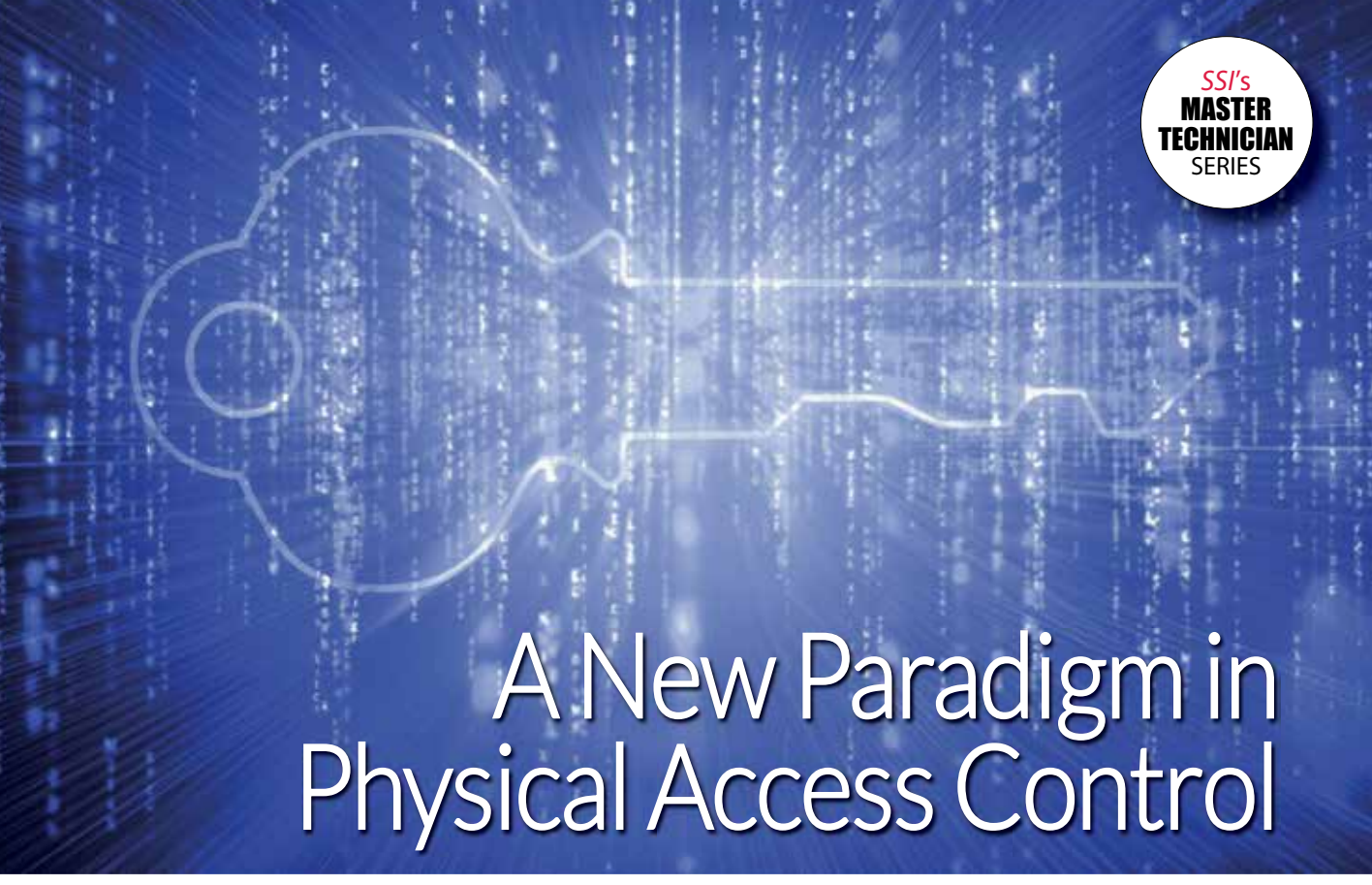


SSI's MASTER TECHNICIAN SERIES

A New Paradigm in Physical Access Control

Open Supervised Device Protocol (OSDP) is enabling better integration of security systems to support advanced applications and data encryption. OSDP could one day supplant the Wiegand standard for its ability to add significant feature sets.

By the Editors of *Security Sales & Integration*

Tectonic shifts in technology and applications are defining the new normal in the security marketplace. This has created a major change in focus for manufacturers and integrators alike that continue to be challenged by the frenetic pace of meshing rapidly advancing security technologies with IT/IP know-how.

In recent years, the phenomenon has pushed many organizations and other industry groups to take the lead in developing actionable security protocols that are extensible to the progressing IT-centric landscape. In short, the industry craves specifications that it can implement sooner rather than later. Case in point: physical access control systems (PACS).

The access control industry has made remarkable advances throughout the past three decades, and yet one area that has remained essentially unchanged is the way that readers are connected to access control systems. "Swipe" readers popularized the Wiegand (D0/D1) interface for PACS in the 1980s. Early RFID readers, introduced in the 1990s, further expanded the use of the Wiegand protocol by following the wiring scheme already common to many installations. Ultimately, the Wiegand interface became one of the access control industry's first standards with creation and release of a complete specification by the Security Industry Association (SIA) in 1996.

As technology advanced and users' security needs grew increasingly more critical, the imperative for a new open communications standard in the PACS industry became massive. Its fruition would have the potential to lower costs, enable interoperability, stimulate systems integration and improve security.

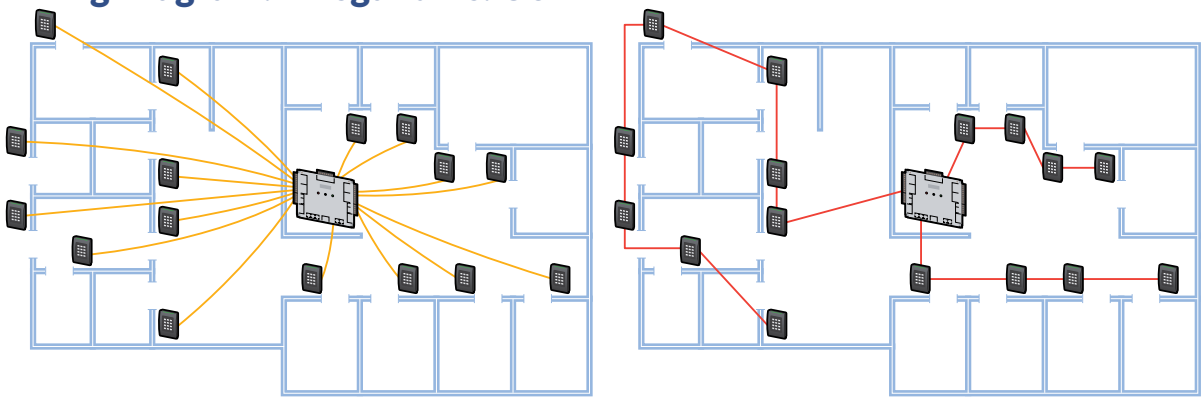
With that preamble, welcome to the latest installment of *Security Sales & Integration*'s Master Technician series. Brought to you by HID Global, this article is intended to educate readers about the genesis of the Open Supervised Device Protocol (OSDP) and its forthcoming impact on the industry.

OPEN, ROBUST STANDARD

Let's first delve into some historical perspective to compare and contrast legacy PACS to platforms based on the latest open standards.

Wiegand and clock-and-data (commonly used with magnetic stripe cre-

Wiring Diagram: Wiegand Vs. OSDP



The wiring diagram above depicts how the Wiegand protocol requires homerun cable pulls from the control panel to individual peripheral devices. OSDP is flexible to support either homerun cable pulls or the daisy-chain methodology, depicted on the right.

dentials) interfaces have much in common. They are both point-to-point, unidirectional protocols that utilize two wires to send a series of data bits from the reader to the system's control panel. Point-to-point means that only one reader can be connected to an interface circuit. Plus, they provide no means for the system to send data to the reader, nor to request data from the reader. If data does need to be sent to the reader, additional discrete wiring is required.

This unidirectional communication scheme has several drawbacks. Because the system is not able to request status from the reader, there is no way to determine the state of the reader other than by using additional circuitry or by simply waiting for the end user to issue a complaint. Another weakness is that all device connection points must be continually ready to receive data in an unsolicited manner, frequently necessitating dedicated buffering circuits or high-speed parallel interrupt processing. Since there is no flow control capability, multidrop configurations are impractical due to the high risk of collisions and the impossibility of requesting a retransmission should a collision occur.

More than anyone, John Wiegand revolutionized the PACS industry in late 1970s with several new inventions based on his patented "Wiegand Wire." The inventor created the Wiegand card by embedding 26 small pieces of wire within the base of the credential. His Wiegand reader was designed to interpret the arrangement of the wires as the card was swiped. He also developed the Wiegand protocol as a way for the reader to send card data to the system where authorized credential values were stored. Wiegand's inventions were very successful throughout the '80s and '90s. Since then most of the products he originated have been replaced by next-generation devices which leverage advancements in technology. The Wiegand interface is his only contribution that remains unchanged and mainstream in the industry today.

Despite widespread adoption, there remain limitations and vulnerabilities to the technology. For instance, there is no encryption on the protocol, which could allow hackers to intercept data transfers from the reader or "spoof" a card read on the control panel.

Wiegand-based systems have also been deemed too slow and insufficient for 200+ bit data transfer needed by the new Personal Identity Verification (PIV) data model. Because Wiegand systems do not allow for central management of all readers, these systems can be costly to maintain. A dedicated, homerun wire is required for each reader since there is no serial/addressed communication. Cable runs are limited to 500 feet and additional conductors are needed to provide monitor/control functionality.

Given such limitations it has become increasingly clear that for reader technology and capabilities to progress, a bi-directional connection between the reader and access control system is a necessity. Some access control and reader manufacturers have recognized this need and developed proprietary bidirectional solutions. However, the development and training investments made in proprietary solutions slows the advancement of interoperable solutions and reduces the available market. An open, far more robust solution is especially needed for larger applications.

Enter OSDP, a nonpriority interface specification that can be implemented without restriction. The protocol was originally developed by HID Global and Mercury Security Corp. in 2008 and adopted by SIA as a standard in 2011. SIA formed OSDP working groups, open to all members, and subsequent contributions have been provided by those participants.

The OSDP specification is a communication protocol for interfacing peripheral devices, such as card readers, to control panels or other security management systems. It is expected to replace the Wiegand interface in many applications that require larger data sizes, two-way communications and/or encryption. Smartcard deployments, public key infrastructure (PKI)-based systems and identity management applications are all examples where these requirements come into play.

The OSDP standard with Secure Channel Protocol (SCP) will support both IP communications and point-to-point serial interfaces, such as RS-485. The serial version of the protocol has been fully adopted by numerous manufacturers and others are in the development stages of implementation.

BI-DIRECTIONAL COMMUNICATION

The access control industry's move to open standards is cultivating a broad range of interoperable products with enhanced features and security. Open standards also ensure that solutions can be easily upgraded to support changes in technology and applications, and give users the confidence that investments in today's technologies can be leveraged in the future.

OSDP with SCP specification provides bi-directional communications and security features for connecting card readers to control panels or other security management systems. This improves integration to support advanced applications and data encryption between components. Bi-directional communication is particularly beneficial for enabling users to change configurations and to poll and query readers from a central system, which reduces costs while speeding and simplifying configuration and improving the ability to service readers.

Unlike earlier unidirectional protocols, including the Wiegand interface and the clock-and-data signal approach used with magnetic stripe readers, OSDP enables continuous reader status monitoring. It can also immediately indicate a failed, missing or malfunctioning reader, as well as provide tamper detection and indication capabilities. All signaling is done over two data lines, providing the ability to use four-conductor cable to both power the reader and send and receive data. This lowers installation cost compared to the 6 to 10 conductors typically used for Wiegand.

The addition of SCP to OSDP has brought strong authentication capabilities that enable secure communications and connections. SCP was developed by Global Platform, a standards body that works across industries to identify, develop and publish specifications that facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. To establish a session using SCP, the reader and control panel are mutually authenticated with each other and a set of keys are established for the session. The secure channel is then terminated and session keys destroyed whenever any error is detected in the SCP.

HID Global is one of the first manufacturers to support OSDP with SCP in its reader portfolio as part of its iCLASS SE platform. iCLASS SE platform readers with OSDP enable central management, which lowers operational costs by making them faster and easier to configure and service.

ENHANCING INTEGRATION

Going beyond the unidirectional Wiegand interface, OSDP provides continuous monitoring of reader status, and can immediately indicate a failed, missing or malfunctioning reader. OSDP can also provide tamper indication for readers with onboard tamper detection capabilities. Further, the OSDP standard documents a protocol for control panels to send messages for display to a cardholder via a screen embedded within or connected to the reader.

The need for such a specification is considerable. This is especially true given the U.S. Federal identity and access management space requires secure communications between the PIV/I card edge and any reader/controller that is intended to authenticate such a credential.

Let's review just some of the key ways an open communications standard could impact systems integrators' ability to expand their PACS projects:

Grow your business. Integrators can differentiate from the competition by promoting open standard protocols, which can help build new customer relationships and win more projects by providing newfound PACS features.

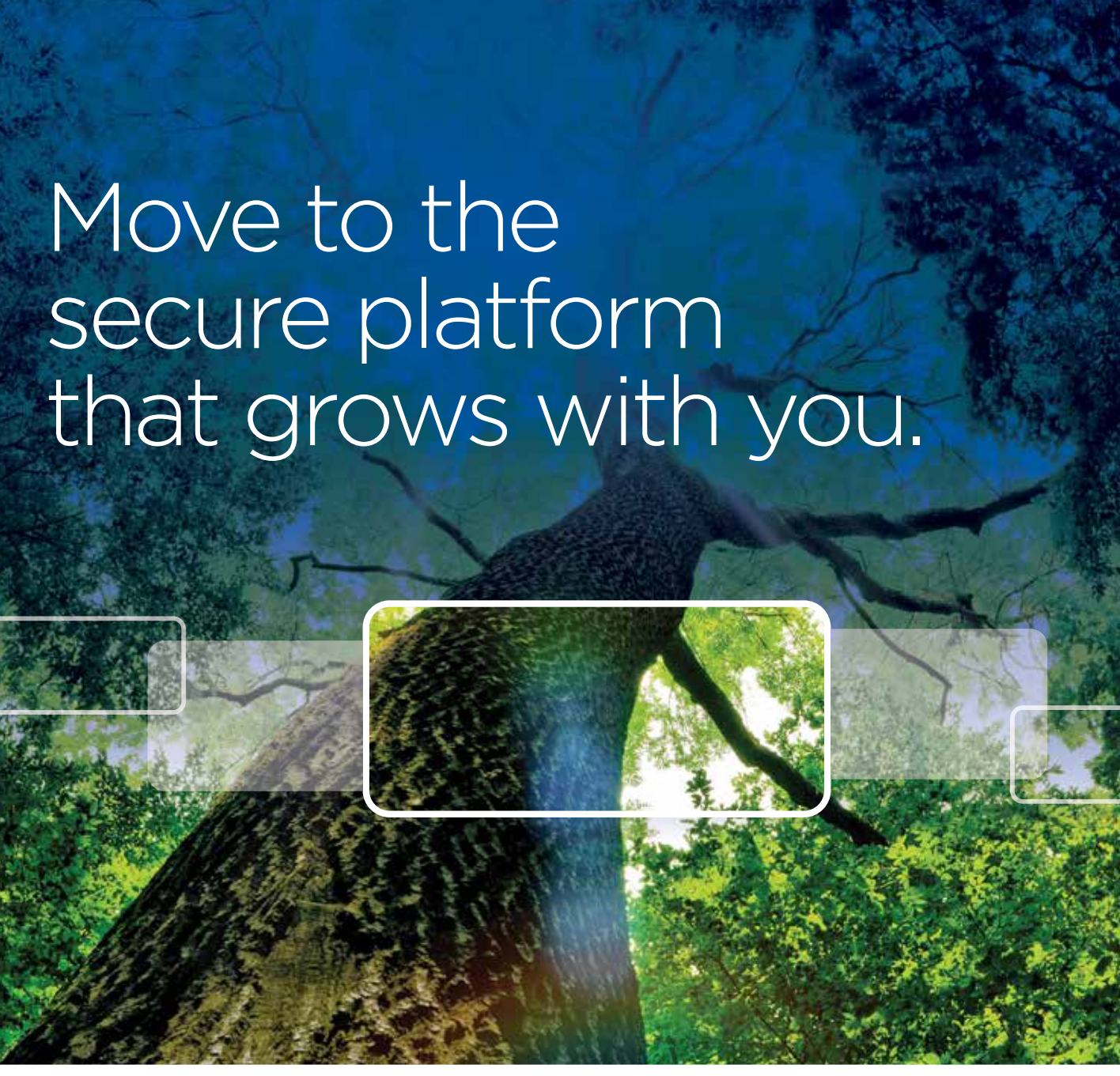
Reduce cost and gain efficiency on installations. Run fewer conductors to each reader. With OSDP only four conductors are ever needed, two for power and two for all communication. With Wiegand, readers can require as many as nine conductors (two for power; two for Wiegand communications; red and green LED; tamper; beeper; RF hold) and still only achieve a small subset of the capability possible with OSDP.

Reduce cost and gain efficiency on service and maintenance. Wiegand does not allow for remote configuration or upgrade of a reader. OSDP enables a customer to remotely change the configuration of a reader (i.e. security keys or LED color) from any network-connected location.

OSDP with SCP and other industry standards will continue to play an increasingly important role in the PACS industry. Those systems integrators that hope to play in this field will be compelled to attain the skills and knowledge necessary to deliver these highly adaptable solutions.

AN OVERVIEW: OPEN SUPERVISED DEVICE PROTOCOL (OSDP)

- Protocol for secure communication between field devices in physical access control systems
- Created by HID Global and Mercury Security Corp. in 2008 with subsequent contributions by other industry leaders
- Adopted by Security Industry Association (SIA) as a standard in 2011
- Primary current function for communication between reader and control panel
- Medium independent but current primary medium is over RS-485 (two-wire copper protocol)



Leverage HID Global's extensible iCLASS SE® Platform to keep your access control optimized, today and tomorrow.

HID®

With constantly evolving access control concerns and demands, how can you ensure your investments today will be operable tomorrow? Go with the new standard in access control—HID Global's iCLASS SE® Platform, the open and adaptable solution that easily integrates smart cards, mobile devices and whatever tomorrow brings, for greater security and flexibility. Now no matter where technology goes, your access control is always growing with you.

Learn more about the iCLASS® SE Platform's advantages at hidglobal.com/grows-ssi