Security Practices & Engineering Concepts

COURSE II. LOCKING ARRANGEMENTS & FIRE CODE COMPLIANCE FOR ENGINEERS AND ARCHITECTS

by

Charles Schnabolk P.E.
LOCKING ARRANGEMENTS & CODE COMPLIANCE FOR ENGINEERS AND ARCHITECTS

Introduction
An extensive review is provided here of the history and changes that have transformed lock and cylinder hardware, from the ancient skeleton key to Linus Yale’s pin-tumbler invention (patented in 1861) to card readers (1970s), pushbuttons (1980s) and the smartphone wireless entry systems (2016). Yale’s invention made duplicating keys easy and created the locksmithing industry that lasted for over a century until the introduction of access control systems and the availability of locking hardware at box stores like Home Depot. The friendly neighborhood locksmith who hasn’t adapted has become as irrelevant as a blacksmith and TV repairman. Access control systems, both wireless and hard-wired, are rarely found in a locksmith shop since most locking arrangements now require a thorough knowledge of digital technology and some understanding of code compliance. Gaining a working knowledge of both new technology and compliance codes should be part of the education of the engineering and architectural professions in this age of homeland security concerns and terrorism threats.

The traditional practice of selecting locking hardware can no longer be limited to counting the number of doors in a building and ordering twice that number in hinges and using the lock manufacturers catalog to select a nice-looking lock is not acceptable. (Prior to 9/11 some architects acted as if they considered door knobs a nuisance since they destroyed the clean lines of the hallway is an attitude that can no longer be tolerated).

This PDH course describes important advances in lock technology:
- Upgrading lock hardware
- Special lock arrangements
- Push button shortcomings
- Electrified locks
- Electromagnetic locks
- Smoke Detectors

Code Compliance: National Fire Prevention Association & Underwriters Laboratory

- Details on the controversial electromagnetic lock and its effect on the National Fire Prevention Association (NFPA) Life Safety Code 101 and its slow exceptions by local fire departments is explained. Installing fail-safe electromagnetic locks on fire exit doors are accepted as being in-compliance with amended national codes and local regulations, but far too many architects still believe that locking fire exits to be a violation of basic building codes that had always mandated that fire exit doors allow egress at all times. The electromagnetic lock, when properly connected to an existing and approved building fire alarm system, will prevent egress unless a fire condition activates the fire alarm system… and its legal in most jurisdictions.

- Lock Picking: Less expensive locks are easier to pick since they are not manufactured within the tolerance of one millionth of an inch as found in finer made items like watches. If locks were manufactured to closer tolerances, the cost of each lock would be so prohibitive that it would be no unmarketable. To keep prices as inexpensive as possible, the average lock is produced with a relatively loose set of tolerances, making it easier to pick. Lock picking techniques are described.
CHAPTER ONE

LOCKING HARDWARE

A. FADING TRADITIONAL LOCKSMITH TRADE

The neighborhood locksmith who hasn’t adapted is following in the tracks of other outdated occupations that have been replaced by new technology. The key-making locksmith trade began to ebb with arrival of card access technology and the fact that Home Depot has a locksmith section stocking more components than the average locksmith store. Key grinders and lock pickers, as locksmiths are sometimes referred to, are slowly becoming as rare as the elevator operator, the toll taker, and the typewriter repairmen. Since major hardware retail outlets started to carry a full array of lock hardware, the local locksmith’s market share has declined but the locksmiths will remain in business as long as people keep losing their keys. These mostly small, self-employed mechanics are often not qualified to install or program any device more complicated than a mechanical lock.

It is not well known, but all locksmiths must not only have a license from the community in which they are working; they are also supposed to follow a code of conduct spelled out in the Baldomeric Oath. The oath is named after St. Baldomerus, the patron saint of locksmiths, who died in the 7th century. Here is an excerpt from the oath, which few locksmiths seem to take seriously and can, on occasion, cause all kinds of problems for those that do so while working in a municipal agency: “That I will maintain this sacred trust, holding myself far aloof from wrong, from corruption, from tempting of others to vice.”

Problem: a well-intentioned locksmith was reported in the newspaper as telling authorities at a city-owned hospital that he was getting overtime pay when he was only working the 40 hours required. It seems that after signing in each morning, supervisors were adding extra hours to the length of his work day without his knowledge or approval. He discovered the fraud when he got bigger checks than the amount he expected. Abiding by the Baldomeric Oath, the locksmith reported the discrepancy to his immediate supervisors who informed him that, since all city employees had had their salaries frozen for three years, the overtime was to make up for this injustice.

The locksmith then went to the inspector general - before he was fired.

> In order to embellish their relatively modest incomes, many locksmiths charge an extra $5 to make duplicate keys marked “DO NOT DUPLICATE.”

> Locksmiths have continuously been criticized for breaking the law by making duplicates of master keys that operate elevators in municipalities throughout the nation and then selling them on eBay. Only a select few authorized people are legally allowed to possess these keys: firefighters, elevator contractors, and building owners.
The modern security industry really started after an anti-trust decision broke up the monopoly that controlled the fledgling industry prior to 1970. Until then the only recognized “security specialist” was the local locksmith whose window displayed several door knobs, key chains, and heavy duty locks, but almost never any electronic devices. Many companies and unskilled individuals entered the security business with absolutely no background in it, although they quickly started having an impact.

There were few electronic security installers until the 1970s and 1980s and their only trade shows were locksmith conventions. Such shows are still scheduled every year and the exhibits are usually focused on the newest innovations in key making machines - with no noticeable displays dedicated to the growing electronic security and access control industries. The number of attendees at these lock hardware meetings has remained about the same over the last three decades, while during the same period the alarm detection, CCTV surveillance, biometric, and digital industries experienced a technological revolution and became some of the fastest-growing industries in the America. During this same time, the number of locksmiths fell from 35,000 in 1940 to 15,000 in 2015.

The most noticeable recent advancement in the traditional locksmith industry is the development of locks and their associated hardware that are decorative and more stylish, but still operate with the old pin-tumbler arrangement. New locks are simply variations of the basic designs that go back a century or more. While some locksmiths will install complicated electromagnetic locks and maybe a few card readers, they generally avoid anything that involves “electronic” connections. Locksmiths consider themselves skilled mechanics who install hardware rather than electricians who install card access control systems with software.

Before the Yale cylinder became the standard in the lock hardware industry, a common protection device was a wooden beam mounted across the door, which was removed with a skeleton key. Yale also invented the key duplicating machine in the early 1900s, which was followed by key code books published in the 1920s, a time that locksmith shops became established storefront businesses in many major cities. Some of those early key-making shops are still in operation with 3rd and 4th generation sons running them. Skilled locksmiths continue to work out of storefronts or from trucks, having graduated from a $1,500 correspondence “Lockmithing” school that includes a syllabus that describes how pin tumblers fall into a shear line and how to pick locks for fun and profit. Most schools provide a duplicating key machine as part of their educational course. The locksmith trade grew slowly and eventually became the main provider for premises protection. Locksmiths could be considered pioneers in the years prior to 1970, when the modern-day security industry had its beginning.

A significant majority of the approximately 2,000 correspondence students who enroll in the locksmith courses each year quit once they master the lock picking session, which is usually
offered halfway through the course. Those who don’t finish include many convicts and future felons who are more interested in learning how to pick locks than in finishing the program.

In most municipalities a locksmith is licensed, but if their shop moves to another city within the state it is still legal for them to start cutting car keys and repairing lock hardware immediately (without a license). Every municipality seems to have their own rules; for example, Las Vegas mandates that the locksmith must not only be licensed, but must work out of a store or office (no truck). In general, locksmiths and security alarm installers (integrators) operate in two different and totally unrelated spheres, yet they share three characteristics: (a) very little money is needed to enter the business, (b) no particular talent, skill, experience, or education is required and (c) both trades operate in a mostly unregulated industry.

New York is one of the few states requiring alarm and fire system installers to possess a license that requires experience as well as passing a written test. The objective is to protect the public and institutions against unreliable and criminal firms installing security systems. The idea was to have all government and major organizations place the licensing requirement into any bid package. If the licensee did not perform as promised, their license would be revoked. A license did not guarantee that an installer was competent, but it could possibly prevent a vendor from repeating shoddy work; a problem that is prevalent in the security industry, which has practically no licensing restrictions. Since the law was enacted in 1993, no significant impact has been made in terms of enforcing it.

Locksmith shop owners depend on the public becoming aware of their presence since people rarely seek out a particular locksmith and simply use the most convenient shop. After all, making a duplicate key doesn’t require a specialist, only someone with a key machine. This fact has led to legal action between locksmiths and other enterprising individuals who are constantly finding ways to gain an unfair competitive advantage over competitors such as:

- Stickers are affixed to every door, mailbox, and key slot that unscrupulous marketers can locate. Many places have outlawed this practice and will force the offending company to remove the stickers and clean up the residue left behind.
- Another, subtler tactic that seems more prevalent in the locksmith industry than in any other business in the security field is the alphanumeric manipulation of company names in Yellow Pages listings in order to appear higher up in the listing category. There is nothing illegal or unethical about this particular practice, but it is an example of how names of companies and their directory listing potential are intentionally chosen and factored in to gain a competitive advantage.
- Multiple listings (employing more than one business name) is another method that is legitimate simply because it has been around since the Yellow Pages were invented. There is a purely mathematical advantage to having more than one listing since a potential customer seeking a locksmith from the phone book or Internet search has a greater chance of picking it. With all other variables being equal, the multiple listing doubles the chance of one company being picked over the other.
- With the increased use of the Internet and GPS to find a locksmith come an entirely new hurdle and opportunity for the locksmith industry as the techniques to set them apart
online are quite different. Having an online presence is something that has challenged the old-fashioned locksmith.

Locksmith scams are one example of how the idea of the reliable neighborhood “key-maker” who makes house calls has been subverted by technology. In one scam, people seeking immediate help after being locked out would Google “locksmith.” Their assumption was that the search results would include names and numbers of local locksmiths. Some of the results, however, were actually call centers (often located out of state or even out of the country) that had used a high-tech trick to appear in the Google results. When contacted they would tell the caller that the cost would be $50 or $90, etc. Then when a subcontractor arrived they would extract a payment of hundreds of dollars from their victim.

Small storefronts with a single locksmith may be disappearing, but many locksmiths have been slowly reinventing themselves by going in-house, working as employees of hospitals, school systems, or corporate entities. The freedom of owning a locksmith shop has been traded in for a position that may not pay very much, yet offers more security and other benefits. Almost all major medical centers with over 400 beds have their own locksmith office with one or two skilled locksmiths.

B. OBSOLETE LOCKING ARRANGEMENTS

A security device that was created in the early 1970s, about the same time IBM Selectric typewriters became the standard word processor in every office in the nation, was the typewriter lock. The Selectric sold for over a $1,000 when first introduced and instantly became a prime target for office equipment thieves. Reportedly up to 12 million of these heavy, bulky typewriters were stolen between 1979 and 1982. The various manufacturers of electric typewriters took absolutely no action to protect their units by offering or incorporating some sort of locking system for obvious reasons. Every time a unit was stolen another typewriter was purchased. The lock industry reacted to this problem by introducing a series of rudimentary to innovative locking devices to keep the typewriter from being removed, with questionable success.

The simplest system was to attach a cable to the side chassis of the unit and affix the other end to a drilled hole in the desk. A key was required to release the cable. The cable was inexpensive and discouraged an opportunist amateur thief (usually an employee) from stealing the typewriter. It did little to prevent a professional thief who simply cut the cable and removed the typewriter.

The most innovative and successful typewriter locking system was introduced in the early 1980s. Called the “Anchor Pad,” it used two-way adhesive tape on a bottom plate that was “pasted” to the desk with an upper plate screwed to the bottom of the typewriter base. The two plates were then locked in place and could only be separated by a key.

The only noticeable change was that the typewriter sat on the 2-inch plates instead of directly on the desk. While the adhesive pad and lock may sound a little impractical, it proved to be the most effective locking device for typewriters for almost ten years. While its cost ($125) was triple that of the cable systems, it provided a much more secure arrangement and it did not damage the furniture since it was removed with a heat pad. The major drawback of this unique unit was that
once the bottom adhesive plate was sealed in place, it could not be removed to relocate the typewriter unless a heat lamp was applied to melt the adhesive. The 1980s is now referred to the end of the typewriter age as computers began to make their appearance. The same adhesive technique was tried to protect desktop computers as well as portable laptop units, but it did not sell for very long for two reasons:

- When the adhesive method was used on the desktop model, the thief simply left the terminal and keyboard in place … and stole the unprotected hard drive.
- Laptops became so prevalent partly due to their portability, so the complicated locking arrangement had no practical cost effective value.

Typewriter locks are now hard to find, as are typewriters. In the mid-1980s, the Yellow Pages still listed several pages of advertisements for typewriter repair services. There are no such ads today. In fact, even the Yellow Pages themselves are shrinking and going online, with many cities passing laws that do not allow those thick telephone directories to be left abandoned in apartment building lobbies every year.

Even the Federal Bureau of Investigation has admitted to a serious breach in their security system that resulted in over 160 weapons and 160 laptops lost or stolen during a recent 44-month period. Six of the missing FBI computers were assigned to the Bureau’s Counterintelligence Division. One belonged to the super-secure Counterterrorism Division. According to the Bureau there were many cases where it was unable to determine whether any of the missing computers had contained classified information.

C. UNCONVENTIONAL CONCEPTS

THE CLUB. Sometimes a simple locking concept can become a universal locking standard when promoted properly. A case in point is the phenomenal success of the automotive security mainstay simply named “The Club.” The simple device was a familiar sight on the steering wheel of millions of cars, but was not unique or innovative. The manufacturer of The Club introduced it to the public in 1986 through Sears and then heavily advertised it on very late night television, featuring a policeman touting it and reminding viewers, “I’m not an actor; I’m a policeman.” (The officer later sued The Club manufacturer over his acting contract.) The Club was hardly a novel device - a similar gadget had been patented in 1919 - and other models were already on the market, but by using advertising and a lot of other promotional efforts, The Club manufacturer became a millionaire by cleverly using an old idea. This same approach is often followed by rich politicians who overwhelm their poorer, more qualified opponents by outspending them on television ads.

Law enforcement agencies and product testing groups proved that The Club was easily defeated, either by spraying it with Freon to make it brittle and then cracking it with a hammer blow or by
taking a hacksaw to the steering wheel. Representatives for The Club refuted the criticism by claiming that thieves didn’t carry hacksaws or Freon.

In spite of its weaknesses, over 10 million “Clubs” were sold during its seven-year life heyday.

D. NO-LOCK NEIGHBORHOODS

The thought of small town living always includes the idea of a community that is so safe that people don’t even lock their doors. These homeowners are known as “no lock people” and they also exist in large numbers in most of the nation’s biggest urban centers. Living in a high-rise building with a doorman, in particular, can create an environment where tenants do not always bother to lock their apartment doors. A study by State Farm Insurance reported that fewer than half of those surveyed always locked their front door. While people who habitually lock their doors are incredulous that others do not, those who don’t lock their doors are surprised that anyone would be shocked by the practice.

According to the FBI’s annual Uniform Crime Report, of the estimated 2,222,200 burglaries committed nationwide in an average year since 2009, over 30% were unlawful entries without force. In 2010 the New York City Police Department reported that of the 20,000 burglaries that took place in the city, 5,000 did not involve forced entry. These figures cannot be flatly equated with those that involve unlocked doors as there may have been open windows, unauthorized use of keys, and theft by workers, family members or business associates. Unlocked doors are certainly a factor, however. The perception of big city dwellers needing to install triple locks and metal bars bracing the door - an image common in movies from the 1960s and 1970s - is dramatically out-of-date. In 1980 the NYPD reported 210,000 burglaries in the city, more than ten times the number of burglaries in 2010.

The decision to lock or not lock is not always logical; often it is based entirely on emotion. A person’s conception of safety is not necessarily tied to statistics, but usually it is associated with a false sense of security, like from having a doorman inspecting every visitor. Yet the doorman has access to a duplicate key that is kept at the front desk. Delivery people are only admitted after first calling the tenant, but there is nothing to prevent these individuals trying other doors after making a delivery. Then there is the risk of a member of the maintenance staff who took a correspondence course from a locksmith school that taught lock picking in ten easy lessons.

E. PINS AND CYLINDERS

The common pin-and-tumbler locking mechanism has a series of spring-loaded pins, which are loaded into a series of small cylinders. Each cylinder has a bottom part, called a pin, and a top part called a driver. Upon insertion of the key, the springs will be compressed as the key lifts the pin, pushing the driver into the upper chambers of the cylinder. When the correct key is in the lock, the bottom and top pins align the space between them around a track similar to a ward, which is called the shear line.

When all of the pins and drivers are aligned to clear the way for the shear line, the key will turn. When the key is not in the lock the pins should be at rest in the chamber, with the bottom pin in
the key chamber and the top part of the pin resting on top of the bottom half due to the gentle pressure of the relaxed spring. An incorrect key will misalign one or more of the locking spring-loaded cylinders, blocking the key from turning by placing at least one of the pins or drivers in the way of the shear line.

The side-locking bar technology is vulnerable to lock-bumping attacks. Lock bumping is an increasingly popular lock-picking technique in which an intruder uses a specially cut key to “bump” a lock open using skilled strikes to the key in the lock. Kwikset SmartKey deadbolts and locks feature the patented side-locking bar technology, which is also central to the SmartKey’s ability to be rapidly and easily re-keyed.

A rim lock is a locking device that attaches to the surface of a door, usually on the inside. A small latch is used to unlock the door from within. On the outside of the door there is normally a smaller sized rim with a keyhole.

A mortise lock is a type of lock that requires a pocket - the mortise - to be cut into the door into which the lock case is to be fitted. Mortise locks have two different locking devices built into the lock case: the latch bolt and the deadbolt.
CHAPTER TWO

LOCK PICKING FOR FUN AND PROFIT

A. AN EASY-TO-LEARN PROFITABLE SKILL

Purists in the lock picking field have honed their special skills like brave matadors or golf professionals. The main difference is that bullfighters and golfers take years to perfect their admired abilities, but picking a lock is not that hard to learn. (A significant number of convicts acquire this skill by filing down bed springs to create lock picks and learning a new trade that is shared by everyone on the cellblock.) There are many books written on the subject directed specifically at amateurs as well as at a significant portion of the criminal element. The special tools needed for lock picking are readily attainable from catalogs and seen in ads online just by searching for “lock picking.” Those who take correspondence courses can often use the award certificate they receive upon successfully completing it to obtain a locksmith license from their local municipality.

Picking a lock requires two tools, a picking instrument and a turning wrench (also called a tension wrench). A typical package consisting of 15 rakes (picks) and two wrenches costs about $15 from any of the lock hardware distributors found on the Internet. Locksmith schools are another source of lock picks, as are catalog companies who sell various types of pick sets from $15 to $300. Google “lock picks” for an up-to-date list of suppliers.

Two major suppliers are: HPC [www.hpcworld.com]
   Lockmasters [www.lockmasters.com]

A typical correspondence course for lock picking usually consists of 30 lessons. Some lock hardware is supplied, such as a set of keys, a cylinder, and eventually a key-making machine. Each lesson includes an instruction booklet and a simple 10-question test that requires answers that are returned to the school with a check as partial payment. The test is graded and returned along with the next lesson package and so on until the course is completed. As long as the check clears no one has been known to fail any of the tests.

The most popular lesson is #18, which includes the lock picking instruction booklet that is accompanied by the “picks.” After mastering that lesson and practicing for an hour or two, the average student can pick 90% of all the locks in their community, including nearby retail stores.

The pins are in a position that prevents the turning of the cylinder.

Once the key is inserted and the cuts in, the key pushes up the pins into the “shear” and the cylinder will turn to unlock the door.
When following instructions for the lock picking lesson, the student is given a lock or cylinder that comes with five pins. The student removes four of the pins and practices the fine art of lock picking by using the picks or rakes and a turning wrench on a cylinder with only one pin. The idea is to move that single pin up and down continually until the pin falls into a “shear line,” allowing the tension tool to turn the cylinder into the unlocked position. After mastering the one pin exercise, the student will dismantle the cylinder and insert two chambers with pins and springs and then practice raising the pins, once again, to the shear line. By adding one pin at a time the student can slowly build up his or her confidence to pick the full five-cylinder arrangement and become a full-blown lock picker.

A cutaway view of the cylinder plug section side will show that none of the pins in a typical cylinder is in exact alignment because, no matter how carefully a manufacturer drills the holes in a plug, they never line up perfectly. The cheaper the lock is, the greater the misalignment. The loose tolerance measurement is why it easy to raise one pin at a time to the very critical shear line. When a pin reaches the shear line, the plug holding all the pins can be turned ever so slightly by applying pressure on the wrench. Continuing to raise one pin a time to the shear line allows the plug to turn, which is a feeling that a lock picker can actually recognize with repeated practice. The movement can be as slight as two thousandths of an inch to get the pin in position.

Locksmiths must know how to pick locks because customers lose their keys, but professional thieves use their lock picking skills to rob premises and to steal cars. After a place has been robbed, and it suspected that the robber used a pick to enter the premises, the police detective takes apart the lock and examines the cylinder to check for any scratches on the pins indicating a pick was used rather than the proper key. If there are no scratches the robbery is considered an “inside” job by someone with a key.

- **Picks:** Come in many shapes to conform with the type of cylinder in the locking hardware. Designed to manipulate the pins inside the cylinder to align them with the shear line, which allows the turning of the cylinder, unlocking the door.

- **Turning Tool:** Used to rotate the lock mechanism’s cylinder. Many crime scenes in movies and TV shows misinform the viewing public by showing a police officer or bad guy picking a lock with a single tool.

The pick and turning tool simulate the shape of a standard key. Picks are used to simulate the pins in the lock cylinder being moved by the cuts in the front section of the metal key. The turning tool simply acts as the rear section of the key that is held by the thumb and first finger and used to rotate the cylinder by applying torsion. After the picks get the pins aligned along the shear line, the cylinder will rotate. The illustration shows that the cuts in the key move the pins into the shear line, which must be duplicated by the pick.

Sometimes the close positioning of the turning wrench and the pick can cause “crowding” within the cylinder keyway, preventing the pick from working freely. Placing the wrench on the top edge of the keyway may prove to be more successful than using it at the conventional lower
To become more proficient, some lock picking instruction manuals suggest that after getting the five-cylinder plug to align with the shear line, that the student try to use this new skill by using the picks to open the door at a nearby appliance store at night when the street is deserted. It will be amazing how easy it is to turn the cylinder, even in the dark. In the event the police catch the student in the act the lock picker can try to explain his or her way out of the situation by telling the officer with the drawn gun that there is no robbery. The student was simply doing a homework assignment. Hopefully, the officer will believe the outrageous explanation because if arrested no judge will accept that excuse.

There are a number of different types and styles of picking instruments and turning tools; some are more flexible while others are better for certain cylinders. Purchasing the proper set of picks is much like selecting any household tool. Alternatives to picks and turning tools include:

- **Pick Gun**: An inexpensive picking device that uses a triggering action to rapidly move the pins into a series of positions until the shear line is in alignment. No particular skill is needed except the ability to pull the trigger.

- **Tubular Vending Machine Picks**: Specifically designed to fit into the round opening in the typical vending machine that has the pins set in the rear of the lock cylinder. The tubular lock pick performs the same operation as the conventional lock pick, but instead of moving the pins up and down it moves them back and forth until the shear line is in place.

- **Bumping**: This technique is a rather unskilled method of lock picking since it involves brute force instead of a careful manipulation of pins and shear lines. It is done by simply inserting a filed-down key into a lock cylinder then knocking the key with a hammer to momentarily pop the lock’s pins into an open position. It takes about ten attempts before the cylinder will turn into the open position. The same lock expert that was responsible for the “bump” technique also exposed the Kryptonite bike lock’s vulnerability to a Bic
pen and how to “shimmy” open combination locks. He also published a 300-page book called *Locks, Safes, and Security: An International Police Reference* (1,411 pages; $220) that is considered the bible of the locksmith trade. The same author published a book that details a method to pick the allegedly uncrackable Medeco high security locks.

There are lock picking clubs in over 30 countries dedicated to picking locks for fun. The original club started in Belgium in 1999 and has since spread to other countries, including the U.S. Many clubs belong to The Open Organization of Lockpickers (TOOL), which meets regularly to share secrets and hold an annual competition, a sort of Olympics of lock picking, in different countries. This event has entrants compete in various categories, such as padlocks, mechanical locks, and free style, in which contestants confront a variety of locks with any tools they choose, as long as they do not damage the lock. Of course, some of the scheduled meetings and events have occasionally attracted unwanted visitors (those wanted by the police). Unlike a burglar, who drills into or otherwise damages locks, the club’s members follow a cardinal rule that locks may not be damaged in any way.

**B. PICKING HIGH SECURITY CYLINDERS**

Around 1970 the lock manufacturer Medeco introduced a unique cylinder that revolutionized the industry. The two inventors, who operated a small locksmith shop in Virginia, designed a keyway where the pins had to be twisted as they moved up the tumbler; conventional lock picks could not duplicate this pick-proof feature. A typical lock cylinder is picked by moving the pins in an up and down manner to place them along the shear line and allow the lock to open. Medeco caused a sensation in the industry and further upped their profile by offering anyone $100,000 if they could pick their twist-pin cylinder within an hour. The NYPD’s Chief of Detectives, who was also head of the robbery squad, took up the challenge. He had already made a name for himself in the industry by checking for pick marks in lock cylinders looking for signs of an inside job following a robbery.

The detective picked the Medeco cylinder within 20 minutes and collected the prize money. Two year later he retired to become the vice president of Medeco. No one else duplicated his feat until 2006, when a lock expert who had exposed the “bumping” method and his new partner discovered a method for opening a Medeco lock in about a minute. They then distributed footage demonstrating exactly how to “Pick and Bump” the Medeco cylinder and published a book titled *Open in Thirty Seconds*, which explains how it was done.

**C. SPECIAL LOCKING ARRANGEMENTS**

> **VAULT COMBINATION LOCKS.** Older vault doors were a foot thick and had combination locks that no human could easily defeat. Bank robbers would use dynamite to destroy the locking mechanism and spring the door open. It was a time consuming and dangerous way to rob the vault area. Another method was to circumvent the bank round vault door was to drill up from the floor below and avoid the thick vault door entirely.

> **PUSH BUTTON - DIGIPADS.** The once popular push button pads were introduced into the marketplace to enhance the security of mechanical key locks by adding another level of
protection, or even eliminating the need for a key. They were then gradually phased out as more sophisticated controls became available, but there still remain millions of these numeric keypads attached to door frames (with their highly secret 4-digit codes clearly written on the adjacent door buck). Some of the better push button pads are built into the locking hardware, but most are the standalone variety that are connected to an electrical door strike. Push button models first appeared in the early 1930s and early on enjoyed a relatively small level of success until the card reader access control systems became the most visible door control device by the late 1980s. Push button numerical digipads are available in various shapes and sizes; their only common characteristic is that they can be easily compromised unless combined with a biometric device, like a fingerprint reader. The push button is used in low security situations like bathrooms, closets, and office doors. Many units include the lock and the pad as a single package, which eliminates wiring the coded pads to an electronic or mechanical lock.

Push button units are compromised whenever people share the codes. The 4-digit or 3-digit codes are often shared (voluntarily or inadvertently) by someone memorizing the digits through simple observation. James Bond would have no trouble breaking the code and neither would a coworker. Just waiting for the numbers to show wear over time can narrow down the code possibilities into something easily breakable. Many times the numbers are sequential (like the popular 1-2-3-4) just like the password is actually password. Push buttons mounted on the entrances to hospital ERs are notorious for using 911 as the code.

There have been few significant advances in push button technology, with three notable exceptions:

* Units are available that can be programmed to allow several unrelated codes to trigger the mechanism.
* There are push buttons that retain the numbers used and the time of operation. This stored data can be retrieved with a portable handheld reader unit.
* The most unusual, and by far the most successful, modification to the traditional fixed layout of numbers is a scrambler that automatically and randomly moves the numbers into new positions on the keypad after each use.

> SCRAMBLER push button units created a new level of mechanical technology that not only confused unauthorized individuals who were trained to read codes by standing behind the user, but also confused the very people the system was designed to serve. This innovative device has the standard ten digit buttons on a backlit keyboard. The numbers are never sequenced in the same position. The locations keep scrambling in a random sequence so that anyone looking over the shoulder of a user cannot identify the number by its position. The top three numbers on other keypads are 1-2-3, but on the scrambler keyboard the top three numbers may be 5-9-1. After activation these top numbers may become 5-2-6, etc. As with many inventive security devices, the public needs time to fully accept any new concept. People are so programmed to associate the position on the keyboard with the digit, for example 3 is always on the upper right hand corner, and that automatic association causes confusion when a user now has to read the keypad.
before every use. Eventually, users became accustomed to the system and appreciated the high level of security it offered.

> **OMNI LOCK.** This standalone digipad allows different users to enter a unique PIN for entrance to a secured space while retaining a record of each authorized user. By connecting it to a portable programmer, it can identify the last series of people who entered their personal codes to gain access to the door … and the time of each entry. The smallest model can support 2,000 codes per door, track up to 5,000 events, and be used in conjunction with a swipe card or proximity reader. Larger models can track 89,000 events and all the models are programmed using a PC-based management system.

> **TOUCH SCREEN** push buttons were introduced in 2011 by several manufactures that hid the numbers under a blank screen until touched.

> **MAGNETIC CAM LOCK.** Scheduled to become available in the fall of 2016, these cam locks do not have open keyways so they cannot be picked. A keyway offers an opening for potential thieves to tamper with a lock, to possibly gain access through it, or to cause internal damage. In the magnetic cam lock, an area on its face is cut out that allows the key to plug directly into it. Magnets are located in both the lock and the key. The key can only fit into the cutout in the corresponding lock in one specific orientation and, when the right key does, magnetism works to open the lock. The locking mechanism within the cam lock is quite similar to that of a combination safe lock. Circular brass discs in the cam lock each contain a magnet. The right magnetism and they rotate until the notches are aligned in the unlock position and the key can turn. There are three magnets in each cam lock and, through different disc and magnetic pole positioning in both the lock and the key, over 1500 key codes are possible.

**D. ELECTRIFIED LOCKS**

The conventional mechanical locking hardware has rapidly been replaced by various types of access control systems including card readers, fobs, biometrics, and electronic cylinders. These locking arrangements operate with electrical power and open when used with the proper programmable device. Some access control systems operate off of batteries, eliminating the need for outside power. The basic electrified lock may be locked to prevent egress under normal conditions, but must allow egress in an emergency. In a growing number of locations, delayed egress locks are being selected since they add additional security to public buildings, like hospitals and schools, and eliminate the dangerous practice of chaining panic bars, which is in complete violation of every safety code.

Different code requirements apply to the various types of electrified locks and these requirements can differ from one jurisdiction to the next. The International Building Code (IBC) has been
adopted by most states and is used primarily during construction. Another code is better known and more important to the security practitioner, however. It is the National Fire Prevention Association (NFPA) Life Safety Code 101 and is used by most municipalities to evaluate the safety of the public buildings under their responsibility. A brief description of major electrified locking hardware’s operating features is as follows:

- **Free Egress Control** allows egress at all times by pushing on the touchpad or panic device or turning the lever handle on a lockset. An access control device is typically on the ingress side of the door and is operated by a card, fob, push button, fingerprint, or other biometric credential to allow access through the door at all times. The locking device does not inhibit egress; it only controls and possibly identifies the user. Other alternatives include:
  > Electromagnetic Lock with Sensor Release
  > Electromagnetic with Hardware Release
  > Controlled Egress
  > Delayed Egress

- **Electric Strikes** are embedded in doorframes and operated by a solenoid. This method of unlocking a door makes use of the door lock’s strike to hold the door closed until the lock is manually released. Or the frame mounted strike is released when power is removed by using a card reader access control system. Most applications use a doorframe embedded unit since it is more aesthetically appealing and easier to install.

- **Electric Locks** can be either deadbolt or electric doorknob locks. Power is provided to the door lock through the electric hinge that carries very fine wire into the door from the frame. From the outside, these locks appear like standard mechanical locks. They operate by applying and removing power to the locks. The lock has a pin or bolt that is moved into the door when a solenoid is activated in the fail-safe version. They are generally used in conjunction with a card access system.

- **Electromagnetic Special Locking Arrangements (or Delayed Egress)** are described in NFPA Life Safety Code 101 under Special Locking Arrangements and are available in two configurations: the direct hold and the less frequently used shear lock. With the direct hold method, a metal plate is mounted on the door frame with the electromagnetic unit bolted to the upper part of the door so when the door is in a closed position the plate and lock become tightly attached. This arrangement is visible to anyone using the door and some architects consider it an eyesore and dangerous. A more subtle application is the shear lock where both the lock body and the plate are hidden in the upper door jam and in the top edge of the door. When the door is in a closed position, both the plate and lock disappear into the upper frame. Architects like it since it is basically hidden, but it can be difficult to maintain since the door alignment shifts slightly over time and the lock has to be constantly adjusted to be in alignment with the upper metal plate.

The history of electromagnetic locking system is one of the most controversial in the locking industry since it met with a great of resistance from the fire code community as well as the local
authorities having jurisdictions (AHJ). Many expressed great concern about allowing a magnetic lock to be used on fire exits that prevented immediate egress and ingress during emergencies. It wasn’t until 1980 that the NFPA amended its Life Safety Code 101 to allow this controversial lock to be used on fire exits, and it wasn’t until four years later that this “special locking arrangement” was actually approved by a local fire department for use on all the fire exits in a high school in Newark, NJ.

E. LOCKING SYSTEMS WITH SMARTPHONE OPERATION

In the age of digital communication, people may leave their home without their keys or the ID card they use for office access, but rarely forget their smartphone. After a few smartphone-operated door entrances appeared in the marketplace in 2015, a deluge of systems became available almost all at once in 2016. Some of the devices were funded by Kickstarter and two were partially owned by an investor on the panel of the show *Shark Tank*. These locks are controlled and managed through a smartphone app. Some require the replacement of the entire existing lock system, while others allow the placement of a device over an existing deadbolt. Some systems open by tapping the lock with a finger and a few are designed to open after the system recognizes the smartphone and unlocks the door. Each smart lock has its own little quirks and perks, but they’re all pretty awesome re-imaginings of a millennia-old technology.

Various features that are either shared or unique to each of the available systems are:

> Controlled and managed from an iOS, Android, or web app.
> Notifies the smartphone owner when certain people come in and out of a door.
> Allows granting of remote access to others through the app.
> Customization for exactly how long others have access, what days, or even between what hours.
> Use low energy Bluetooth to recognize when a phone with a digital key is near. No need to bring out the phone; it unlocks automatically.
> Fit directly over the deadbolt on the back of door.
> Built-in WiFi to allow notifications no matter where the owner is located.
> An LED screen on the face of one lock (pictured) displays a greeting to the person who is entering or leaving the home.

Perhaps the fanciest feature is that a lock includes a built-in camera that takes a photo of each person who activates the lock.

F. > Fit directly over the deadbolt on the back of door.
> Built-in WiFi to allow notifications no matter where the owner is located.
> An LED screen on the face of one lock (pictured) displays a greeting to the person who is entering or leaving the home.

Perhaps the fanciest feature is that a lock includes a built-in camera that takes a photo of each person who activates the lock.
F. ACCESS CONTROL WITH PROGRAMMABLE KEYS

After the introduction of the proximity (PROX) reader by the Schlage Lock company in 1982, very little advancement in access control technology until about 2003 with the development of a remarkable system that was able to duplicate all the data/audit trail storage and ID information of the conventional hard-wire reader system by simply replacing the pin-tumbler cylinder with a programmable cylinder that contains a built-in microprocessor. The “Cyberlock” cut the cost of the labor intensive reader concept by 1/10th and could be installed in an entire building complex in a matter of hours instead of weeks.

The Cyberlock system consists of the microprocessor cylinder and a key that is actually a mini-computer that is programmed by connecting it to a computer. This key contains the battery that powers both the key and the cylinder providing all the same information found in the conventional card reader systems. It can also be used with a Padlock with cannot be done using a conventional card reader which requires a hardwired connection to the control panel.

Its acceptance was slow only mainly because the security industry doesn’t react rapidly to advanced technology. It took many years for the industry to understand and integrate the remarkable system into its network of door control devices. The NYC Transit Authority system has over 12,000 of these cylinders throughout their subway system.
A. FAIL-SAFE DELAYED FIRE EXITS LOCKING SYSTEMS

One man is responsible for introducing a unique lock that eventually became a multimillion dollar sector within the traditional lock industry. This strange-looking lock, with no moving parts, was introduced in 1972 when a salesman for a major lock company hand-molded a few 20-pound electromagnetic locks and sold them one at a time through a firm he named “Locknetics.” The lock was about a foot long (the shape of a cigarette carton) with a coil of wire embedded inside the casing to carry the 24 volts that converted the metal shield into a magnet with a powerful holding force. It was bulky and very conspicuous when mounted on the upper door buck, as well as relatively expensive ($300 per lock).

No one in the security industry appreciated its potential value or what advantages it offered over the key-cylinder standard lock hardware. The principal feature of the electromagnetic lock was based on the same technology used by the powerful electromagnetic devices hanging from cranes in junkyards that lift a crushed car body and then release it in another location by cutting off the power. It didn’t sell very well at first and a total of 10 of the magnetic locks were made and sold in the first few years by this one-man pioneer.

It almost became an instant sensation when, in 1975, a security consultant under a contract to design a perimeter locking system for New York City’s Bellevue Hospital was contacted by the Locknetics entrepreneur. Together they participated in the nation’s first program to lock fire exit perimeter doors using this heavy gadget. It was the only locking device that would stop unauthorized ingress and egress at selected hospital fire exit doors by overriding the existing panic hardware. The magnetic lock prevented the opening of the door (from both sides) as long as electric power was running through the electromagnetic coil. In order to be in compliance with fire codes concerning egress and ingress, the power cable was connected to the building’s fire alarm system circuit, which would automatically remove power to the electromagnet whenever a fire alarm was activated, hence the term “fail-safe.” It appeared to offer the ideal solution to the problem of unauthorized entrance and exiting into or out of the hospital premises without compromising life safety regulations. The concept was enthusiastically endorsed by the Bellevue administration and six doors were locked. Then the experiment took a turn.

Bellevue Hospital executive directors requested Fire Department of the City of New York (FDNY) commissioners visit the premises to witness a demonstration of this innovative and remarkable fire exit door lock. They needed to gain the fire department’s approval not only to keep the six doors locked, but to eventually expand the locks to 45 secondary doors throughout the hospital complex. While the installation was a milestone in the security field, it also conflicted with all existing fire codes that had been in existence since the Revolutionary War. Of course the FDNY officials who were invited to inspect the locking system had never heard of a fail-safe lock before their historic visit. Three fire marshals witnessed a test where the fire alarm was activated and the locks opened immediately. The Bellevue hospital administrators were overjoyed, the consultant and the inventor were counting their potential millions … but these
feelings were shattered when the unimpressed fire officials rejected the system as being unsafe and in violation of every fire code in existence.

The six locks were removed from the doors, for the time being which ended the short life span of electro-magnetic locks.

The shocking rationale for the rejection was that the fire marshals did not want another Triangle Fire disaster under their watch. That comment made in 1975 referred to the famous Triangle Shirtwaist Factory fire that happened in 1911. Over hundred and forty garment factory workers died (most young immigrant women) because the workers could not escape the inferno since the exit doors were padlocked to prevent employee theft. That 60-year-old event was the basis for the Bellevue rejection as well as the fact that firemen may be among the bravest people alive, but they are not always open to new concepts - even after a half century of technical advancements.

After the unexpected rejection by the fire officials, the concept of locking fire exits anywhere in the nation lay dormant until 1980, when the NFPA amended the Life Safety Code 101. They recognized that security had become a serious problem, one that posed as much of a threat to life safety as a fire (especially after the introduction of the ion smoke detector in the 1970s by the Swiss firm Cerberus). Until the NFPA amendment was adopted, the locking of any exit in any building without allowing immediate ingress and egress was considered illegal by every agency having jurisdiction in the nation.
The amendment made the Bellevue rejection shortsighted and the concept was now considered a groundbreaking advancement in exit door control.

After the NFPA code amendment was approved, not one building in the nation attempted to challenge local fire officials by following it. It took until 1984 before any public building had the courage to act. The installation took place at a high school in Newark, NJ. The Newark school district had hired the same security consultant who had been responsible for the Bellevue confrontation a decade earlier and the consultant’s task was to upgrade security in all of the city’s 100 schools. That assignment included finding a replacement for the chains that were mounted on all the exit doors, a practice followed by many inner schools throughout the nation at that time. The consultant worked closely with local fire officials to design the same exact fail-safe electromagnetic lock system as that he had set up in 1975. This time, however, the locking system received approval from the local fire department.

Security in the Newark high school improved dramatically and the state of New Jersey amended the State Fire Safety Code based on the results in Newark. Soon after the state approval, the famous Paterson, NJ Eastside High School (that was the basis of a famous movie, Lean on Me, starring Morgan Freeman as the principal, Joe Clark) became the second building to replace door chains with magnetic locks. Officials from the FDNY then visited the Newark school to witness a demonstration in 1984 (not the same fire officials from the Bellevue Hospital fiasco of a decade previously) and they approved the use of the locking system for school facilities in New York City. They recognized the fact that the fail-safe lock was a far better alternative to the common practice of chaining secondary doors shut followed.

A Brooklyn technical high school became the third building in the nation to obtain approval from AHJ to lock fire exits.

After the locks proved their value and it was made legal to lock fire exit doors (the weakest part of any school building security system), the amazing fail-safe locking arrangement did not receive overwhelming acceptance by fire department officials, building managers, architects, and consulting engineers, or very many public officials in city agencies. Even though decades have passed since the locking of a fire exit became part of the NFPA Life Safety Code, the concept of delaying egress by locking fire exits is not a practice with which many people feel comfortable. Most building owners will not attach any device to fire exit doors so they don’t have to deal with potentially violating local fire regulations.

Except for a pilot program in a single school with intruder problems, no New York City facility appropriated funds to allow the same locking arrangement on any exit doors for several years because most fire inspectors failed to recognize that security considerations had become as important as the threat from a fire (particularly in certain dangerous high school environments) even if the building had an automatic fire alarm system with smoke and heat detectors. It took time for old habits to die and fire officials were reluctant to encourage the use of these controversial locking systems. No one in the architectural community would design a new building with electromagnetic locks because the perceived liability risk was deemed more important than the safety of the building occupants. The NFPA Amendment turned out to be a pyrrhic victory and the concept of locking fire exits went dormant again … until 1986.
Sometimes it takes an outside event to force authorities to accept new concepts, especially when dealing with life safety and security issues. There were very few fire codes in existence until the Triangle fire in 1911. Similarly, fire doors remained chained or unlocked until 1986, when an event took place that changed the history of electromagnetic locks. A student in a Brooklyn high school was shot dead in the corridor by another student who had smuggled the gun into the school through an unlocked secondary exit. The Department of Education suddenly discovered extra funds and immediately authorized the installation of new fire alarm systems along with the electromagnetic locks in 43 high schools at a cost of over $30 million. It was a typical example of the difficulty of getting financial support to upgrade security in private or public institutions until some disastrous event forces a positive reaction. After all, security is a non-revenue producing investment.

Finding a competent installation firm posed a challenging problem for the Department of Education since the contract involved more than an innovative electromagnetic locking system. It had to be integrated into the new fire alarm system and be in full compliance with codes and regulations concerning life safety. Finding a competent vendor that understood all the restrictions and the method to interconnect into the fire alarm system was not an easy task.

- **Locksmiths** sometimes mounted these locks on interior office doors, which avoided code compliance obligation - or the need to connect the lock into the FAS (fire alarm systems) in some cases. Locksmiths are mechanics, not electricians.
- **Alarm Installers** were not familiar with the lock hardware since they left that responsibility to the locksmith - unless it involved access control or biometric systems.
- **Licensed Electricians** avoided getting involved with any security devices since they were unfamiliar with building protection procedures and usually focused on high voltage infrastructure (above 50 volts).
- **Fire Alarm Installers** rarely worked on security systems and never on a questionable locking arrangement.

The consultant who had believed in the fail-safe locking concept since the Bellevue fiasco and was involved in the Newark design formed an installation company that was selected to install the electromagnetic locking system in all the schools. The ultimately very justified consultant purchased the lock hardware from the same company who had created them in 1972. An order was also placed for six locks in that same year to be reinstalled on the six doors at Bellevue; the FDNY finally approved them in 1987.

The electromagnetic lock industry is now well established. These controversial locking arrangements can be found in every type of institution in every section of the nation and in many foreign countries. About 10% of the installations are on fire exit doors. These locks are found in every public building where security is essential and the AHJ have understood their value:

- On out-of-the way doors through which inventory might disappear
- Preventing paintings from leaving a museum undetected
- On locks on airport doors leading to the flight line tarmac areas
- In schools using delayed egress systems to maintain a safe environment and prevent drugs from entering
• In hospitals with locked maternity ward doors to prevent infant abduction

Obtaining approvals from the Agencies Having Jurisdiction is still a complicated task that involves the services of a Professional Engineer (Department of Buildings), a filing by a Licensed Master Electrician (Fire Department approval), etc. There are only a few consultant engineering firms that are capable of obtaining approvals from AHJ to lock fire exits and the fee for their service is justifiably expensive.

B. REPLACING CHAINS ON FIRE EXITS WITH FAIL-SAFE LOCKS

PRE-1980. The nation’s leading fire code writing organization is the National Fire Protection Association. It publishes its well-known Life Safety Code 101, which is used as a guideline by almost every municipality in the nation. The code only recognized fire hazards and did not consider any security problems as of equal importance to fire safety; nor did it recognize the common practice of chaining exit doors shut. The Life Safety Code specified that every fire exit door must remain unobstructed to allow immediate egress and ingress to any occupied public building. (In some situations it allowed the locking of doors after the building was closed and empty of occupants.) The Electromagnetic Fail-Safe Locking System for secondary doors offered the perfect alternative to chaining of doors, but was illegal under national and municipal fire codes that simply dictated that no fire exit door could be locked. Free egress from a building is a fire code fundamental, but it began to be challenged with the advent of smoke detectors, sprinkler systems, and magnetic locking systems.

1980. Under a great deal of pressure from the security community, the powers that be at NFPA, who had a history of treating fire safety as far more important than personal security, began to realize that they had to take the latter more seriously. Buildings had become less vulnerable to significant fire damage after the introduction of smoke detectors and the installation of sprinklers. Meanwhile maintaining a secure environment had become a greater problem due to the sometimes violent behavior of intruders. The NFPA amendment to the code that allowed the locking of secondary exits with a delayed fail-safe magnetic locking system once it was connected to the building fire alarm system was a significant step towards prioritizing security concerns.

1984. The combination of a strong-willed principal, a school district security director who was probably the nation’s most knowledgeable expert on school security, and an open-minded Newark fire commissioner led to the system being installed throughout Newark. It was the first time any building in the U.S. was permitted to legally lock their fire exits and the method became part of the NJ State Fire Safety Code.

The New York City Department of Education, in their infinite wisdom, was reluctant to spend money on security devices except for metal detectors at the front entrances, contact switches on exit doors, and audio detection systems for nighttime security. The tragic shooting death of a student in a school changed all that.

1987. The NFPA amendment was incorporated into the NYC fire code for buildings in 1987.
1988. School districts all over the country became aware of what Newark and New York City
were doing and the fire door setup started appearing throughout the country. Not everybody was
easily persuaded, however.

1991. A student at Jefferson High School in Brooklyn, NY wanted to settle a dispute with another
student and could not get past the secured front entrance of the school. Instead he entered
through an unlocked secondary door, carrying a loaded gun that would have set off the metal
detector at the front entrance. The student shot and killed another student in the main corridor.
Twenty-four hours later, that school district found $30 million to lock 35 high schools with
electromagnetic locks and install new fire alarm systems so as to be in compliance with all
municipal and national fire codes.

C. FAIL-SAFE LOCKING SYSTEMS - A CONFLICT

On the surface, it would appear that there are irreconcilable conflicts between fire safety
requirement and physical security requirements. Fire codes have as a principal objective the
assurance that occupants of buildings can always promptly evacuate the premises. They specify
that there be nothing that prevents any person from gaining instant egress from a building. In
many cases that is about the last thing that the security officer wants since it should be made
difficult for people to leave at will, without being seen, especially in situations where someone is
carrying a recently stolen painting from a museum.

Another example is in the nursery of a hospital with an infant abduction security system.
Magnetic locks make it almost impossible to prevent abduction from the nursery. Every door
within the nursery area (corridor, stairwells, elevator, etc.) is programmed to lock whenever an
infant protection system detects unauthorized movement of an infant near the exit door. Yet only
about 1/3 of the nation’s 4,200 birthing hospitals have installed an infant protection system
(including 90% of 42 NYC hospitals) with many facilities still relying on just an audible alarm
signal to indicate that their infant protection system was activated. That approach is not as
effective as locking the door would be.

As seen in the tenth edition of the “Guidelines on Prevention of and Response to Infant
Abduction” published by the National Center for Missing & Exploited Children, they
recommend locking the perimeter doors leading into the nursery area:

Install alarms, preferably with time-delayed egress, on all stairwell and exit doors leading
to/from or in close proximity to the maternity, nursery, neonatal intensive care, and
pediatrics units. Establish a policy of responding to all alarms and instruct responsible
staff members to silence and reset an activated alarm only after direct observation of the
stairwell or exit and person using it. The alarm system should never be disabled.

There are still some misinformed hospital administrators who continue to refuse to accept the
fact that it is legal to lock fire exits in buildings as long as they operate in conformance with the
NFPA code.
The real problem is not always preventing people from leaving a building unnoticed as it is keeping unauthorized people from entering. For generations, this issue was caught between fire code or security requirements. Panic hardware was usually installed on exit doors, particularly schools and hospitals. The problem was that panic release locking hardware did not provide any level of security as it was deliberately rendered useless as building authorities used bars, chains, padlocks, and other means to keep people from breaking in. Removing the panic hardware where it was unnecessary and substituting deadbolts or deadlatch hardware, plus providing other security for the door, seemed to remove the problem and the conflict.

Another method to prevent unauthorized egress is to eliminate unnecessary doors, which architects have sometimes installed because they believe that normal ingress-egress routes will not be satisfactory under fire conditions. These special exit doors are put in for that purpose even if the fire code does not explicitly require them. Security can be weakened considerably by having more doors than are necessary to satisfy the life safety code. Keeping people in a building from walking out a fire exit that has to be kept unlocked from the inside is a challenge. It became less of one when the NFPA allowed the use of fail-safe electromagnetic locks in 1980.

Fire safety advocates and security specialists cannot strive for their opposing measures to be accepted without regard to the possible effect of one on the other. Security regulations cannot blandly state that it is all right to put bars across doors or to use chains and padlocks when fire safety regulations clearly state that their use violates basic life safety principles. The 1980 amendment was the very first attempt to resolve the age-old feud between fire safety and security and to try to balance the requirements of both disciplines.

Only a small fraction of the fail-safe electromagnetic delayed egress locks in use at healthcare and school facilities have obtained the necessary variance from their municipal Department of Buildings to lock fire exits. For example, in New York City, of the 38 infant protection systems in use by 2012, 33 were connected to fail-safe electromagnetic locking systems, but only 8 had filed with AHJ for a variance making the locking of their exits illegal. That ratio is probably the same one found in facilities throughout the nation. The issue centers on the fact that manufacturers providing magnetic locks may not be familiar with the different municipal fire codes issued by the AHJ. Compounding the problem is the fact that installation firms are unaware of the NFPA Code and have no experience in filing for the necessary approvals. The process is expensive, requiring the preparation of plans and schematics signed by a Professional Engineer or Licensed Architect and for the installation to be supervised by a Master Electrician. As a consequence, most locking systems throughout the nation have not received approval from AHJ.

The overriding codes for installing fire alarm systems or any device attached to the system must be in compliance with the Fire Code, Building Code, and Electrical Code. When a magnetic lock is used on a fire exit door, it must be connected to the fire alarm system and operate exactly as it is described in the NFPA code under “special locking arrangement.” In New York City, for instance, the installation and all ancillary components have to be approved by both the FDNY and the Department of Buildings. It has to meet the city’s municipal code even though the locking arrangement is meant to improve security - not life safety. The NFPA Life Safety Code is used as a guideline, but the municipal code is considered law.
D. OPERATION CHARACTERISTICS

Since electromagnetic locks have no moving parts they are completely silent even when powered and locked. They are vandal-proof, weather resistant, and virtually maintenance free. There are several configurations of magnetic locks, with the most common type being the pull magnet. The lock comes in two separate pieces; there is an armature mounted on the door frame (strike plate) and an electromagnet bolted to the upper edge of the door. The magnet and the strike plate must align properly to secure the door in a locked position. The locks are powered through a relay in a building’s fire alarm system. In the event of a fire alarm activation, the power is removed instantly and the locked door can now be opened. According to all codes, the building must have an approved Fire Alarm System (FAS) and the approving authority must also approve the locking system. When an electromagnetic lock is used on an office door in place of a mechanical lock, and not connected to the FAS, it isn’t required to be in code compliance.

There may be situations where a fire condition exists but does not activate the FAS. There are mandatory provisions in every building code that a door shall have power removed after someone manually pushes on the door for 15 seconds (or for 30 seconds under special situations). A nuisance delay period is programmed into the initiating circuit that ignores short pressure on the door caused by someone accidentally bumping into it or a gust of wind, etc. The obvious intent of this nuisance alarm is to minimize false alarms without compromising the integrity of the system. If an exit is required by emergency conditions and the FAS was not activated, escape can be accomplished by pressing on the door for the programmed period of seconds. In order to activate this delay egress override, pressure must be maintained on the door until the nuisance delay period has expired. The irrevocable release countdown will continue until the lock automatically releases. It will then remain unlocked (without power) until manually relocked by a reset device.

Other core requirements that every delay egress system must meet are:

- A circuit that ignores the 3-second nuisance “push,” but once the 3-second threshold is passed the 15-second release cycle continues to the end of the 15-second delay period before power is removed from the lock. It solves the annoyance problem.

- Applying no more than 15 lbs. of pressure for more than 3 seconds (ignoring under 3 seconds to eliminate a nuisance delay), will start an irreversible process to unlock the door in 15 seconds. The NFPA code allows an extension to 30 seconds when a door is located far from the security desk, for instance, and the longer delay is approved by AHJ. The lock must be manually reset at the door to ensure that someone visits the site and no fire condition exists.

- A sign must be applied to the door stating how to open it in an emergency, such as, “PUSH UNTIL ALARM SOUNDS. DOOR CAN BE OPENED IN 15 SECONDS.”

BASIC LOCKING SYSTEM DEFINITIONS

Ingress: The act of entering a building.
Egress  Leaving or going out of a facility.
Fail Safe  Usually relating ensuring that the loss of power supplied to an electromagnetic or electric strike lock causes it to open and remain in an unlocked condition until power is restored.
Fail-Secure  A failure in electric power causes a secure or failed closed condition when power is not sent to the lock, as during a power outage. The only way to release the lock is by using the manual override feature. There are very few situations where this type of power configuration can be employed and still be in conformance with national fire codes.
Latched  Door can be opened (as in turning a doorknob), but cannot be pushed open without operating the door handle to release the latch.
Access Control  Popular term that usually refers to a card reader system, although not necessarily. It is a setup that grants or denies an individual access to a specific area based on their possession of a card, code, programmable key, or even specific physical characteristic. Since access control systems have the potential to limit a person’s ability to escape a fire or other emergency, fire and safety codes must be strictly observed.
Fire Rating  A door assembly (consisting of a door and its frame) that is rated in terms of its ability to withstand a fire. Building codes determine the fire rating in a particular community. After door lock hardware is installed and the door is then penetrated to allow wiring, the fire rating may be significantly affected. Access control locking systems must conform to the door’s fire rating so as to not reduce the fire rating of the door.

ORGANIZATIONS INVOLVED IN FIRE EXIT LOCKING SYSTEMS

- NFPA 101 SPECIAL LOCKING ARRANGEMENTS
  Nuisance Delay: up to 3 seconds permitted
  Release Delay: 15 seconds total or 30 seconds with approval from AHJ
  Re-locking: Manual switch, cannot be a switch located on or triggered by door movement

- STANDARD BUILDING CODE (SBC)
  Nuisance Delay: Not allowed.
  Release Delay: 15 seconds or 30 seconds with approval from AHJ.
  Re-locking: Reset must occur only on opening, must be a switch located on or triggered by the movement of the door

- UNIFORM BUILDING CODE (UBC)
  Nuisance Delay: Required, must be set to 2 seconds.
  Release Delay: 15 seconds total, no other options.
  Re-locking: Manual switch, cannot be a switch triggered by the movement of the door.

- BUILDING OFFICIALS CODE ADMINISTRATOR (BOCA)
  Nuisance Delay: Required, must be 1 second.
  Release Delay: 15 seconds total or 30 seconds with approval from AHJ.
  Re-locking: Must be a switch located on or triggered by the movement of the door
This section focuses on various types of fire and smoke detectors and how they operate using the different technology that has been available since they were introduced in the mid-1970s. These small, inexpensive, and highly effective detectors have been the basis for the decline in the nation’s fire deaths - while security threats have grown exponentially. Yet the security industry has never adopted “Security Codes” to counteract the influence of the NFPA’s codes. The detectors include:

- Ionization Detectors
- Photoelectrical Detectors
- Products of Combustion Sensors
- CO detectors

### A. HISTORY OF SMOKE DETECTORS

1. In the 1930s, American firms concentrated on upgrading burglary protection and expanding central station coverage, while Europeans took the lead in developing new technology that improved the art of fire detection. It was during this period that a device was developed that would eventually change the way fires were detected throughout the world. The amazing device was an “ionization” smoke detector which was far superior to existing heat and flow detectors, since it could detect a fire before it burst into flame or gives off heat. [Heat sensors failed to provide an early earning for fires that smolder and produce deadly smoke before bursting into hot flames.]

2. The device was invented in Germany to protect munitions plants in the late 1930s and was refined by a scientist (Dr. Miele) working with a Swiss firm, Cerberus, that was investigating techniques to detect toxic gases in underground mine shafts. Some experts in the fire alarm detection industry insist that Dr. Miele was a heavy smoker and would accidentally activate the gas sensor. The invisible products of combustion from cigarettes caused the gas sensor to alarm. When it was realized that there was more potential in developing a smoke detector rather than a
gas detector, a patent was obtained. The ionization detector was born and sold throughout the European market following the end of WWII.

3. Smoke detectors immediately changed the way fires were detected since they could sense a fire earlier than all other sensors used in the fire protection/detection industry. Ionization smoke detectors could sense “charged particles” which are common to all fires in their early stages. The technology was so innovative that no American firm could be found to distribute the smoke detector. Several fire alarm system manufacturers and installers such as ADT, Grinnell and Edwards were contacted by the Swiss manufacturer [since they controlled most of the fire protection and monitoring market in the USA] but were not interested. These well-established firms did not have the slightest understanding of the enormous market potential for a ceiling mounted device that could detect a fire before the flame or heat was noticeable. In later years an entirely new industry was created; in the late 1950s a very small company in New Jersey sold CO2 fire extinguishers (Pyrene), becoming this nation’s sole distributor for the product. They sold millions of detectors, which eventually changed fire codes throughout the nation and significantly lowered the death and injury rate from fire.

The first description of a smoke detector in a municipal fire code was in 1975, when New York City issued the Local Law 5 code for high rise buildings. The code included many changes that were very controversial and it took many years before it was approved. Most of the experiments used to develop this important code were conducted during controlled burning of buildings in downtown NYC that were being ripped or burned down to be replaced by the World Trade Center.

4. Facility fire and safety protection has evolved slowly over the last century and changes were made, not usually because of technology, but most often as a result of a fire related tragedy. There has been little controversy surrounding fire safety since the introduction of smoke detectors in the United States by the Swiss firm Cerberus in 1973 and the installation of sprinklers in all types of structures. Fire safety requirements are strictly enforced by local, state and federally mandated codes and regulations, but there is no such enforcement governing security of personnel and property protection.

5. There is really only one national fire code followed by practically every municipality in the nation, and it is not monitored by a federal agency; on the other hand, the Department of Homeland Security has been attempting to integrate security requirements into building codes since 2001. This universally accepted set of fire codes is issued by the civilian membership of the NFPA. Even the few large cities that have their own municipal fire codes – they generally follow closely the codes based on the NFPA Life Safety Code 101, (with only minor modifications). There is no comprehensive organization that compares to the NFPA which sets standards and establishes regulations; their manual is considered the bible of fire codes in the nation.

The entire scenario that defines the fire alarm industry is more convoluted than the evolution that has defined the security industry. The following table of corporate buyouts, mergers, name changes and takeovers describe the complicated lifecycle of the smoke detection industry:
• 1950 **Cerberus** manufactures the high voltage ionization smoke detector in Switzerland and sells it throughout Europe
• 1956 **Pyrene CO2** becomes the American – Canadian – South American distributor for the high voltage ionization smoke detector
• 1958 Pyrene changes name and forms **Pyrotronics** Inc [owned by Baker Industries]
• 1958
• 1970 **Baker Industries** starts armored car division and buys Wells Fargo name from bank
• 1970 Photoelectric and low voltage ionization detectors introduced
• 1975 Fire code changes allows its use as a better sensor than fixed temperature heat detectors and lists ionization detectors for high-rise buildings
• 1980 **Borg Warner** buys Baker Industries/Pyrotronics/Wells Fargo
• 1980
• 1988 **Merrill Lynch** buys Borg Warner – takes company private – sells off fire divisions
• 1989 Cerberus buys Pyrotronics
• 1998 **Siemens** buys Cerberus

**PRODUCTS OF COMBUSTION DETECTORS**

• **Ionization Smoke or products of combustion detectors** are the most important of all the fire detection devices and the following description indicates many of the same growing problems that were experienced in the security industry.
• **Photoelectric Smoke detectors** rely on a different principle to detect invisible smoke.
• **Air Sampling detectors** are used mainly in data processing centers and similar environments. Air from a duct is drawn into the detection chamber where a laser is used to look for a certain number of smoke particles in a given amount of time.

> **IONIZATION SMOKE DETECTORS**

1. These small, inexpensive early warning detectors measure the electrical properties of particles by creating an electrical current using a minute amount of radioactive radium. The radium alpha particles emit energy that “ionize” the air molecules between two plates with the positive molecules attaching themselves to the negative plate and the negative ions attaching to the positive plate. When incoming smoke particles attach themselves to the charged ions, in effect, they add weight to the ions and slow down their movement, causing a current flow to decrease. This change is detected and recorded as an alarm condition.

2. The amount of radioactive radium element in each detector was so infinitesimal that it would be harmless to humans (unless 50 detectors were swallowed all at once). The concern over low level radiation isotopes in the detectors caused some municipalities and agencies to ban their use because there were fears as to how to destroy used units without contaminating the atmosphere. The public is actually exposed to more radiation every time they go out in the sun or board a commercial jetliner than if they carried a thousand detectors in their pocket. Once a rumor starts, it is hard to stop. The manufacturer substituted Americium 241 for radium to respond to the radiation fear.
3. The ionization detector was an advance over every other existing detector but it wasn’t perfect; it proved too sensitive for certain areas (it could not be used in the kitchen and it was slow to detect fires that smoldered in rugs, couches and other cloth material). The biggest shortcoming was that the required power source was 220 volts of direct current (DC) – which was costly to provide and it had to be connected to the electrical system. If a fire destroyed the electrical system first, the detector would not be able to send an alarm. The original units sold in the US cost $110.

In 1964, an American firm refined the device and manufactured an ionization smoke detector that operated off 24 volts and could use alternating current (AC). In the mid-1970s this company designed a battery operated unit that was suitable for the private homeowner marketplace; that unit became the first to be mass merchandized through retail stores at a cost of $10 or less and was described on the front page of Consumer Reports magazine.

PHOTOELECTRIC SMOKE DETECTORS

Ionization and Photoelectric detectors operated on different scientific principles, with the photoelectric type sensor operating more or less like the light beam detectors that were in use as early as 1935. The theory behind this application relies on the principle that smoke can block a light beam just as a human can block the light beam on the intrusion device. The small photoelectric cell allows detection of visible smoke and the operating principle is similar to that of the movie theater projection beam. If the theater were absolutely smoke and dust free, it would be difficult to see the beam of light between the projector booth in the back of the theater and the screen.

1. The beam actually becomes visible (“lighting up”) due to smoke particles being illuminated along its length. The audience in the theater does not see a light beam, it sees the dust particles reflecting the light from the theater projector. In the photocell detector, the projection booth is replaced by a light bulb and when particles of smoke enter the chamber, they are illuminated and detected by the photocell. In order to overcome the need to periodically replace the bulb, a firm developed a chamber with a pulsing LED that lasts for years before the need to replace it.

2. The only new feature that has been added to smoke detectors is instead of emitting a screeching sound when smoke is detected in a home, the recordings of parents’ voices are substituted. The prerecorded voice of a parent has proven to be much more effective in alerting a child to an emergency situation than the conventional audible alarm sound which often fails to awaken young children who are sleeping soundly.

ARSONISTS. These criminals have become almost invisible due to the wide use of early warning smoke and heat detectors, but they still cause a lot of property damage and many deaths.
Most arsonists are not professionals whose services are for hire. Many like to set fires to give them instant gratification while watching the effects of their work and the response from the firemen. They are often found standing around the area where the fire rages. That is why the police often record the crowds around a superstitious fire to possible identify a person who has been frequently discovered near previous fires. There are arson investigators who are members of the fire department who are experts in determining the cause of a suspicious fire. There are also private arson investigators who often find the basic cause of the fire without ever setting foot on the damaged premises. They do most of their work by examining the financial and social background of the building owner, who is usually the recipient of the fire insurance policy. A business about to go bankrupt, gambling debts, or a girlfriend [not the wife] driving an expensive car and living in luxury etc., are better indicators of arson than the smell of gasoline on the premises or the discovery of frayed electrical wires.

**CHEMICAL DETECTORS**

The possibility of a nuclear, biological or chemical attack is now the most feared event concerning government agencies because of the potential for mass casualties.

1. Vacuum cleaner type chemical detectors have been installed and tested in large train stations, most notably (a) Grand Central, (b) Penn Station, (c) 30th Street in Philadelphia and Union Stations in (d) Washington and (e) Chicago. These very expensive systems were first developed in a government controlled laboratory following the Tokyo subway incident in 1995. The system uses a modified vacuum cleaner type apparatus to “sniff” the air collected by sensors scattered throughout the station and analyses it for chemical toxins and lethal gases. The prototype models would false-trigger the chemical sensor caused by the odor emitted from the janitor’s cleaning bucket even though the sensors were programmed for the specific chemicals expected to be dropped by a terrorist. The first installation in the nation was in Grand Central Station during the 2004 Republic National Convention. Cameras were strategically placed near the sensors to help security staff isolate real terrorist threats.

2. The program was developed under Homeland Security sponsorship and was known as PROTEC [the acronym stands for Program for Response Options and Technology Enhancement for Chemical/Biological Terrorism]. The proper response to a chemical attack in a train station [or anywhere else] is not clearly defined and the choice of having the police department or the fire department as first responders is still being debated. In NYC stations, the Metropolitan Transit Authority [MTA] had to develop plans that defined the relationship and chain-of-command between the MTA police force, the FDNY, the NYPD and even the Health Department on how to coordinate their response in the event the sensors actually detected an attack. It remains to be determined how hospitals will participate as first receivers, since there are serious concerns as to the treatment of victims [the vaccines and decontamination process].

   In the Tokyo event, the police followed standard procedures and stationed the control desk directly above the subway vent to monitor victims as they were brought to the street level. The gas coming out of the vent killed some policemen.

3. Some major cities have followed the lead of NYC in establishing certain medical facilities as special emergency burn units to treat victims in a chemical or nuclear attack. Under the guidance
of the Health Department’s Bioterrorism Hospital Preparedness program, each designated hospital will be provided burn care equipment, supplies and eight-hour staff training sessions. The original strategy was to set aside about 70 beds in four widespread hospitals, which were thought to be enough in normal times, but the selected centers would be overwhelmed in the event of a major catastrophe. Any effective citywide response would require coordinated mobilization of city, state and federal resources and the use of radiation detectors and decontamination units. Without the system ever being tested in a real life situation, the city has spent over $1 billion on anti-terror initiatives since 9/11 [most from government sources]. Security Directors at the designated health care facilities have been trained and instructed on the operation of the detectors but there is serious doubt that any of these so-called emergency plans will ever prove effective.

4. The Department of Homeland Security, working with the FBI, has been quietly assigning handheld radiological devices to specially trained Transportation Security Administration agents since 2009. The agents randomly board trains and buses and visit transit hubs to prevent terrorists from hauling dirty bombs and other explosives to big city targets. The small portable instruments detect radiological and biological particles emitted from materials that may be transported in baggage or personal belongings.

- **FIRE/HEAT DETECTORS**
  - **Heat-sensitive** devices react (a) to preset fixed temperatures or (b) to rapidly changing temperatures of 15°/min (rate-of-rise type). These have been available for over 100 years as the first line of defense against fire damage. While these detectors are the least expensive, they are also the slowest to react to a fire. They are not considered life safety devices since most fire deaths are caused by smoke inhalation, not heat. These slow detectors are typically used in unoccupied locations as property protection devices. Most national codes indicate that if the space has sprinklers, there is no need to install a heat detector since a sprinkler head is nothing more than a heat detector.

  - **Flame or gas sensors** are designed to “see” the light emitted by a flame or detect flammable gases. They are usually used to detect explosive situations from a long distance.

  - **Sprinkler Flow sensors** are activated when the heat sensor on an individual sprinkler head melts and water flows through the system.
A. NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

1. The NFPA Life Safety Code 101 Amendment in 1980 to allow the locking of fire exits was a revolutionary concession by the most important fire alarm code-writing organization in the nation. Although the NFPA issues most of the nation’s fire codes and regulations relating to life safety, there were never any compromising life safety codes to include security considerations. The conflict between fire safety advocates and security practitioners exposed two divergent philosophies that often clash, especially when protecting large public buildings and the means of egress and ingress though fire exit doors.

Almost all municipalities follow NFPA codes when developing their own building codes, particularly in areas relating to the installation and operation of fire alarm systems. A few of the nation’s largest cities, like New York, Chicago, and Los Angeles, have developed their own building and fire codes, although they usually follow the guidelines issued in the NFPA Codes. They are modified before being adopted for inclusion into the municipal codes to reflect the particular requirements of their metropolitan area.

NFPA has published close to 400 codes and standards, with the mission to prevent the loss of life and property. Topics include fire prevention equipment, extinguishing systems, inspection, residential and commercial dwellings, and safety of flammable gases. They also publish the National Electrical Code, which is the most widely-adopted code in the world and is used in every state in the nation. Standards include many directives that involve a specific facility or a system, such as:

- NFPA 10 Portable Fire Extinguishers
- NFPA 90A Installation of Air Conditioners
- NFPA 704 National Fire Alarm Code
- NFPA 1600 Disaster/Emergency Management
- NFPA 101 Life Safety Code 101
- NFPA 99 Healthcare Facilities
- NFPA 70 National Electrical Code
- NFPA 1561 Incident Management Incidents
Fire safety rules and codes have been around for over a century and follow well-established rules and regulations established by the NFPA (and a few other code writing organizations). Security follows a far different set of protocols since it isn’t guided by codes or statutory requirements; it follows available technology - unencumbered by codes or regulations. This lack of any restrictive codes has resulted in the phenomenal grown of the modern security industry since the late 1970s. The separation of fire safety from security had never been breached … until 2005 when the NFPA unexpectedly entered the no-man’s land separating the two industries by issuing a set of controversial security standards that, from all indications, has been totally ignored by the security community who feels justified in disregarding any and all security code recommendations written by basically, a fire code writing organization.

B. JURISDICTIONAL DISPUTES

Agencies under the control of a large municipality can become redundant or create problems with different and conflicting levels of authority, especially when defining codes, regulations, and standards. Within the boundaries of one New York City borough, for example, there are several facilities that fall under the purview of different governmental agencies. Each agency mandates their own special set of codes and standards. This jurisdictional mess is probably common in the nation’s 100 largest cities and it illustrates how baffling and difficult it can be to obtain approval to install a new concept using technology that is more advanced than any code or standard in existence.

Sometimes one agency will approve an installation that is rejected by another enforcement agency within the same jurisdiction. This overlap can be seen at the township level and beyond. For example, a locking system is used on a facility that is owned by the state with its own fire code, but it is located in a city with another fire code - and that facility is an airport so it is also under the jurisdiction of the FAA. Other instances are:

- A state-owned mental institution that is authorized to operate under New York State Code must also meet New York City’s code because the FDNY responds to fire emergencies.
- Federally-owned veteran’s hospitals operate according to federal agency fire codes and standards, but also have to be in compliance with the local municipal fire codes.
- Terminals at LaGuardia and Kennedy Airports are under the control of the FAA (federal), yet they are under an ownership agreement with the Port Authority of NY & NJ (state), and are located in New York City (municipality).

The federal, state and municipal fire codes vary and expecting that each facility be in compliance with all the fire codes is an impractical and almost impossible task. In the latter case, if a fire emergency arises, which fire department has jurisdiction? Is it the airport (FAA) fire department or the FDNY? If both respond there is the possibility of a jurisdictional dispute.

C. FIRE PROTECTION CODES AND STANDARDS ORGANIZATIONS
The NFPA has about 80,000 members, encompassing about 200 technical committees and 7,000 voluntary participants in the standards development process. Its codes and regulations are adopted by thousands of municipalities all over the world, with some larger cities having their own codes actually incorporating the NFPA codes and standards into their municipal electrical and fire codes, with minor modifications. Membership is made up of representatives from various technical disciplines and industries, including the American Institute of Architects, National Electrical Contractors Association, Builders Hardware Manufacturers Association, and the International Council of Shopping Centers, as well as thousands of non-affiliated individuals. Anyone who can afford the $150/year dues can join and vote on any new proposed codes at the organization’s annual meeting.

A few security practitioners have become active in it in recent years mainly as representatives of the Professional Alarm Services Organization of North America, Security Industry Association, and the American Society of Industrial Security (ASIS). NFPA’s main focus since its founding in 1922 by the fire insurance industry has been trying to develop a balanced membership, however the voting membership has traditionally come from the fire alarm industry, not from the security industry. As a comparison, ASIS, which is in many ways the security counterpart to the NFPA, has 35,000 members with almost all of them from the security field and very few from the fire alarm industry. There has never been much commingling between fire safety people and security advocates or between the NFPA and ASIS. ASIS was formed almost a half century after the NFPA and these two highly visible organizations share an interest in life safety, but come from different directions with different goals. While this observation may be too simplistic an evaluation, the differences in the two organizations became more evident in 2005 when the NFPA issued two security standards, 730 and 731, that were concerned with security standards. The publication met with some hostility from the security community (outrage many be a better term) and ASIS reacted almost immediately by establishing their own standards and guidelines in 2007. In doing so, ASIS started a rivalry with the NFPA (possibly unintentionally) and may expand their standards committee to issue fire alarm system codes.

Fire prevention standards developed within the NFPA are based on a consensus vote procedure. A member in good standing is allowed to participate in the development of codes and regulations such as those that deal with the design of fire detection systems. Votes on new or revised standards are then taken at its annual meeting. Members who are not present at the meeting cannot vote. While the process may not be scientific, it is a method that has produced fire codes that have been adopted by municipalities throughout all 50 states and copied by numerous foreign nations. There has never been an equivalent code writing group in the security field with influence comparable to the NFPA’s within the fire safety community. The few attempts that have been made by other code and testing organizations have never produced any significant results in building design as the NFPA has.

D. CONSENSUS VOTE IN ESTABLISHING UNSCIENTIFIC CODES

The subject of smoke detectors in hospitals was debated by the NFPA membership in the early 1980s. It illustrates the popular misconception surrounding codes and regulations, how they are developed, and how competent the members of a code-writing organization are who are able to create these life safety codes simply by paying their annual dues. The public, by and large
accepts the codes as if they are scientifically tested and based on a lengthy research development procedure. These codes, whether they be fire, building, or electrical, do not go through the rigorous hurdles like the Food and Drug Administration makes the pharmaceutical industry go through before a drugs is approved. The NFPA does no testing, has no laboratory facilities, and no legal authority to enforce any of the codes it establishes. Some of its codes have been criticized for being impractical, unscientific, and too closely allied with particular segments within the alarm system manufacturing industry. Fire codes are issued almost 100% of the time by the NFPA; sometimes these codes are harmful or based on financial gain rather that directed toward improving life safety.

In contrast to life safety and fire codes, those who design, construct, and install security systems have not shown any desire to establish codes. There have been many attempts by many national standards writing organization to establish codes relating to the security industry, going as far back as 1975. These attempts have had no impact on the security industry, mainly due to rapid changes in technology and the lack of any centralized code writing organization that has a similar influence as the NFPA on the fire prevention community. The technology changes in the security field have been so rapid that any attempt to set a standard acceptable to all concerned parties would fail, since any basic standard that would satisfy everyone’s interests would take so long to develop that a security standard would become obsolete by the time it was adopted by the relatively slow consensus vote process.

Fire alarms affect life safety, with their main focus on protecting against fire damage to a building and injury to occupants. Security systems are primarily concerned with protecting property and occupants at all times - not from fire, but from theft or other crimes against occupants. That separation of goals between the two technologies is sometimes overridden by the federal government’s emphasis on terrorism. Commingling of codes between the two factions will never be achieved and it is unlikely that the conflict between the NFPA and ASIS in the area of codes and regulations will ever be fully solved.

Since the 1980 amendment to the NFPA Life Safety Code 101 dealing with the locking of fire exit doors, very few other concessions have been addressed specifically to the security community by that organization. That indifference (neglect may be a better descriptive word) changed in 2005 when NFPA 731 and NFPA 730 were issued. The new codes were developed by one of the many NFPA committees made up of members with fire alarm backgrounds, but who had limited experience in the security field. The NFPA went against tradition by entering the domain of the security industry, based partly on the previously issued NFPA 5000, which is the “Building Construction and Safety Code.” The wide acceptance of that code appears to have encouraged the organization to move into the whole building environment, including topics related to electronic security systems. This was a bold attempt to enter the domain that usually fell into areas that the ASIS considered their sphere of influence and it prompted ASIS to issue their own guidelines and standards. In a sense, the two organizations tried to defend their domains and, in doing so, created a sort of technical Hatfield-McCoy feud or the NFPA vs. ASIS.

Even though the NFPA attempted to recruit the expertise required to develop a security code and solicited comments from security industry practitioners, the resulting standards have become very controversial and it is doubtful that the NFPA 731 and 730 codes will ever be accepted by
the security community. It wouldn’t be the first failed attempt to establish standards in the security field and it probably won't be the last:

**NFPA 731**: “Installation of Electronic Premises Security System”  
**NFPA 730**: “Guide for Premises Security”  
**NFPA 99**: “Standard for Healthcare Facilities”  

These four standards were intended to provide a minimum standard for the installation of several types of security systems. NFPA 731 focuses on eliminating false alarms as much as possible. The code also discusses the training and qualifications of the installer and other superfluous conditions. NFPA 730 focuses more on security management in a healthcare facility. These two security-related codes were prepared by a fire alarm organization and have been ignored by the security community. NFPA 99 is a little known standard that requires the installation of electronic premises security systems that meet the requirements of NFPA 731.

The non-standardized security industry seems to periodically attract a few well-meaning code writing organizations that, for over four decades, have tried to establish guidelines that cover some of the same objectives that have been used in the century since the NFPA was established. Such code writing attempts for security standards seem to reappear every five years and repeat the same mistakes as their predecessors. There are no organizations that perform for the security industry some of the same functions that the NFPA has done so successfully for the fire safety industry since 1896. Many of the individuals involved in past attempts to establish security standards have retired without leaving any lasting impact on the subject, resulting in many of the same mistakes being repeated and discarded. There are other highly technical industries that have also resisted attempts to establish codes and standards, like the computer industry that changes technology almost annually or the aircraft industry, which generally has only to meet safety or hazard standards - not aerodynamic standards. Some of the early adventures in developing security standards occurred in 1973 when two of the nation’s largest standard writing organizations combined forces to develop some standards for a new, evolving security industry. The first private code writing organization to focus on security standards and regulations was the American Society for Testing and Materials (ASTM). They formed the F-12 Committee on Security in 1972 and held a series of meetings at their headquarters in Philadelphia that only a few attended; no one paid much attention to their recommendations.

In 1979 the ASTM was still trying to write standards and co-sponsored a symposium on the topic of building security with the federal agency that was then known as the National Bureau of Standards (it became the National Institute for Design and Technology in 1982). The meeting at the NBS was attended by 200 practitioners in the various disciplines that comprised the private security industry and that meeting is considered the very first attempt to establish an industry-wide set of standards in the security industry. It resulted in a series of publications on various security-related subjects and a book was published by the NBS containing the 14 presentations made by the experts at that historic meeting. Some of the topics discussed at that meeting could still be informative in today’s environment, even decades later. A partial list includes:

1. Emerging Concepts in Building Design
Nothing concrete ever came out of that well-intentioned meeting and in the ensuing years there have been several code-writing organizations that have attempted to become pioneers in developing security-related codes and standards, including the ASTM, ANSI, and BOCA. These national organizations issued a few basic codes and regulations, supposedly to force manufacturers to follow certain guidelines in manufacturing protection and detection devices and systems. All those early efforts have had one common trait... all the codes related to security systems have been ignored and long forgotten. Even the government’s Sandia Laboratory, a world-renowned testing organization, had, as long ago as 1980, tested and issued some standards on security devices. Yet no one still in the industry from those early years can remember exactly what the standards involved and all the devices tested have, of course, become obsolete.

E. AN UNFORTUNATE EXAMPLE OF CODE CREATION

In the creation of a code or standard certain voting members of code writing organizations that rely on consensus votes to develop codes can be influenced to favor vested interests over practical considerations. One such example of “stacking” the vote occurred during the NFPA’s annual meeting in early the 1980s. They were considering adding smoke detectors to every patient room in a hospital. The previously established code specified smoke detectors in the corridors at designated separations. The vote to add a smoke detector to hundreds of interior patient rooms would be a costly expense for medical facilities. The code was submitted to members prior to the annual meeting so as to promote discussion and allow possible revisions to some of the conditions spelled out in the code. Several hundred members assembled, which was unusual high attendance for a meeting on a code change. Instead of a calm discussion, there was a heated debate between proponents and opponents that appeared as if it were a political debate.

Hospitals within a thousand miles of the meeting location had hundreds of their medical and building staff join the NFPA prior to the meeting and bused the brand new members in to vote. At the same time, manufacturers of smoke detectors had also arranged for their employees to join the NFPA and provided dozens of buses for their “new” members to attend. Not many individuals in either group knew exactly what the difference was between a smoke detector and a thermostat. Ultimately, the vote was close and the smoke detector in every room amendment was defeated. The following year, however, the amendment was approved because manufacturers had
gathered more “voting employees” that time around. There are now some safeguards in place to prevent one industry from controlling a vote by limiting the right to vote to only those individuals who have been a NFPA member for a year or longer instead of just 24 hours.

F. UNDERWRITERS LABORATORIES (UL)

In contrast to the NFPA is Underwriters Laboratories, now known as UL. It is the largest independent testing laboratory in the nation with 5,000 employees who have conducted tests on systems, devices, and materials to ensure compliance with safety and health standards for over 100 years. UL has established 800 standards and inspects or tests over 70,000 products each year, including firefighting equipment, lighting fixtures, access control systems, etc. Some examples of the tests they do are on the thickness and type of material used as wire insulation, proper grounding, the components in a fire alarm system, and electrical appliances to ensure that there is no danger of overheating or electrical shock, etc. The tests are also performed on many of the fire and security products found in hospitals, like electromagnetic locks and infant protection systems. They test to make sure a product meets the existing standards used to test access control systems, for example. UL listed devices are identified by their UL Listing Mark (attached to over 20 billion items).

UL began its association with the burglar alarm industry in the 1920s. This relationship was formed when a group of insurance companies requested the assistance of UL in the establishment of a rating system for alarm installations for the few existing security products available that were then available. The result of this request was the development of different levels of alarm protection and the establishment of priorities of vulnerability and grades of alarm protection, a reference that was totally lacking until this time. In general, before a standard is adopted, comments are solicited from interested parties who include manufacturers, consumers, individuals associated with consumer-oriented organizations, academicians, government officials, and industrial and commercial users. Care is taken to avoid having a small group of manufacturers design the testing procedure for their own products.

A manufacturer seeking a UL listing pays a fee to have the unit tested against a related standard. In the security arena, the UL label is essential for any device that is connected to any part of the fire alarm system, meaning that fail-safe electromagnetic locks must be UL listed under most circumstances. A UL label for many other security products is not really essential; the average security device is upgraded so often just to stay competitive that any practical test would be useless. By the time a test was completed the product would be obsolete and commercially unavailable. Or sometimes there may not be relevant tests available. One infant bracelet protection system used to prevent the kidnapping of newborns from the nursery ward had been UN tested, but the test was probably related to environmental tests involving humidity and temperature limits. In other words, the tests proved that the system would operate at temperatures over a hundred degrees Fahrenheit and in humidity. There was no test to ensure that the system would activate the alarm system when the tag (on the bracelet) was moved near an exit. Once a device is listed, the manufacturer must affix a UL label to each unit - there is a charge for each label. The public relies on these labels when purchasing electrical supplies like lamp cords and light bulbs, but the UL label is not very important for a rapidly changing and complex security system (except for the electrical cord connecting the panels to the power source).
When any security device is connected to a building’s fire alarm system, it is considered an ancillary component of the system and must be UL Listed or meet the testing standards of another approved laboratory. Otherwise the device will not be accepted as meeting local fire codes.

**GENERAL DEFINITIONS**

- **REGULATIONS** are usually requirements published by local, state, and federal agencies that may evolve from a directive set forth in a statutory law. Regulations can have the same authority as if they were issued by a legislature and are often considered more binding than codes or standards.

- **STANDARDS** are a set of voluntary criteria, guidelines, or best practices. They are usually used to enhance the quality, performance, and consistency of a product, service, or process. Standards are often interchangeable with “codes” since both become effective only after being adopted as a regulation by some governmental authority (federal, state, or municipal). A standard does not contain mandatory provisions, especially when it uses the word “shall” to indicate requirements, and is written in a form that is generally suitable as a reference for other standards or codes or for adoption into law. A standard is often adopted into law, but it is typically made applicable only when it is referenced in a building code.

Many major cities publish their own codes and regulations due to their sheer size and unique requirements. Smaller cities usually do not have the need or the resources to write and enforce their codes and simply adopt the building, fire, and electrical codes published by code writing organizations and created for that specific purpose.

- **CODES** are a set of rules put in place by various authorities. They are usually modified to accommodate or reflect specific conditions of a jurisdiction before conversion into laws and regulations. Florida stresses hurricane code compliance while Midwestern cities address tornadoes, etc. The many code-writing organizations that deal with building construction and fire protection traditionally have tried to publish a code for every conceivable situation, making them sometimes either redundant or conflicting. A code becomes a legal mandate after it is adopted by a municipal, state, or federal agency. The National Fire Protection Association is, by far, the most recognizable code-writing association in the nation, but there are other organizations that develop codes. Those codes usually closely follow the procedures adopted by the NFPA. Codes are not meant to be unchallenged, nor are they based on some scientific discovery. They are updated due to changes in technology or events that expose an established code to be inadequate or even obsolete. Codes generally undergo a revision cycle every three years, which is often done by committees that deal with specific categories such as building, fire, electrical, plumbing, and so forth.

When a code is referenced in a state or municipal statute, it will usually specify a particular edition of that code since it takes a significant amount of time for a governmental agency to
adopt a code and the latest code will override the older editions. Codes have a long and proven record of success in the fire alarm and building construction industries, but have not been universally accepted in the disorganized and segmented security industry; an industry that has grown since its birth in 1970 without being encumbered with regulations or having to conform to municipal or state codes.

The New York City Department of Buildings, with its 1,300 employees, has over 800 plan examiners and building inspectors to ensure that the city’s 950,000 buildings are in compliance with all codes and statutes. The cost inherent in that endeavor is more than most other municipalities can bear.

An illustration of the complexity and restrictiveness of certain codes can be seen in the construction of a hospital complex in any major city. Architects on the staff of some of the nation’s largest firms consider getting the proper permits and approvals from a bureaucratic agency, like a Department of Buildings, more exasperating than if the buildings were to be constructed in a small rural community. A rural community would follow national codes rather than customized local codes and statutes. Negotiating through a maze of federal, city, and state codes is complicated enough, but working with government officials can be a frustrating experience, especially when state codes and municipal codes conflict or are interpreted differently by various plan examiners even within the same agency. In many situations, problems aren’t discovered until after a structure is built and occupied. One solution that has been tried to mitigate the disputes between agencies has been the creation of a universal hospital building code, which was endorsed by 28 state agencies.

A classic example in code enforcement was the construction of a neonatal intensive care unit where, just prior to full occupancy, the state building inspector refused to approve a 5-foot wide corridor leading to a storage room. The code required an 8-foot wide corridor, which is the width of an adult stretcher. Meanwhile, while bassinets are only 2 feet wide making a 5-foot corridor more than adequate. Widening the corridor would have cost $100,000 and months of delay before occupants could use the unit. The architect in charge of the project refused to comply with the inspector's demand and the matter was brought to higher-ranking government officials and the hospital threatened to initiate a lawsuit to remove the violation. Civil servants and code compliance officials at all levels simply do not like confrontations. They rely more on intimidation than negotiation and usually back down when a decision is challenged by a “logical explanation.” In this case, the corridor remained at 5 feet and the unit was granted a variance, opening on schedule. The original inspector was reassigned to less complicated projects. Codes are obviously important for any society to function, but they can be challenged and variances issued if a reasonable request is made that will satisfy all concerned parties.

- **FIRE CODES** are (usually mandatory) standards set up to prevent and protect from fire. They normally follow the National Fire Protection Association codes with a few exceptions where several of the nation’s largest cities combine the NFPA codes with certain modifications that reflect certain specific requirements of a particular municipality. For many years the fire code in New York City was customized according to the requirements issued by their fire department, but since 2009 the city’s fire code has more or less followed the NFPA’s codes.
Fire codes are continuously upgraded following a disastrous fire that results in a massive death toll. Four major fires that caused radical changes in fire codes, after it was determined that fires started because fire protection and signaling system were not in code compliance, are:

- Iroquois Theater
- Triangle Shirtwaist Factory
- Coconut Grove Restaurant
- Beverly Hills Supper Club

There has always been a strong interrelationship between fire and building codes, although their goals do not always align perfectly. Balancing both building construction codes and fire codes has placed a burden on the architectural community, who has to comply with both sets of codes. A fire code is considered a “model” code since it is adopted into law by a jurisdiction and enforced by municipal fire prevention officials. It prescribes minimum requirements relating to fire protection, explosive hazards arising from storage procedures, handling the use of dangerous materials or other specific hazardous conditions, and focuses on fire suppression equipment (sprinklers and smoke detectors) as well as specifies the schedules of inspection of premises and the fire prevention equipment (extinguishers).

- **LOCAL ORDINANCES** are generally produced through a process that involves a vote by elected officials (city councils), who then issue a “local law.” Sometimes the state will mandate minimum requirements that can supersede a local ordinance (a smoking ban in restaurants, gun control, medical marijuana dispensaries, to name a few), but the public usually adheres to local laws. A municipal code may be the interpretation of a local ordinance. In larger cities it is enforced by their department of buildings. It is revised slowly, with local laws periodically issued to amend the basic code.

After the tragic events at the World Trade Center on 9/11, certain changes were made to the building code, which had remained essentially the same since it was last revised in 1972. A new, revised code was issued in 2008 that reflected on the collapse of the Twin Towers and provisions were added in many areas concerning with factors that addressed emergency situations that might be caused by future disastrous events.

- **STATUTORY LAW** is used at the federal and state levels to cover the building code for fire and safety requirements, never for security purposes. It encompasses the written laws set down by, normally, a legislature. On non-federally owned property, authority rests with the state and local governing bodies who issues laws, ordinances, or statutes for specific situations.

- **RULES** should not be confused with “rulings” made by a judge or other decisions made in a judicial setting. A rule may not be enforceable since in that case it would make it a regulation or a code. A rule is usually an authoritative statement of what to do or not to do in a particular situation and may be issued by an appropriate person or organization. It often becomes a regular practice even informally, like a rule of thumb. While a rule could also be used to clarify or interpret a law or policy, in general it is just a little more significant than a guideline or tradition. Rules can become important over time simply...
due to repetition, which is best described as “according to Hoyle.” Edmond Hoyle died at
the age of 97 in London in 1769. While Hoyle did not invent rules, in 1746 he published
a treatise on the rules of whist, a widely played card game of the period. The manuscript’s
popularity led to the creation of rule books for other card games, the most notable of
which was poker 50 years later. Referring to Hoyle’s guidelines was used so often and
generally that “according to Hoyle,” became synonymous with appealing to somebody
deemed an authority on a subject.

Sometimes certain rules can create problems when they are old and have not been upgraded to be
meaningful when applied to modern day society. In the security community, rules are too vague
and serve no purpose unless they are in written form, published by a respected organization, and
most importantly, there is a penalty involved if a rule is broken. Rules can be divided into four
categories:

**Folklore** - Conveyed by behavior and are implicitly understood.

**Guidelines** - Commonly published as recommended practices. Advisory or informative in
nature, they can be interpreted differently at times and do not have the force of law.

**Mandates** - Commands that cannot be ignored; violators are punished.

**Policies** - rules of expected behavior with leeway allowed under certain circumstances regarding
violations.

**SUMMARY**

There has been a steady but revolutionary change in the way locking hardware is selected for a
new structure and has caused the local locksmith “keymaker” to gradually fade into obscurity
like the TV and typewriter repairmen. While the selection of the hardware for any entrance door
is still one of the most rudimentary component of a security system, it is no longer limited to
simple mechanical hardware and requires the knowledge that a trained engineer and architect can
provide. Access control technology has become complicated with the introduction of the
magnetic stripe card reader in the 1970s, the proximity reader of the 80s, and now the use of
digital communication devices (smartphone and the cloud) to monitor the identity of the user and
store the event of each door openings.

The engineer and architect have to participate in the design, the selection and the installation
process of a controlled entrance. They need to replace the locksmith and the salesmen from the
alarm installation company (or the building security director) because none of these
aforementioned have the level of education to understand the intricacies and complexities of a
new age access door control system. Most large complexes have begun to rely on the IT people
for selection of security systems but they are more concerned with bandwidth than door controls
which has caused a vacuum in in a field that must be filled by engineers, a group that has not
keep up with the latest technology.

The courses offered under the “Security Practices & Engineering Concepts” is intended to
expose some basic security topics but the reader is urged to attend a security conference and
exhibition to learn more about the state-of-the-art in the door control field. The information to
make an intelligent choice of security systems cannot be found in Home Depot of from the
clueless integrator salesmen or the obsolete and disappearing locksmith.
The most informative conference is the week-long annual meeting of the American Society of “Industrial Security (ASIS) that displays over 2,000 systems and state-of-the-art devices that attract over 20,000 attendees every year.