minimize cybercrime and security breaches. This assessment starts by identifying plausible threats. Based on these threats, the facility's vulnerability to the attacks and the potential impact and downtime from them is further assessed. The risk of the identified threats can then be classified by a combined assessment of the impact of the loss and the facility's vulnerability. This information can be used to inform a customized cybersecurity strategy for the facility or organization, based on the identified risks.

Acknowledgements

Special thanks go to the American Society for Healthcare Engineering, Telgian, Procter and Gamble and NFPA, without their financial support the project would not have been possible.

References

[1] Chevreaux, J., Owen, P., Donaldson, K., Bright, K., Largen, A., Meiselman, D., . . . Uribe, A. (2021). *Cybersecurity for Fire Protection Systems.* Quincy: Fire Protection Research Foundation.

[2] Chivers, K. (2020, March 26). What is a man-in-the-middle attack? Retrieved from https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

[3] Cybersecurity and Infrastructure Security Agency (CISA). (2020, August 25). Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks. Washington, DC, United States.

[4] Driz, S. E. (2018, June 16). What is Remote Code Execution Attack and How to Prevent this Type of Cyberattack.

[5] Kalluri, B., Kivac, A., & Rosenqvist, H. (2020). *A Taxonomy for Cross-Domain Fire Hazards in Buildings.* Singapore: Research Publishing.

[6] Scarfone, K., Tibbs, C., & Sexton, M. (2010). *NIST Special Publication 800-127: Guide to Securing WiMAX Wireless Communication.* Gaithersburg: National Institute of Standards and Technology.