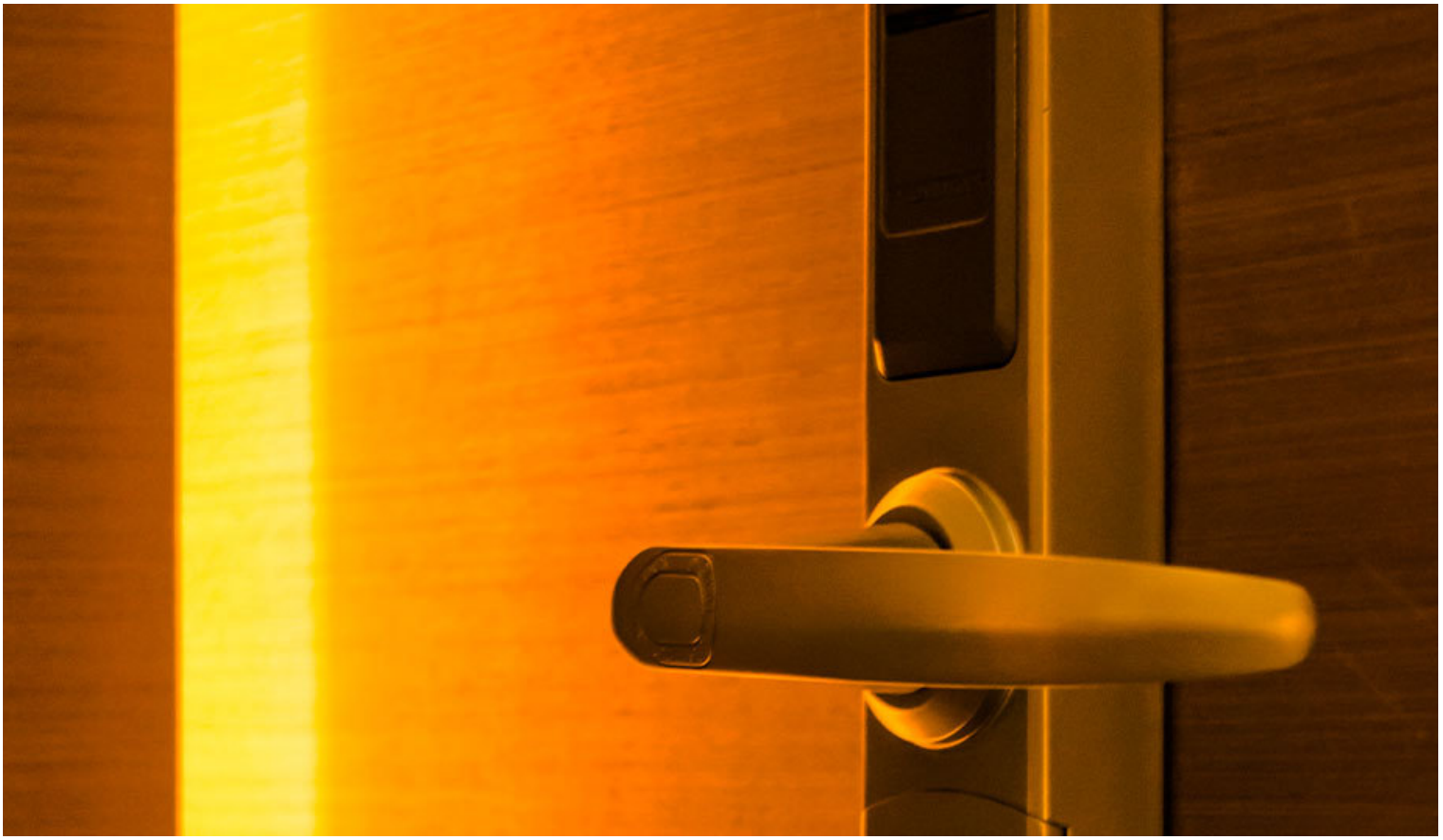
Open Supervised Data Protocol (OSDP): the gold standard for access control installations

Published on 1 Feb 2019



Today's security industry technology standards create a common framework for achieving predictable performance. Systems are made more secure and easier to install, use and integrate with other devices. Standards are also intended to be living documents, open to continual refinements to benefit manufacturers, integrators and end users.

An excellent example is the Open Supervised Data Protocol (OSDP), which is now the industry's gold standard for physical access control installations. It was designed to offer a higher level of security with more flexible options than the aging defacto Weigand wiring standard.

Updating OSDP-readers simultaneously

> One recent addition enables end users to push firmware and software updates to thousands of OSDP-enabled card readers simultaneously

OSDP, first introduced in 2011 by the Security Industry Association (SIA), continues to evolve with significant manufacturer input. One recent addition enables end users to push firmware and/or software updates to a few or thousands of OSDP-enabled card readers simultaneously. Weigand technology requires updates to be made one at a time at each reader.

Regularly changing reader encryption keys is an excellent way to enhance facility security. It's easy using the OSDP file transfer capability and the latest DESFire EV2 credentials containing multiple encryption keys. You can transfer the next code on the card to all readers and the job is done. And there's no need to create a new card for each user or reprogram each individual reader.

AES-128 encryption ensures cybersecurity

It's time to migrate entirely away from Weigand technology. If greater security, convenience and reduced labour from the latest OSDP updates isn't reason enough, here are a few more things to consider.

- The 40-year-old Weigand protocol provides no signal encryption, making it easy for hackers to capture the raw data transmitted between cards and readers. OSDP readers support AES-128 encryption while providing continuous monitoring of wires to guard against cybercriminals.
- Weigand reader installations require homerun cable pulls from the control panel to each peripheral device. OSDP readers can be daisy chained, providing additional savings on cabling and installation time.

> Weigand technology is simply too slow to work with today's most versatile and secure card technologies. OSDP readers work with virtually all modern access control cards. The OSDP standard also works with biometric devices; Weigand does not.

Meeting requirements of FICAM guidelines

> SIA is pushing to make the latest OSDP version a standard recognised by the ANSI, a move to enhance the global competitiveness of U.S. security businesses

Also, OSDP is becoming a must-have standard for organisations demanding the highest security levels. The standard meets requirements of the Federal Identity, Credential and Access Management (FICAM) guidelines that affect how the access control industry does business with the federal government.

SIA is pushing to make the latest OSDP version a standard recognised by the American National Standard Institute (ANSI), a move to enhance the global competitiveness of U.S. security businesses.

There's still a large worldwide reader installation base that works solely with the Weigand protocol. Admittedly, changing them all at one time may be prohibitively expensive; however, standards should be viewed as a journey, not a destination. That's why a measured migration is the right choice for many organisations. Begin by securing the perimeter.

Replace only the outside-facing Weigand readers. As long as the walls are secured, the inside can remain a softer target until OSDP-compatible readers can be added indoors. The case for moving to OSDP as a standard is compelling. It offers our industry the opportunity to design access control software and products that provide what end users want most – greater security, flexibility and convenience.

Author Profile

Greg Berry

You may also be interested in...

Unlocking profits for integrators in the ever-evolving world of access...

Whether you are a veteran in the access control world or have never installed a card reader before, there are always ways to increase profit...

Why aren't the Federal Government's Physical Access Systems compliant...

In the wake of 9/11, the Federal Government's secure-the-fort, big idea was to create an identity credential for all federal employees...

Access Control as a Service (ACaaS) solutions growth with mobile acces...

IHS Markit projects that the market for physical electronic access control solutions has grown to over $5.2 billion in 2018. The market has...

Debunking the myths of the security of access control systems

It's not surprising that people are nervous about the security of newer technologies, many of which are part of the Internet of Things...