SECURITYIN30
LIVE WITH ALLEGION

The Risks of Aging Control Systems and How to Address Them

August 21, 2020

Question & Answer with Brian Marris & Jake Fergerstrom

Q. Why is deploying a mobile credential solution worth the extra money in hardware compared to transitioning to smart credentials.

A. This will be a customer by customer decision; in some cases, it isn't worth making the jump to a mobile credential depending on the needs and desire of the customer or end user. Some reasons for spending more money up front include:

- Future proofing for the potential to upgrade to a mobile credential solution in the future
- Eco friendly solution because it eliminates the need for the plastic credential
- Some Universities and multifamily complexes will use it as a value-add proposition

Q. Do wireless locks come with LBS?

A. Wireless locks do not often include a latch bolt sensor (LBS aka LX) but always have a request to exit sensor (RX) and door position switch (DPS). In an event where a strike plate is taped over for repeat access, an RX or DPS would not directly be able to detect this occurrence. However, all-in-one E-locks look for an order of events to remain in a normal state. When in the locked state, the E-lock looks for a valid credential presentation (reader) then the door to open (DPS). If a strike is taped and the door is pushed open without a valid credential read and only detects a door position change, the E-lock will respond with a "door forced" transaction. When properly flagged in your Access Control System (PACS) the door forced alert can trigger a personnel response to investigate.

Q. How long does it take to perform a lock down using wireless locksets?

A. Lockdown time is unique to each wireless product and the technology the wireless product uses. For WiFi locks, there is often no lockdown capability because the lock needs to wake to communicate with the network and this is often limited to a scheduled wake or a certain occurrence (like a door forced condition) from the lock's side. Bluetooth Low Energy locks communicate every 5-7 seconds, so you can expect a lockdown command to take a maximum of 7 seconds to reach the lock, though it could take as little as 1 second depending on when the command was initiated and when the lock's next communication pulse occurs. There are several types of 900 MHz solutions on the market. The Schlage 900 MHz wireless lock sends normal communication on a scheduled heartbeat while also waking on any user interaction (credential presentation, lever turn, etc.). In the PACS integration process, lockdown commands are specifically programmed to a separate sub-frequency that forces the lock to wake and respond. This occurs every 10 seconds by default but can be adjusted. This configuration is the ideal balance between responsiveness and battery life.

Q. **How do we know a wireless lock will reach a hub?**

A. Most manufacturers offer a way to test or simulate the range of a deployment using a wireless range test kit. These test kits are very helpful in existing buildings, and a strong indicator at the core and shell phase of new construction. If hub and lock placements are being created in the planning phase of new construction, it is prudent to adhere to manufacturer recommended ranges and placement guidelines. We also recommend having a few wireless hubs in attic stock on hand in a case where a lock is not reaching the hub. Finally, including service loops in your hub wiring will allow you to relocate the hub slightly for a better connection. Sometimes just a few feet will do it.

Q. **Why are there certain consultants that are against using wireless technology even though it is more cost effective?**

A. There are many arguments for or against wireless technology based on a variety of factors. Many times, certain consultants are hesitant to utilize wireless technology because they aren't comfortable with the technology, are extremely comfortable with wired technology with limited or no issues or have had one or two bad experiences that make them avoid it. Wireless technology can be a cost effective and convenient solution, but there are other factors that must be taken into consideration such as connectivity, environmental conditions and site management knowledge of wireless technology to name a few.

Q. **Can Wiegand cables be re-used for OSDP?**

A. This varies from manufacturer to manufacturer, so the key is do some research and understand first if the reader has RS-485 and is OSDP capable. Then it is important to understand how you correctly wire the reader up to use OSDP communication. Next, make sure the panel or single door controller is capable of handling RS-485 and OSDP communication. Lastly, be sure to understand what integrations are completed with specific access control platforms to understand if other features, outside of the encrypted communication, are available for use.

Q. **Wireless locks are highly proprietary and non-changeable, please address.**

A. Depending on the wireless lock they can be proprietary and not interchangeable. There are a couple of factors that play into this issue. The first is door prep for the lock. There are common door preps and most wireless locks in the market can fit into those common door preps with some additional prep for the electronics. The next factor is communication and integration requirements. Many times, these communication protocols and integration requirements are unique to each manufacturer because of the different technologies used and because there is no industry standard for easy and simple integration, with an access control platform, for example. Lastly, when moving to smart and mobile technology, to provide the appropriate level of security, each lock must have a key to assure the credential being presented has permission to pass along data. These keys must be protected and can make it difficult to drive interoperability. If the smart technology used is open, like NXP MIFARE technology is open for smart credentials, there is opportunity for interoperability between different wireless locks if there is a secure way to leverage the key on other hardware. It is best to engage with your manufacturer to discuss options.