OSDP in Enterprise Settings: Lessons from the Front Lines

JASON HART, CEO, FOUNDER at Safetrust

SAL D'AGOSTINO, FOUNDER at IDmachines LLC and Surveillance Trust

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

Session Objectives

- Identify key benefits and challenges of OSDP.
- Explain security enhancements provided by OSDP.
- Discuss OSDP's role in future-proofing access control.
- Compare OSDP with Wiegand.
- Share lessons learned from large enterprise OSDP deployments.

What is OSDP?

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 was approved as an international standard by the International Electrotechnical Commission in May 2020 and has been published as IEC 60839-11-5.

Source: Open Supervised Device Protocol (OSDP)

The latest version 2.2.2 was recently published by the OSDP Technical Subcommittee which maintains the standard.

Source: Security Industry Association Releases Version 2.2.2 of SIA Open Supervised Device Protocol Standard - Security Industry Association

What Does Being OSDP Verified™ Mean?

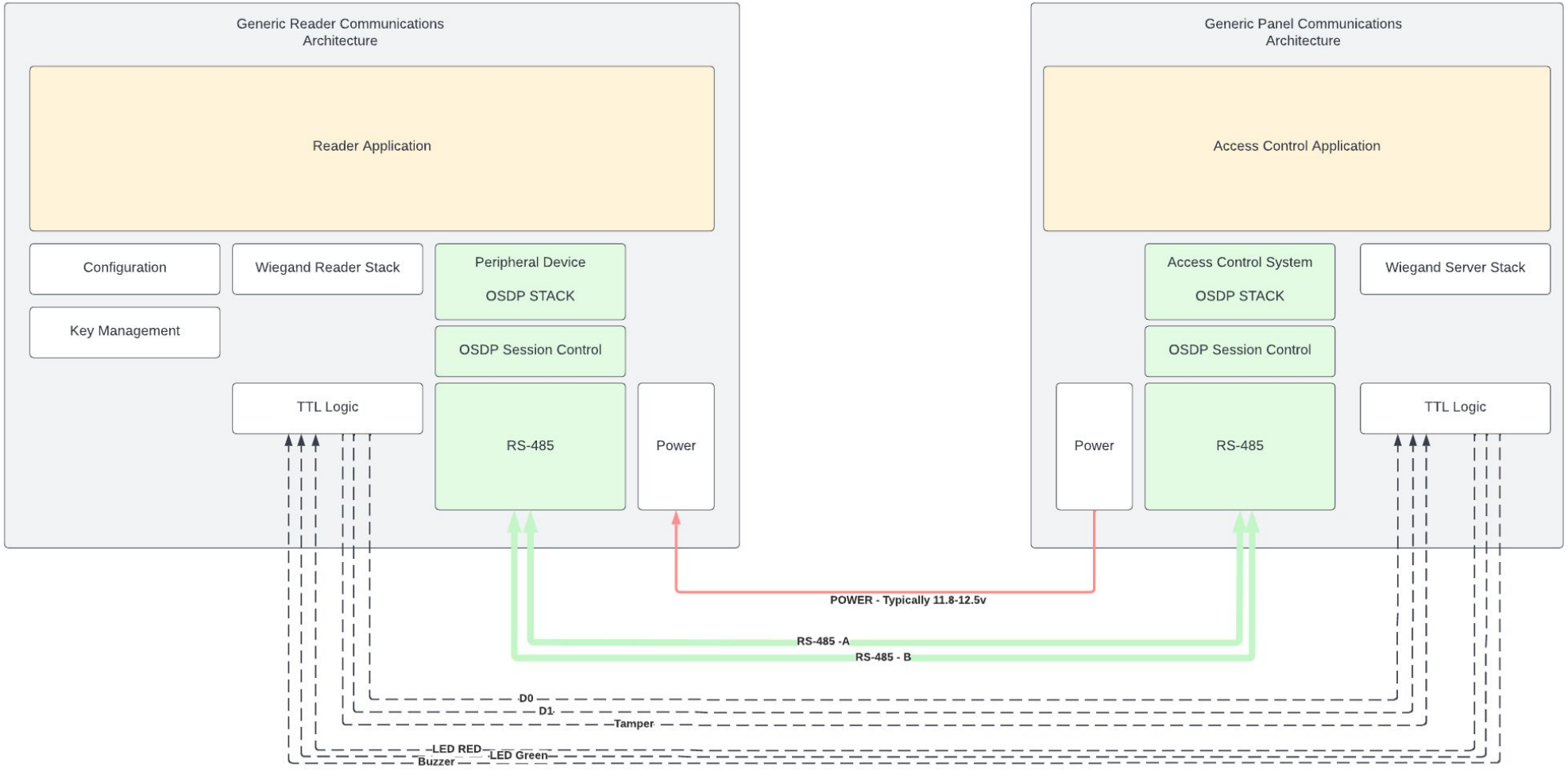
SIA OSDP Verified™ is a comprehensive testing program that validates that a device conforms to the SIA Open Supervised Device Protocol (OSDP) standard and the related performance profiles.

The SIA OSDP Verified™ mark instills confidence in integrators, specifiers and practitioners that OSDP devices will work as intended for various types of access control use cases.

Over 100 products from 25 companies from North America, Europe, Asia, and Oceania have been certified.

The program has been highlighted at cybersecurity conferences as essential to the security and compliance of physical access control systems by independent 3rd parties.

OSDP Basic Architecture



OSDP vs. Wiegand: Comparative Analysis

OSDP	Wiegand
Managed	**Unmanaged**
Bi-directional communication	**One-way** communication
Secure communication (AES-128)	**Unencrypted** communication (susceptible to man-in-the-middle and replay attacks)
Two-wire communication ($) (and can use existing or new cable in most cases)	**Four-wire communication** ($$$)
Up to **~1000 ft** cable distance. Extendable with RS485 repeaters.	Up to **~500 ft** cable distance **Up to 1000 ft with 18 AWG based on conditions.
Multi-drop enabled	**Point-to-point** only
Reader **offline detection**, other **health, diagnostic, and troubleshooting data**	No status of reader at panel, **offline reader only detected when cards don't work**
Link layer protocol	No link layer protocol

OSDP vs. Wiegand: Key Questions

What are the limitations of Wiegand that OSDP addresses?

- Lack of Encryption
- One-Way Communication
- Limited Data Capacity
- No Device Authentication
- Distance Limitations
- Interoperability Issues
- High Maintenance Costs

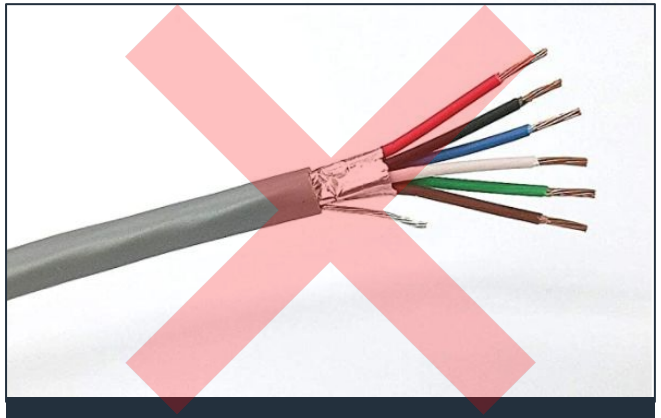
In what scenarios might Wiegand still be preferred over OSDP?

- Legacy System Compatibility
- Lower Upfront Costs
- Simple Installations
- No Need for Advanced Security
- Short Cable Runs
- Minimal Interoperability Concerns
- Quick Deployments

Key Question:
Can I use my existing Wiegand cabling?

OSDP

Rated Cable



RS485 specifies

twisted pair cabling

Both will function over solid core wiring, but it's not optimal, as speed and distance may be affected.

However, OSDP with RS485 operates at a lower speed of 9,600–115,200 bps, with most installations running at 38,400 bps, compared to 4 Mbps or 10 Gbps.

Key Advantages of OSDP: Security, Communication & Compatibility

Secure Communications

OSDP encrypts data transmitted over RS-485, preventing wire taps from exposing cardholder information.

Bi-directional Communication

OSDP enables two-way communication between a panel and a reader, supporting real-time status, diagnostics, and the ability to send commands and updates from the panel to the reader.

Interoperability

As long as each OSDP device is SIA-certified as **OSDP Verified**, compatibility validation isn't needed, and readers and panels will work together seamlessly.

Challenges of OSDP: Complexity, Cost and Existing Systems

Implementation Complexity

Deploying OSDP may require specialized knowledge and additional configuration compared to legacy protocols.

Cost Considerations

Upgrading to OSDP can involve higher initial costs for compatible hardware and installation. Like anything with encryption, there are higher service costs to reset encryption when replacing devices.

Interoperability with Existing Systems

Integrating OSDP with older infrastructure may require additional upgrades to ensure compatibility.

Key Questions

What are the primary drivers for adopting OSDP in enterprises?

- Demand for Modern Security
- Improved Device Communication
- Interoperability & Standardization
- Operational Cost Savings
- Regulatory Compliance

How can organizations overcome implementation challenges?

- Plan for Expertise & Training
- Gradual Migration Strategy
- Use OSDP Verified™ Devices
- Leverage Open-source Tools
- Budget and Justify Upgrades
- Utilize Gateway Converters
- Test & Validate Before Full Deployment

Lessons Learned from Large Enterprise OSDP Deployments

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

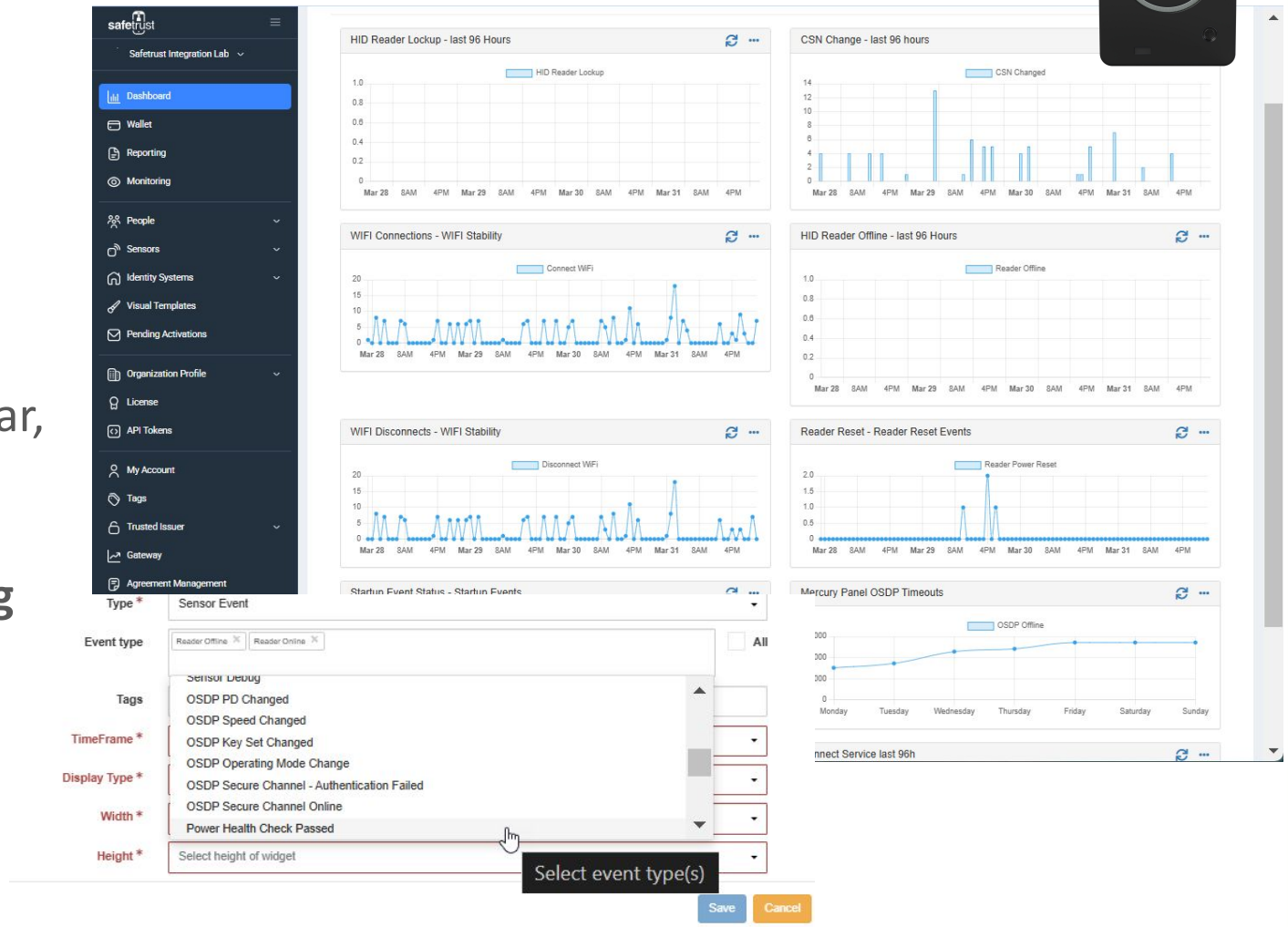
Unique Insights Into Global OSDP

Global OSDP Deployments

- 300k end points
- 30+ countries
- 100+ SIs
- 20+ wiring configurations
- Multiple vendors OSDP implementations (Mercury, iStar, etc.)

WiFi Connected Readers Reporting

- OSDP statistics
- Power/DMM/TDR
- Health
- Security changes



In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

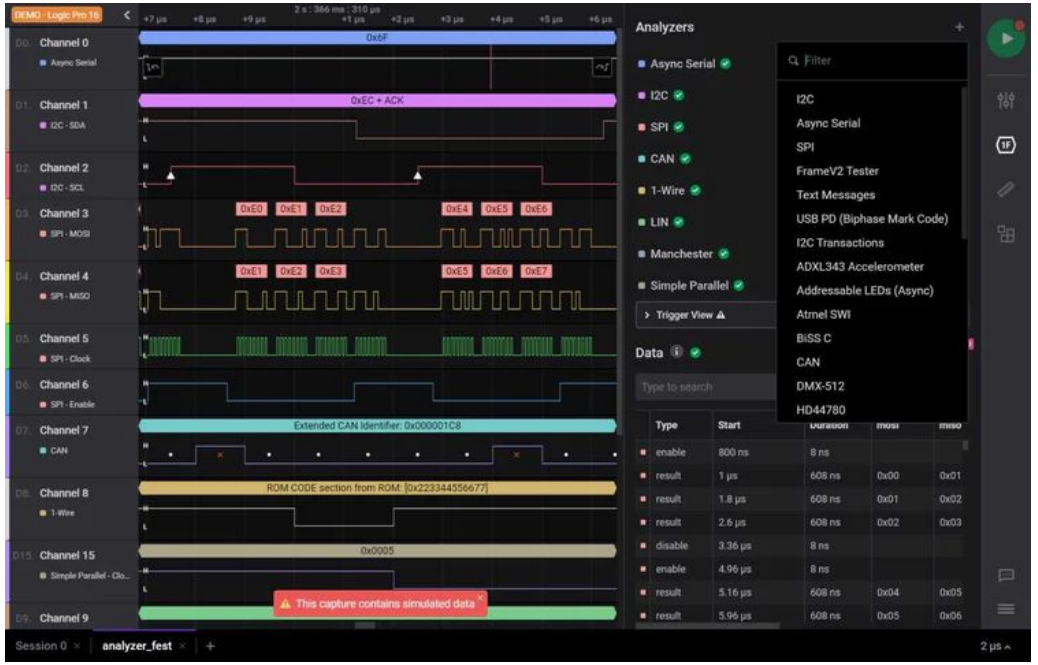
Your Second Best Friend - Logic Analyzer

12v Power

- Over time and operation
- Measure at both ends

3-5v Communication Line

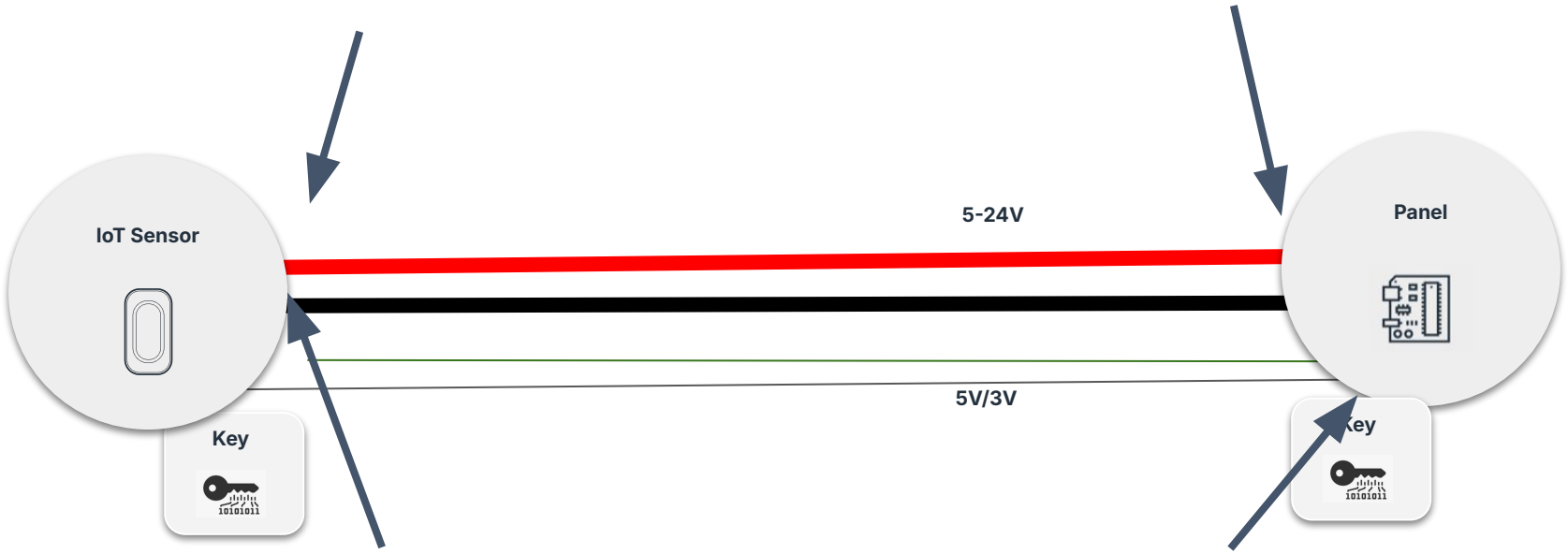
- Noise on line
- Each line is inverted
- Measure at each end of the cable

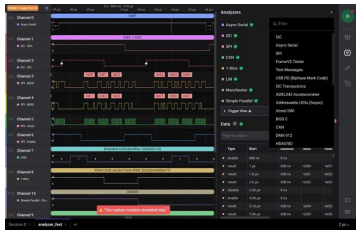


Pull Ups and Termination

- As a general rule, don't.
- Devices self sense or software control.
  Early devices may, but confirm with trace.

Simple OSDP Installation

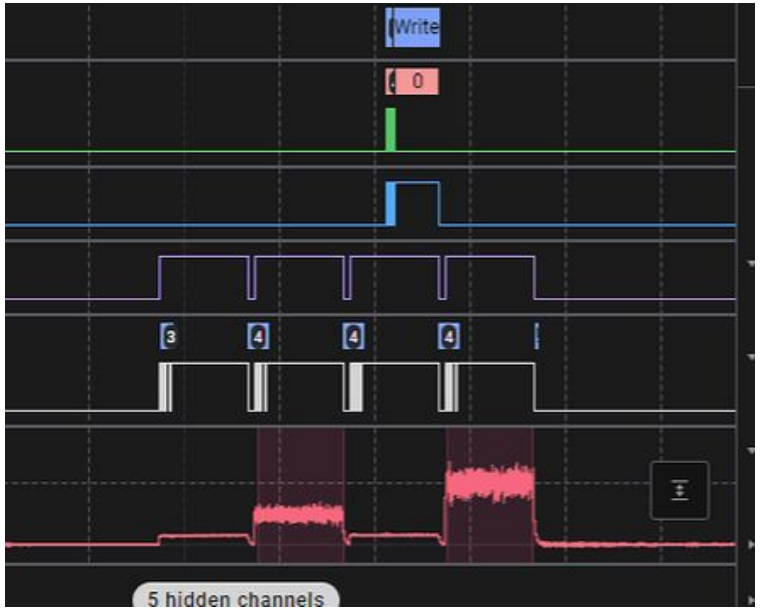


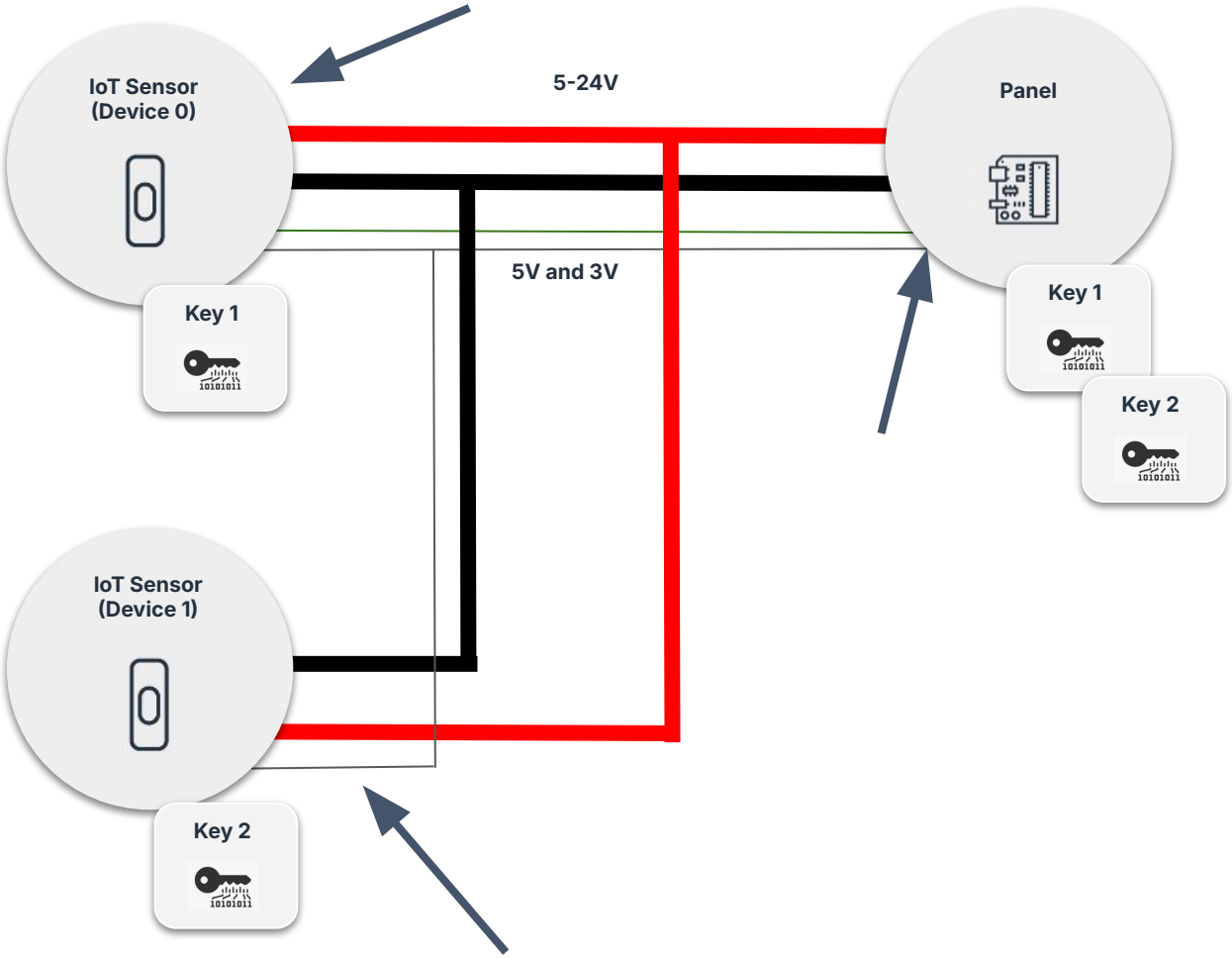


A simple multimeter isn’t sufficient to diagnose problems.

Multi-Drop OSDP Installation

Each device is polled individually. If device 1 goes offline, device 0 may appear slower to respond as a result.





Avoid Deployment Pitfalls

What are the most common pitfalls during OSDP deployment?

- **Training**
  OSDP and RS-485 are powerful—but they do require proper training. Diagnosing issues can be complex. (**Pro tip:** Check out the SIA Boot Camp.)
- **Wire Gauge**
  Avoid using small-gauge 24 AWG wire. Many devices draw more power than 24 AWG can deliver over distance. Use a minimum of 22 AWG—but for high-power devices, go with twisted pair 18 AWG.
- **Power, Power, Power**
  Underrated power supplies are a common issue. Twisted pair wiring can't defy the laws of physics—remember that voltage drops over distance, especially with 24 AWG. Also, RS-485 doesn't define peripheral power—but with OSDP, you can use 24V for peripherals that support it.

But wait, there's more…

Avoid Deployment Pitfalls

What are the most common pitfalls during OSDP deployment?

- **Device Address Conflicts** – Ensure each OSDP device has a unique address.
- **Secure Channel Key Mismatches** – Encryption keys must match between panel and device.
- **Firmware Incompatibility** – Use **OSDP Verified™** devices. Panels and peripherals must be version-aligned to ensure compatibility.
- **Bus Limitations** – Don't overlook them. Some devices may operate at just 3V on the data lines.
- **Evolving Hardware** – Older vendor hardware may require termination and pass-through power—check the specs.
- **Documentation** – If you manually terminate, leave a cable tag. It'll save headaches later.
- **Labor Planning** – Secure Channel adds complexity—budget for additional labor.
- And Finally… Please don't splice 500 ft reels together in the ceiling. **Seriously.**

#1 Support Call - Weigand to OSDP

"The reader is dead—my card doesn't beep!"

- In OSDP, the reader does not beep or change LED color when a card is presented.
- This often leads people to mistakenly assume the reader is faulty.
- In reality, the reader has likely read the card as expected.
- The reader sends the credential to the panel.
- The **panel** is responsible for sending the beep and LED commands back to the reader.

All this means is that the reader and the panel are not communicating.

Safetrust readers flash yellow by default when OSDP is offline, providing clear visual feedback—unlike most readers, which remain blank.

OSDP Wishlist

- Health and Communication Protocol
- Device Power Management
- Standardized Configuration Management
- Standardize Firmware Management
- High Speed Modern RS-485 >10Mb/s
- Device Digital Certificate Support & TLS 1.3
- Support for Door Strikes, REX etc

Q&A

Thank you!

Have thoughts about SIA Education@ISC?

Scan the QR Code on the left to provide your feedback on SIA Education@ISC Sessions at ISC West

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses