Access Control Done Right the First Time

Tim Clevenger



About me

Day job: Network Cybersecurity Engineer

Hardware junkie

Vintage computing enthusiast

Lenel/S2 certified (access/video) in a previous life

nsfw on the Physical Security Village Discord



About this talk

I’m here to present some tips and tricks for those looking to install, better maintain or upgrade a physical access control system.

Many vendors sell a “minimum viable product”

This talk focuses on larger facilities and those who need or want a more secure and reliable access control system



About this talk

Sample RFP on my Github:

https://github.com/TClevenger/access_control





Choosing a system

Mercury Security equipment

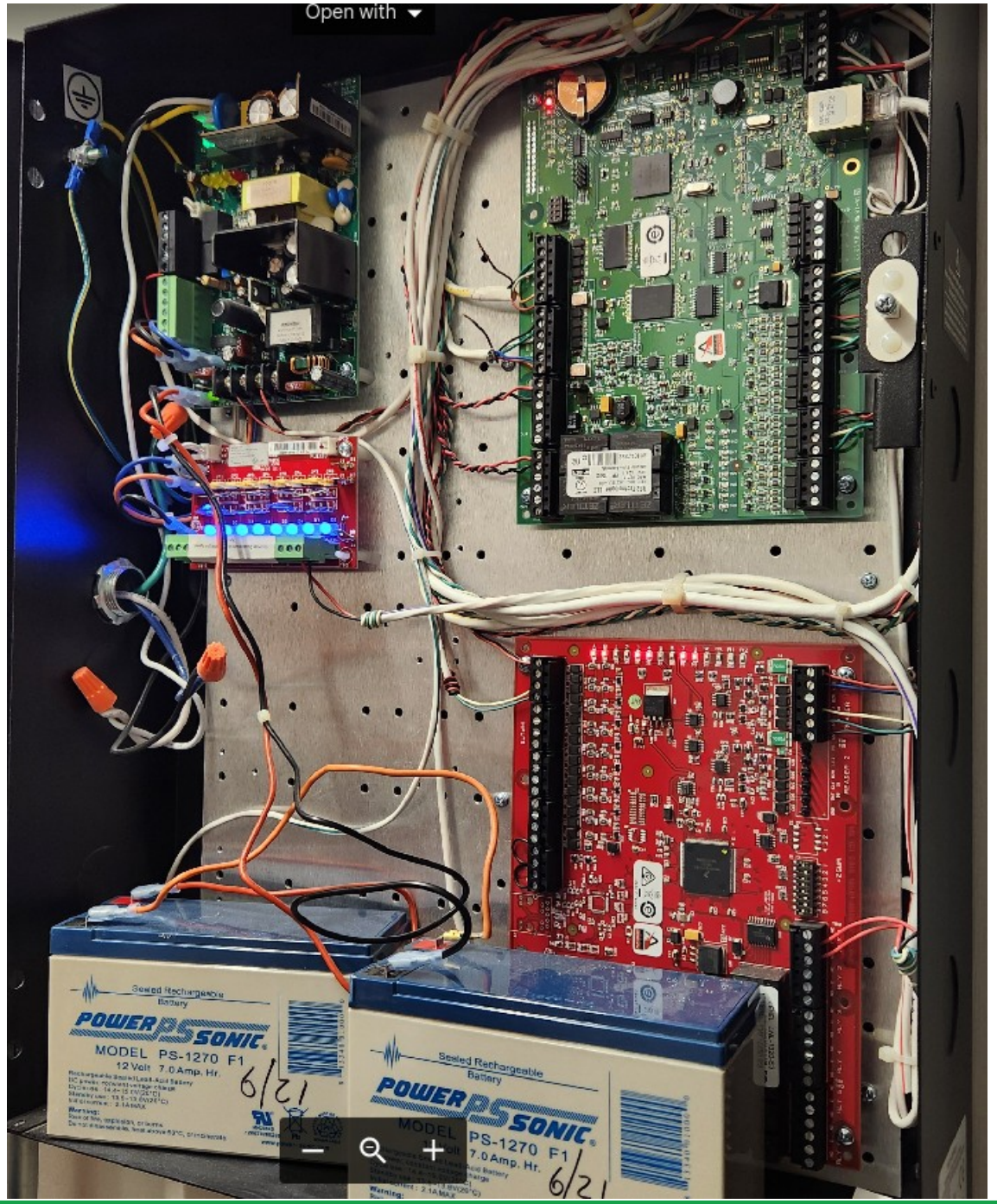
- Local storage, independent processing
- Multiple vendor support
- Reusable

Avigilon, Genetec, Honeywell,
Lenel/S2, RS2/Acre



System layout considerations





Access panel

Door controllers

Enclosure

Power supply

Batteries

System layout considerations

Panel placement considerations

- Environment (heat, humidity, dust)
- Power
- Physical security
- Accessibility
- The future



System layout considerations

Wiring considerations

- Ethernet drops: 328 feet (100m)
- RS-485 communications: 4,000 feet (1,220m)?
- Distance to doors: will I need a remote power supply?
- Hard lid, block walls, integrity/security (conduit)
- High EMI situations

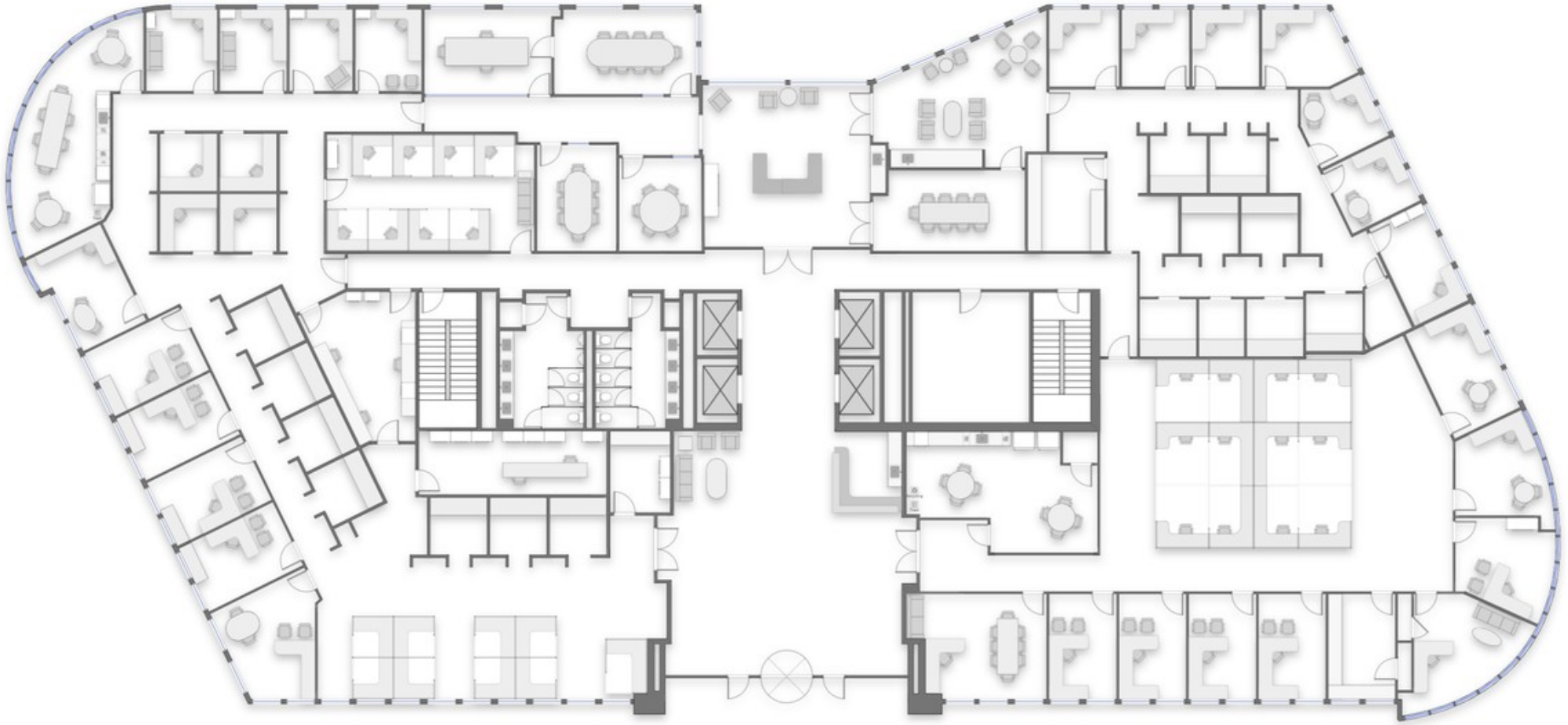


System layout considerations



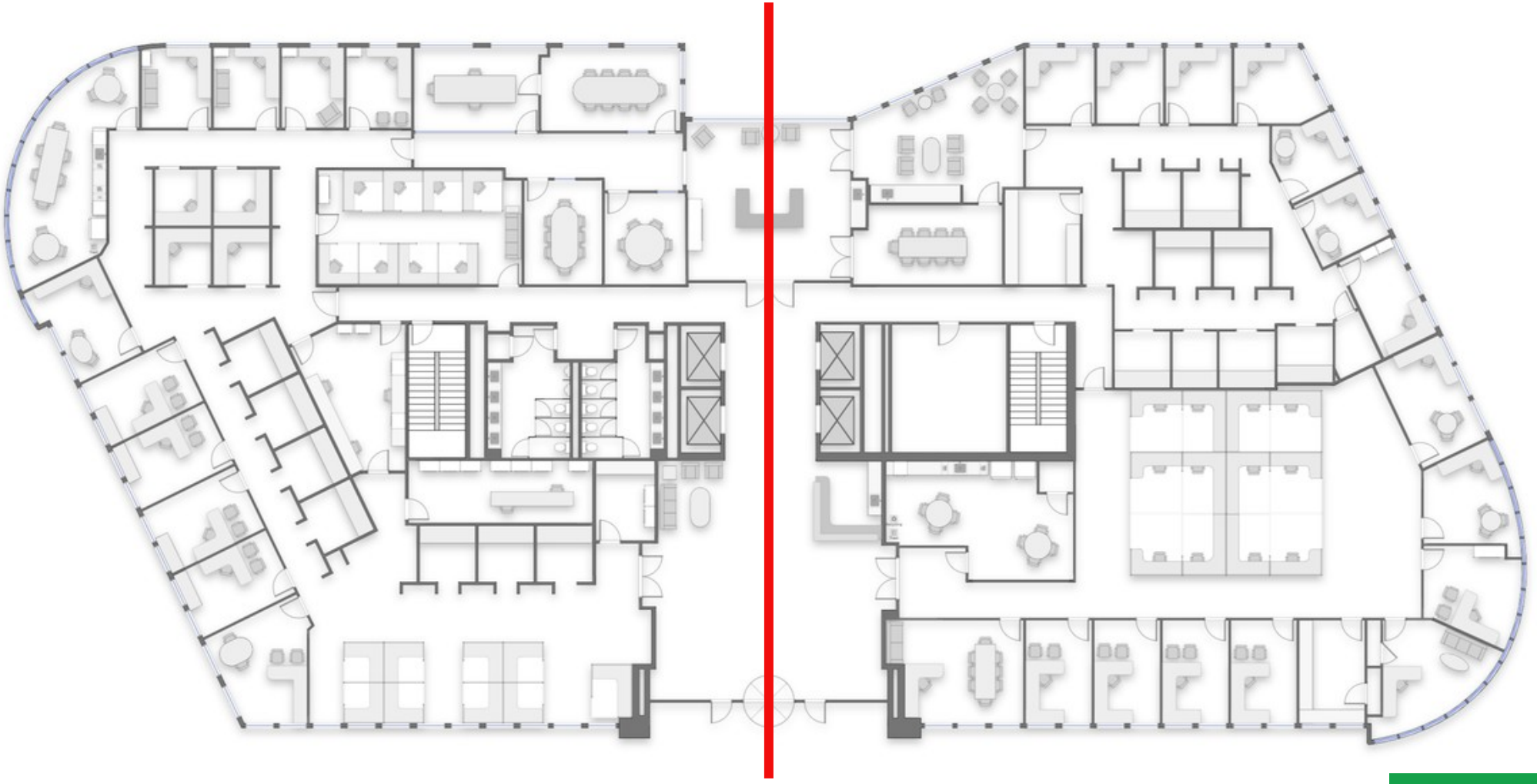
Long linear run exceeds Ethernet distance; remote power supplies probably needed

System layout considerations

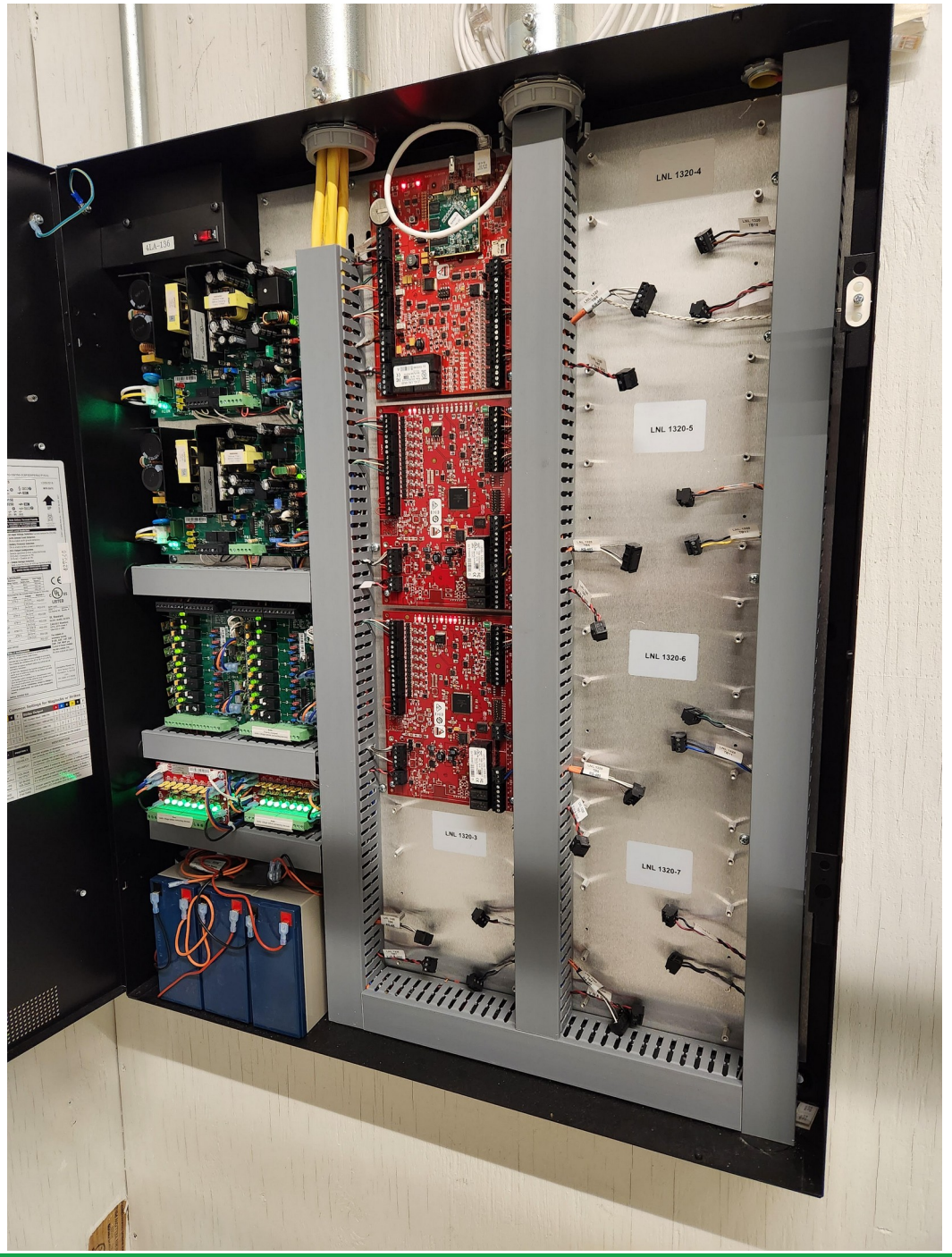


Single central panel

System layout considerations



Two independent panels


LNL 1320-4
LNL 1320-5
LNL 1320-6
LNL 1320-3
LNL 1320-7

Wiring to the doors

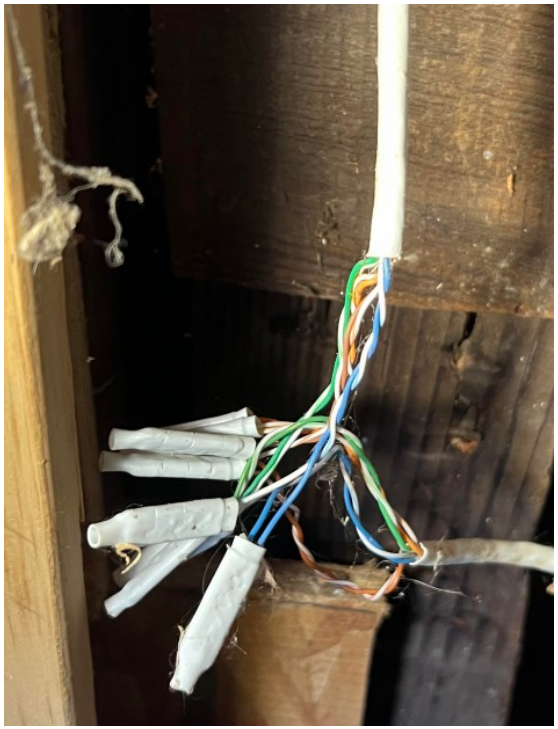
Wiring considerations

- Power to door hardware, motion sensors
- Shielded cable to badge reader (or RS-485)
- Door contact and REX wiring
- Tamper switches, aux inputs/outputs



Wiring (the WRONG way)

Undersized power conductors
- Insufficient power to unlock door
- Fire hazard



Unshielded or spliced cable to reader or controller
- Communications intermittent
- Can’t open door

No wiring for tamper and aux inputs/outputs
- Badge duplication/compromise
- Limited expandability

Wiring (the RIGHT way)

Composite access control cable

Multiple options

- Card reader comms
- Auxiliary and spare conductors

Properly shielded

Thick exterior jacket



Power supplies and enclosures

Power supply

- AC/DC, typically 12V and/or 24V
- Power supply/charger
- Verify amperage and temperature range
- AC fail and battery fail outputs

Power supplies and enclosures

Enclosure

- Single or multiple panels
- Sold as kit with power supply
- Pre-wired or DIY
- Key lock and tamper switch
- Optionally weatherproof



Batteries

12V gel-cell batteries in series/parallel

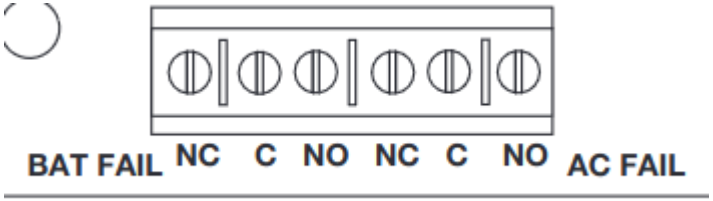
Requires power supply/charger

Write install date on batteries

Replace every 3 to 5 years

Use battery fail outputs





Remote power supplies

Required for power-hungry locks

- Motorized crash bar
- Magnetic locks
- Long distance runs

Often hidden above the ceiling

Choose power supply/charger

Tamper/battery fail/AC fail

Batteries



Fire safety

Fail safe vs. fail secure

Local fire code and AHJ

Building fire alarm

Knox box



Door hardware

Electrified strike
- Noisy and finicky

Solenoid
- Can get hot/fail

Magnetic lock
- Needs more power
- Always fails safe

Motorized crash bar
- Expensive



Door hardware

Door contact

- Door status (open or closed)
- Reed switch or integrated into handle

REX (Request to Exit)

- Detects door forced/bypassed
- Allows door to open from “secure” side
- Button, buzzer, motion detector or integrated into handle



Supervision

For door contact and REX

Resistors in serial/parallel

- As close to contact as possible



Different resistance readings (NC)

- Wires cut: infinite ohms
- Wires shorted: zero ohms
- Contact open: 1,000 ohms
- Contact closed: 2,000 ohms

Motion detectors

Used for REX (request to exit)

- Often triggers an unlock

Attack examples

- Mylar balloon
- Frozen spray from air duster

Mitigations

- Move motion farther away
- Don’t trigger unlock
- Use different lockset
- Use other REX methods



Door handle attacks

Under-door attack

- “Door forced” alarm won’t be triggered if door handle has integrated REX

Attack: Under-door tool



Mitigations

- Door handle surround/skirt
- Dual REX (handle AND motion)
- Second badge reader for exit
- Pushbutton REX

Badges and readers

Badge readers

- Multiple sizes and shapes
  Fobs, badges, smart cards, Bluetooth, magstripe cards
- Additional factors
  Biometrics, PIN entry



Badges

- 125KHz Prox (trivially broken)
- 13.56MHz iClass (broken)
- Mifare DESfire (not broken...maybe)
- Seos (not broken...maybe)

Badges

Prox and iClass have facility code and badge ID

- Facility code 0-255 (26-bit format)
- Cards can be purchased with any facility code and valid range of badge IDs

26-bit Prox and iClass format is trivial to clone

- Any compatible reader can read it
- Data can be captured from portable reader



Badges

Solution: Custom badges

- HID Corporate 1000
  - Seos
    * More secure
  - Dedicated facility code
    * Only you can order more cards
  - 48-bit format (8.3 million badge numbers)
    * Less chance of collision with acquisitions

- Disable older formats on readers



Badge reader communications

Wiegand communications protocol

- Low-speed serial protocol from 1975
- Inline capture/replay devices are cheap and trivial to deploy
- Mitigation: reader tamper switches a OSDP



Badge reader communications

OSDP – “Open” Supervised Device Protocol

- High-speed two-way protocol from 2015
- 128-bit encryption
- Badge reader enrollment
- RS-485 with daisy chaining
- Not perfect:
  - Compromise during reader pairing
  - 84% of installers “never or seldom use it*”
  - Mitigation:
    - Mind your daisy chains
    - Reader tamper switches

* https://www.sageintegration.com/blog/wiegand-nostalgia



What else should I do?

Test your readers regularly

Set up alerts

Document!

Check your batteries

Audit your users regularly

Visit the Physical Security Village



Thank you very much!

Sample RFP on my Github:

https://github.com/TClevenger/access_control



