CYPRESS
INTEGRATION SOLUTIONS

OSDP™ Solutions

The Cypress toolbox of OSDP solutions: for a frictionless upgrade to the SIA OSDP standard.

OSMIUM™ OSDP-Ethernet Bridge

The Cypress OSMIUM OSDP-Ethernet Bridge securely connects IT and access control by bridging OSDP and the internet. Use the Bridge to connect a reader to an access control system via Ethernet, to securely manage an access control point with a host computer control program. Also available with general I/O control for door control and monitoring devices.

Encrypted Wireless Handheld Reader with OSDP v2 Secure Channel

The Cypress Encrypted Wireless Handheld Reader incorporates OSDP v2 Secure Channel with AES-128 encryption to secure the wireless connection against playback attacks. The reader verifies credentials by connecting wirelessly to an existing live database through its base unit. Select models offer handheld control of a relay function, such as opening a door or triggering a duress alarm.

CE certified

OSMIUM Lite embedded OSDP-Wiegand conversion module

The OSMIUM Lite OSDP-Wiegand Conversion module is an embedded solution which allows manufacturers to add OSDP to their readers or other access control devices.

OSMIUM OSDP-Wiegand Converter

To easily migrate a legacy access control system to OSDP, use the Wiegand-OSDP converter board. The OSM-1000 Converter connects an OSDP reader with a legacy Wiegand access controller.

OSMIUM Crystal OSDP-Wiegand panel converter

The OSMIUM Crystal Converter offers all the benefits of the OSM-1000 OSDP-Wiegand Converter in a compact form factor.

2018_09_24

1778 Imlay City Road, Lapeer, MI 48446 800-807-2977

MADE IN USA

RoHS

SIA's Open Supervised Device Protocol (OSDP) v2.1.7 communication standard benefits

Security: OSDP Secure Channel halts Wiegand hacking with AES-128 encryption

Interoperability: Mix-and-match devices to help future-proof systems

Functionality: 2-way communication, access control that withstands the elements, multi-drop installations, 2 wires instead of 10+

Communication: With OSDP's 2-way communication, the panel can query readers to find out capabilities, without physically reconfiguring devices. The panel is alerted if the reader does not answer its query.

Savings: OSDP is scalable. It supports many more devices – and many more types of devices (such as readers, strike sensors and alarms) – than the Wiegand protocol.

Learn more at OSDP-Connect.com or CypressIntegration.com/OSDP

What is OSDP?

The Open Supervised Device Protocol (OSDP™) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP v2.1.7 is currently in-process to become a standard recognized by the American National Standards Institute (ANSI), and OSDP is in constant refinement to retain its industry-leading position.

Why specify or adopt OSDP?

Already in wide use by many leading manufacturers like Cypress, HID Global, Mercury and others, the Security Industry Association encourages broad adoption of this standard and recommends specifying OSDP for any access control installations that require real security and/or will be used in government and other higher security settings. It is particularly valuable for government applications because OSDP meets federal access control requirements like PKI for FICAM.

Source: Security Industry Association
From https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/

OSDP prevents Wiegand hacking

To see how easy it is to hack an access control system, Google any of the following phrases:

- Wiegand reader hack
- Wiegand reader security flaw
- Wiegand reader vulnerability

Hackers can slip a skimmer into many readers - even some readers with advanced technology - and within seconds harvest credential information to sell or access a facility and deny access to authorized personnel. Hacking a physical access control system can compromise lives, safety and assets.

To protect access control systems from hacking, OSDP with Secure Channel uses AES-128 encryption, so data is not exposed to hackers.