A note on BAS Security

Target: IT Security Failure

- HVAC vendor has corporate IT password to support BAS from outside
- Password is stolen
- Attackers hack Target's Point Of Sale system
  - Never touched the BAS
  - Why does HVAC password get you to POS system?

- My toilet is broken
- I give plumber my house keys -- and car keys
- Plumber looses keys and my car gets stolen
- The security fix: A padlock on my toilet

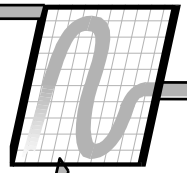
Securing the BAS

- Attacks on infrastructure very much in the news
- What is the risk to me from my BAS?
- ***Risk*** is made up of ***vulnerability*** and ***consequences***
  - My shed is unlocked (vulnerability = HIGH) but there's nothing of value there (consequence = LOW)
  - My house is locked (vulnerability = LOW) but there's high value things there (consequence = HIGH)
    - Which is the higher risk?
    - Which do I add security to first?
- Risk is what insurance companies deal with:
  - How much is your house worth?
  - Do you have smoke detectors?

Basic Security Steps

- Don’t allow remote access – particularly via vendor backdoors
- Lock down your OWSes: don’t allow standard applications or Internet access from an OWS
- Change passwords regularly
  - Limit access by user
- Turn on auditing: track operator actions
- Keep mechanical rooms locked
  - How to secure terminal equipment?
  - Whole bunch of non-cyber security things…..

“Cybersecurity” Design



- Design to minimize failure
  - Reduce dependency on the network
    - Local start of backup / redundant units
    - Local displays
  - Reduce extraneous functionality
    - Limit Remote adjustment capability
    - Limit Complexity - KISS
- Do not implement standard IT functions
- Do not provide remote (off campus) access in control system
  - Use existing IT infrastructure, or get IT Pros to provide

Good Mechanical Design

- Good mechanical design goes a long way:
  - Redundant systems: DX CRAC in data center
  - Manual operation modes: HOA switch for fan
  - Fail-to positions make sense: Fail to full cooling in data center

- In cyber speak these are “compensating” or “avoidance”, but it’s hard to tell the difference, just address it in the design and let them name it later.

“Cybersecurity” Design

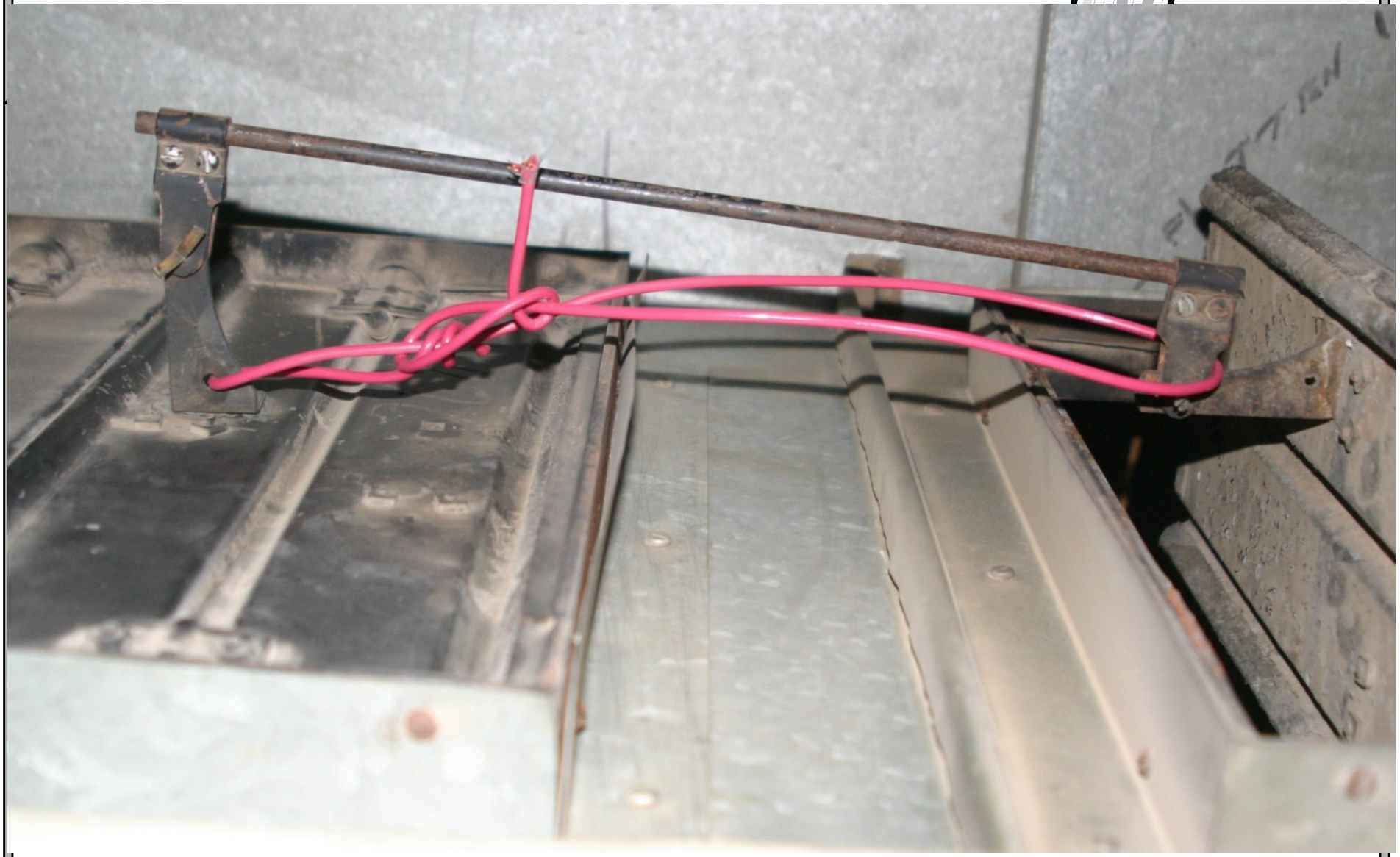
- Design to manage failure
  - Design for graceful failure
    - Individual mech/elec systems fail safe
    - Loss of a mech/elec system doesn’t affect others
      - UMCS is really lots of semi-independent systems
  - Degraded operation
    - May fail safe to degraded operation
    - Provide manual capabilities – HOA, manual valves etc.
  - Redundancy
    - Start spares automatically
    - Keep humans out of the loop – also reduces requirements for front end

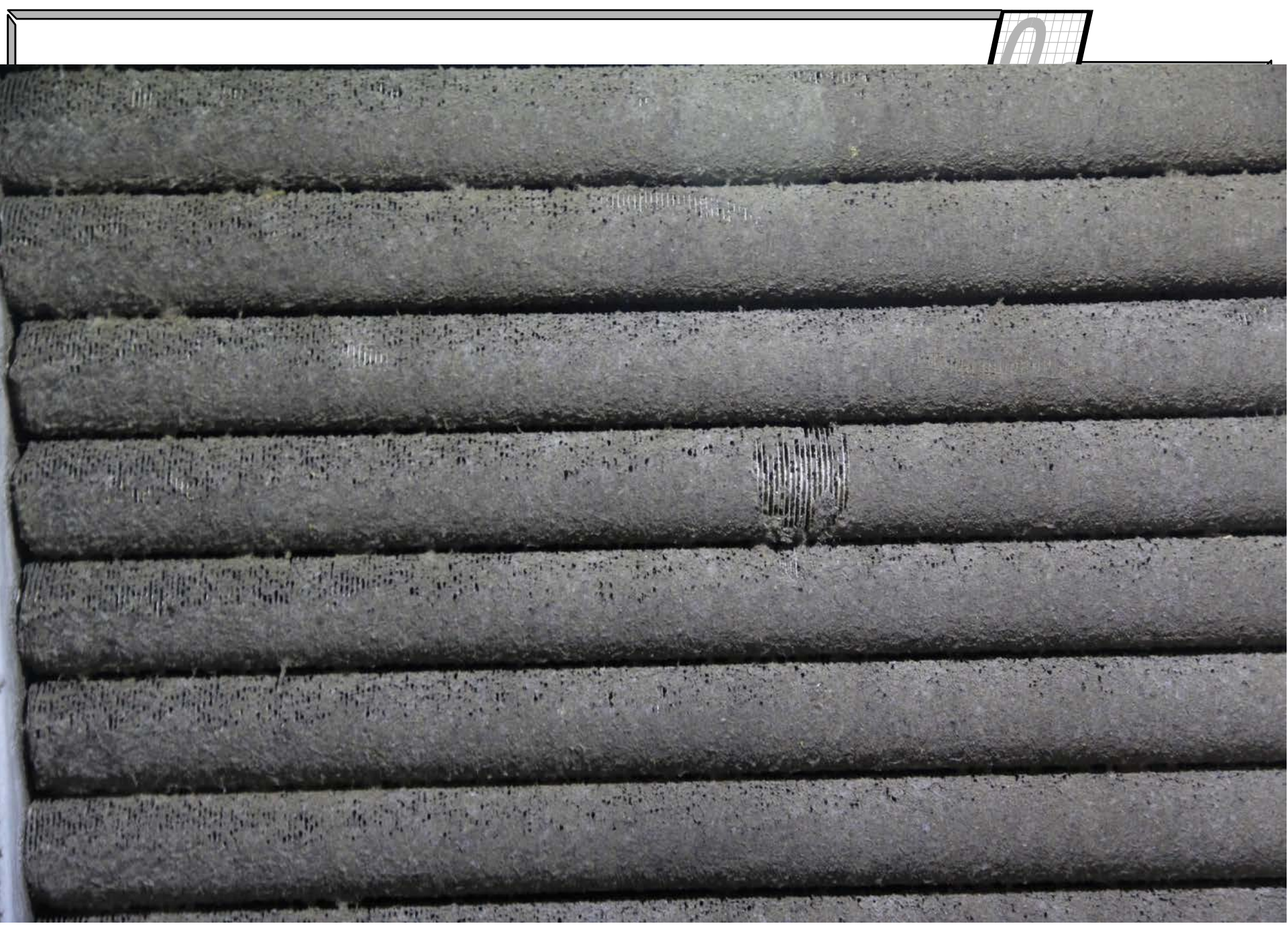
Most BAS is LOW risk

- ***Most*** building aren't worth attacking.
  - Turn off heat to classroom or admin building
  - Go turn heat back on, manually if necessary
  - Mechanical design (and physics!) limit consequences
- Often easier to attack mechanical system directly

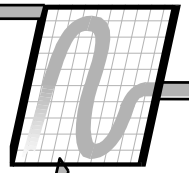

3/7/2000 15:14


3/7/2000 15:14





Most BAS is LOW risk



BUT

- There are ***critical*** exceptions:
  - Turning off cooling to a data center
  - Turning off airflow in a bio containment lab
  - Turning off power
- Often not cost-effective to protect the whole BAS
  - Protect critical systems from the BAS

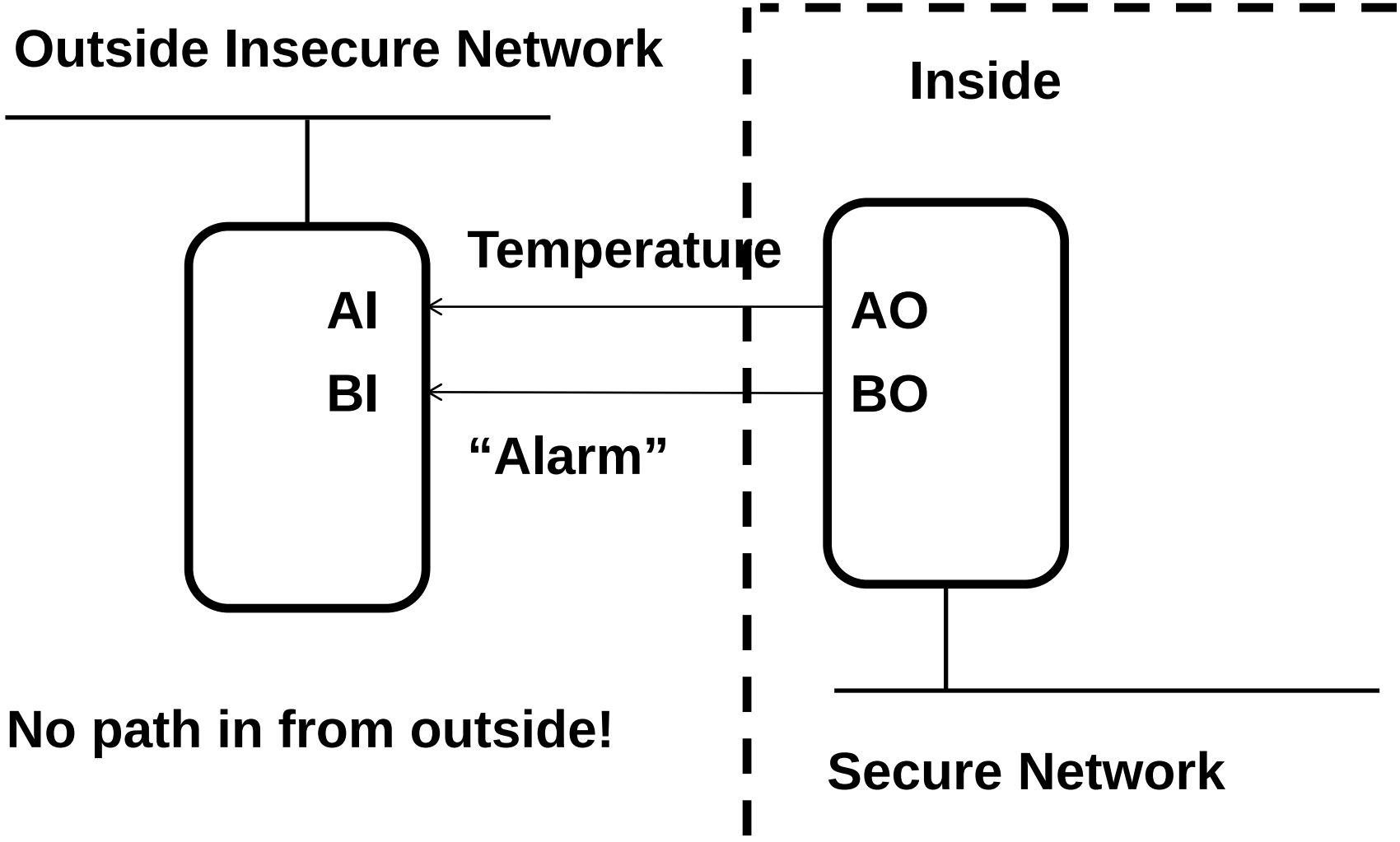
Limit OWS Functionality

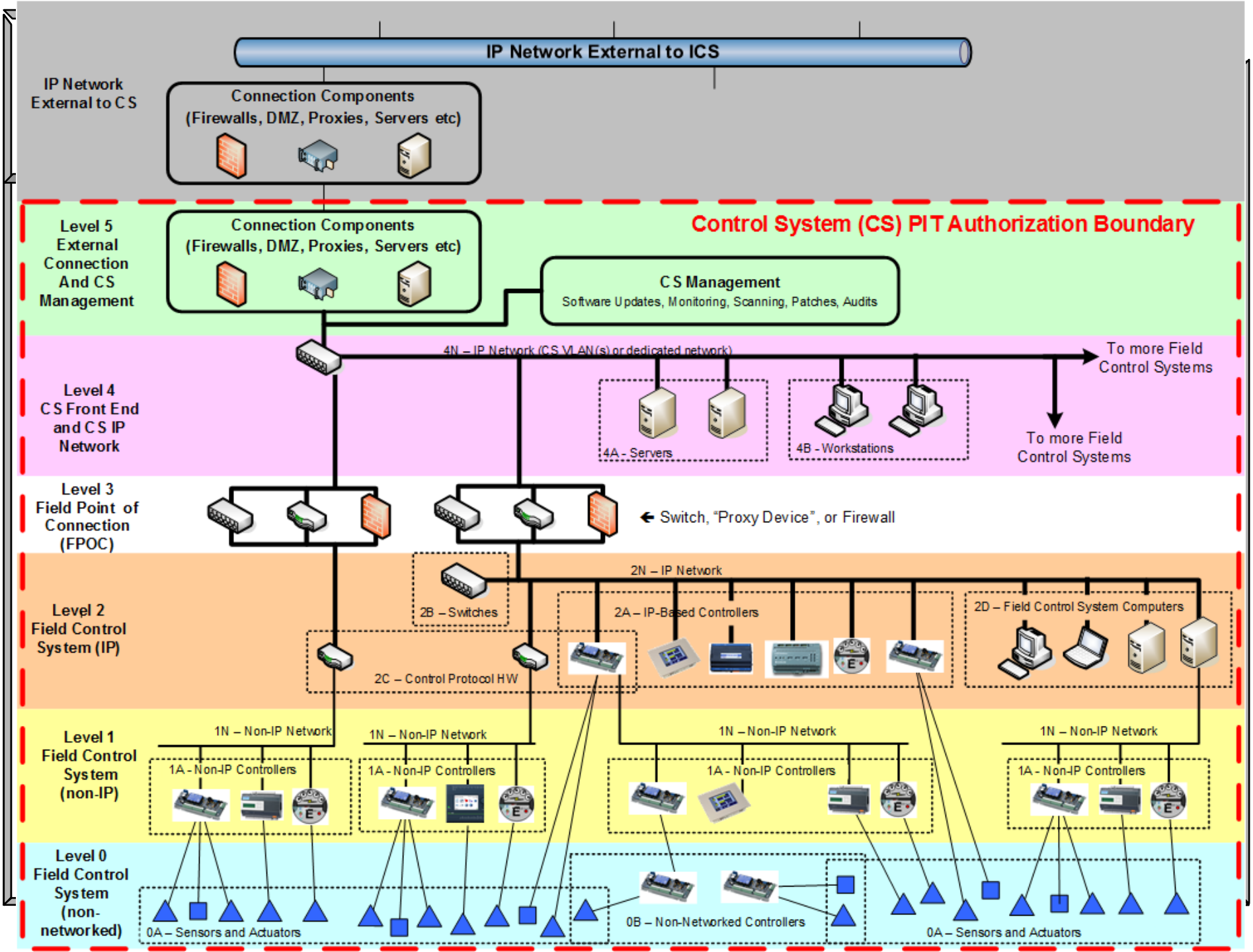
- Normally, our goal is: Make sure we can do **<*x*>** from the front end.
- Now, our goal is: Make sure ***no one*** can do **<*x*>** from “outside”
  - “outside” usually being some physical perimeter
- Seems counter-intuitive… but
  - Critical systems may need more monitoring
  - They seldom need more outside control
    - When do you change the setpoint on the data center?
    - When do you ***remotely*** change airflow in the lab?
    - When do you turn off the A/C for the UPS?
    - When do you want to stop a generator remotely?

How to Limit

- ***RECOMMENDED:***
- Hardware only interface: AO/BOs talking to AI/BIs
  - BO on inside device providing alarm contact to outside BI
- Other options:
- Use a different protocol for the critical system and a limited gateway to connect to BAS
  - Only map through commands / statuses that are absolutely necessary
- May be some custom firewall approach as well to limit traffic between critical system and outside

Hardware I/O Only




IP Network External to ICS
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control System (CS) PIT Authorization Boundary
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 CS Front End and CS IP Network
4N – IP Network (CS VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
Switch, "Proxy Device", or Firewall
Level 2 Field Control System (IP)
2N – IP Network
2B – Switches
2A – IP-Based Controllers
2D – Field Control System Computers
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1A - Non-IP Controllers
Level 0 Field Control System (non-networked)
0A – Sensors and Actuators
0B – Non-Networked Controllers
0A – Sensors and Actuators