



SCADA & PLCs in  
Correctional Facilities:  
The Nightmare Before Christmas

John Strauchs  
Tiffany Rad  
Teague Newman

Defcon 19

# Objectives

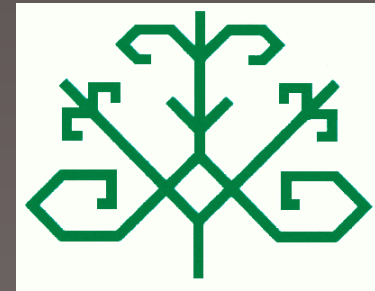
- Analyze SCADA systems and PLC vulnerabilities in correctional and government secured facilities
- Discuss modern prison design
- Theorize possible attack vectors and routes of malicious code introduction
- Explain ladder logic & demo a vulnerability on a Siemens PLC
- Recommend solutions


# Tiffany Rad



- BS, MA, MBA, JD,
- President of ELCnetworks, LLC., in Washington, D.C. & Portland, ME
  - > Consulting projects have included law, business and technology development for start-ups and security consulting for U.S. government.
- A part-time Adjunct Professor in the computer science department at the University of Southern Maine teaching computer law, ethics and information security.
- Academic background includes studies at Carnegie Mellon University, Oxford University, and Tsinghua University (Beijing, China).
- Presented at Black Hat USA, Black Hat Abu Dhabi, Defcon 17 & 18, SecTor, HOPE in 2008 & 2010, 27C3 and regional information security conferences.

# John J. Strauchs



- > M.A., C.P.P.
- > Senior Principal of Strauchs LLC
- > Conducted the security engineering or consulting for more than 114 justice design (police, courts, and corrections) projects including 14 federal prisons, 23 state prisons, and 27 city or county jails
- > Owned and operated a professional engineering firm, Systech Group, Inc., for 23 years. Prior to that he was an equity principal in charge of security engineering for Gage-Babcock & Associates
- ❖ Consultant to  RECURSION VENTURES
- ❖ Presenter at Hackers On Planet Earth (HOPE) in 2008 and DojoCon in 2010
- ❖ Tag-along at Hacking at Random, The Netherlands, 2009

# Teague Newman

- Independent information security consultant based in the Washington, D.C. and Reno, Nevada areas
- In 2009, competed in the Netwars segment of the US Cyber Challenge and ranked within the Top 10 in the US in all rounds in which he participated.
- Instructor and penetration tester for Core Security Technologies
  - > Instructed professionals on the topics of information security and penetration testing at places like NASA, DHS, US Army, US Marine Corps (Red Team), DOE, various nuclear facilities as well as for large corporate enterprises.
- Projects include GPU-based password auditing and liquid nitrogen overclocking.

# Dora the SCADA Explorer

- Exploit Writer
- Has a pretty, crafty backpack
- Is nice
- Is really good at coding
- Lives in a tropical area:
  - > Columbia [Maryland]



# The Red Team Always Wins



# Why present about prison vulnerabilities?

- Provide support for wardens and corrections administrators to get funding to fix the problems
- Everyone is short of money these days and they need all the help they can get
- To scare prison guards and LEOs to follow their operating procedures
  - > No looking at Gmail or memes in the Control Room! !





We briefed some Federal Agencies. One was stealthy, probably difficult to see at night – or ever. Another has some handsome Agents, but also has the capability to extend its domestic claws. They are “friends”

# Story of Christmas Eve

- Discovered that the correctional facility contractor had not followed specification
- Used two hardware components not specified and had never been used together
- The PLC and the relay were part of the specs.
- The ratings were different
  - The circuit board on the Square D was supposed to be 0 volts out but more volts went into it with a power surge and the one-way diode was leaking voltage
  - When the controls work at 25 millivolts, a low power spike is all that needs to trigger it
  - Possibly with increased power consumption on Christmas Eve, all the doors opened when there was a power surge

# It started with Stuxnet

- Few people knew what a programmable logic controller (PLC) was before Stuxnet when Siemens PLCs in Iran were exploited & damaged nuclear processing centrifuges
  - > PLCs have been around for more than 40 years.
- Stuxnet research: discussions at Black Hat Abu Dhabi with Tom Parker and FX
  - > Tom Parker's Black Hat Abu Dhabi presentation
  - > FX's 27c3 presentation
    - <http://www.youtube.com/watch?v=Q9ezff6Ll0l>

# Stuxnet for Correctional Facilities?

What if someone wrote a virus or worm, similar to Stuxnet, but targeted government or state locations like correctional facilities?

# Introduction to correctional facilities security designs

❖ John Strauchs

❖ A former operations officer with the CIA

(either the U.S. Central Intelligence Agency  
or the Culinary Institute of America)

My company  
and work were  
inspirations for  
the 1992 movie,  
*Sneakers* for  
which I was the  
security  
consultant



Sneakers ©1992 Universal Studios

# It started with Stuxnet

- The attack was directed against STEP 7, the Siemens software that is used to reprogram PLCs.
- Supposedly, Microsoft patches MS08-067, MS10-046 and MS10-061 for Windows fixed the vulnerabilities that allowed the compromise

# Now its all about PLCs

- The cyber-security and hacking communities have been focusing on SCADA systems in the use of PLCs in the national infrastructure:
  - > Power grid
  - > Pipelines
  - > Water systems
  - > And so forth



# Its still all about PLCs

- But...because most people don't know how prisons and jails are designed and constructed, most people didn't realize that they are controlled by PLCs.

# Something about nomenclature

- **Prison : A federal or state facility**

- > Many have hundreds of cells and thousands of inmates
- > Confinement is typically a year to life

# Something about nomenclature

- **Jail : A county, city or town facility**

- > Most have a few cells but some have many hundreds of cells, especially regional jails
  - Orange County Jail, California, has 2540 inmates
- > Usually confinement is less than one year
  - But, pre-trial confinement could be for a pickpocket or a terrorist or serial killer

# Prisons and jails

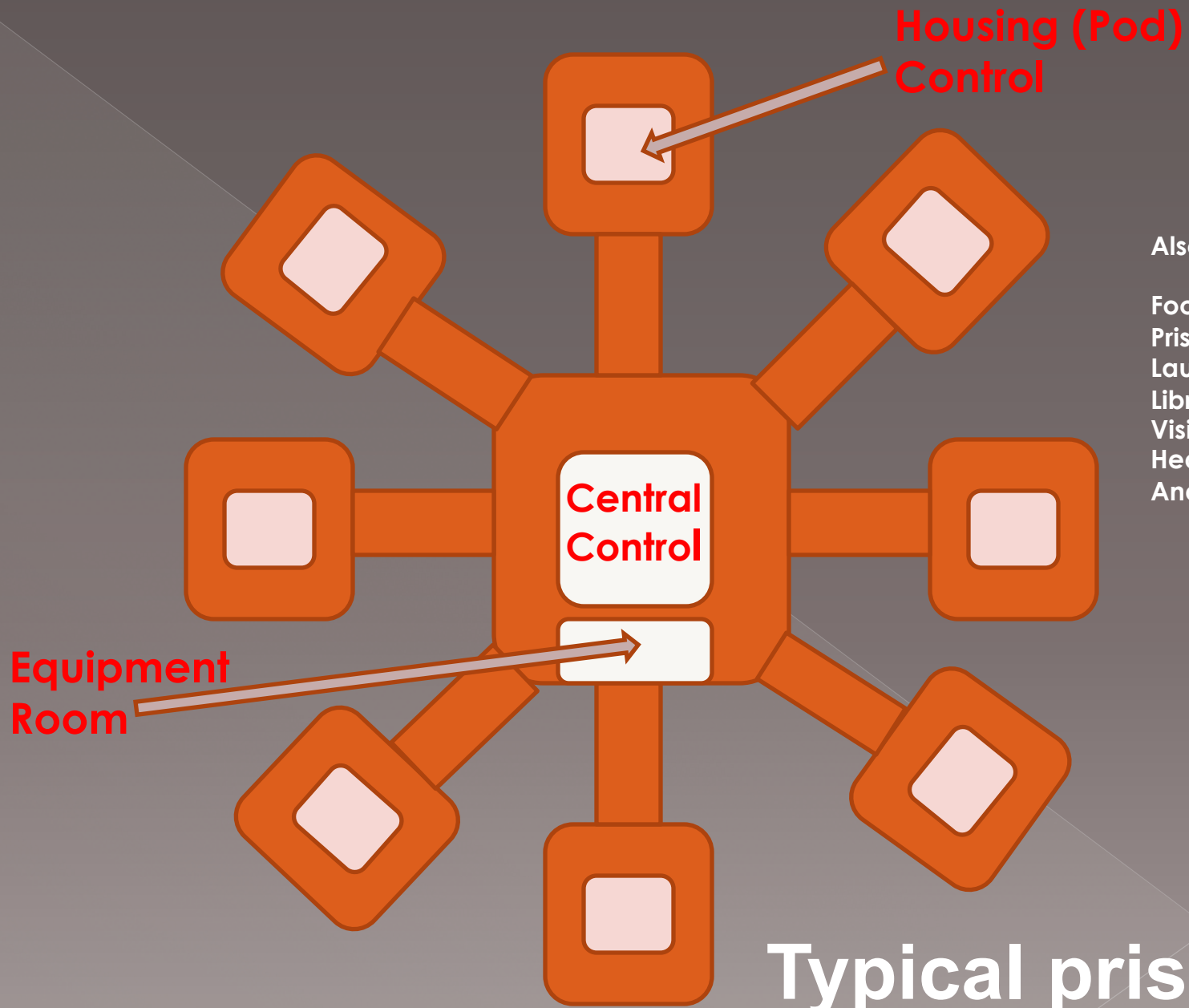
- **In the United States:**

- > 117 federal correctional facilities
- > 1,700 prisons (penitentiaries)
- > 3,000 jails
- > About 160 are operated by private companies

- **And most use PLCs in their electronic security systems**

I've been in many prisons and jails





Also, may have:

- Food Service
- Prison Industries
- Laundry
- Library
- Visitation
- Health Services
- And other

Typical prison  
design

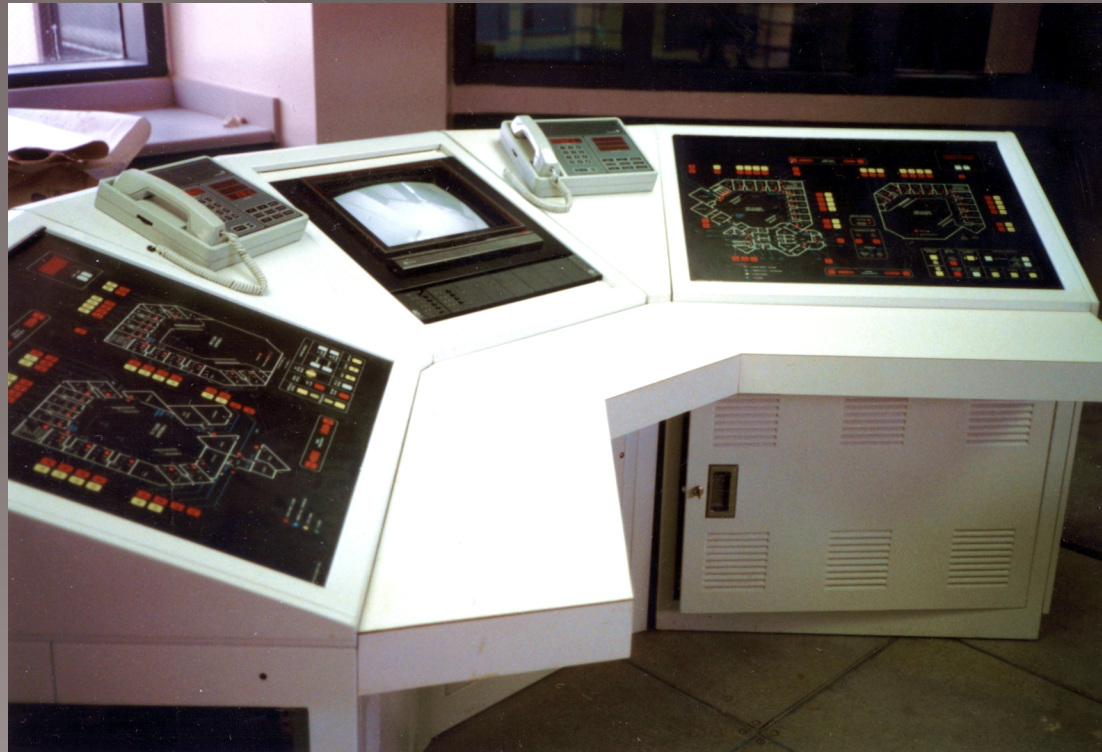




There may be hundreds of  
cells



All but the smallest have a control center



**So...what does an  
electronic security system  
for a prison look like?**

Work  
Station



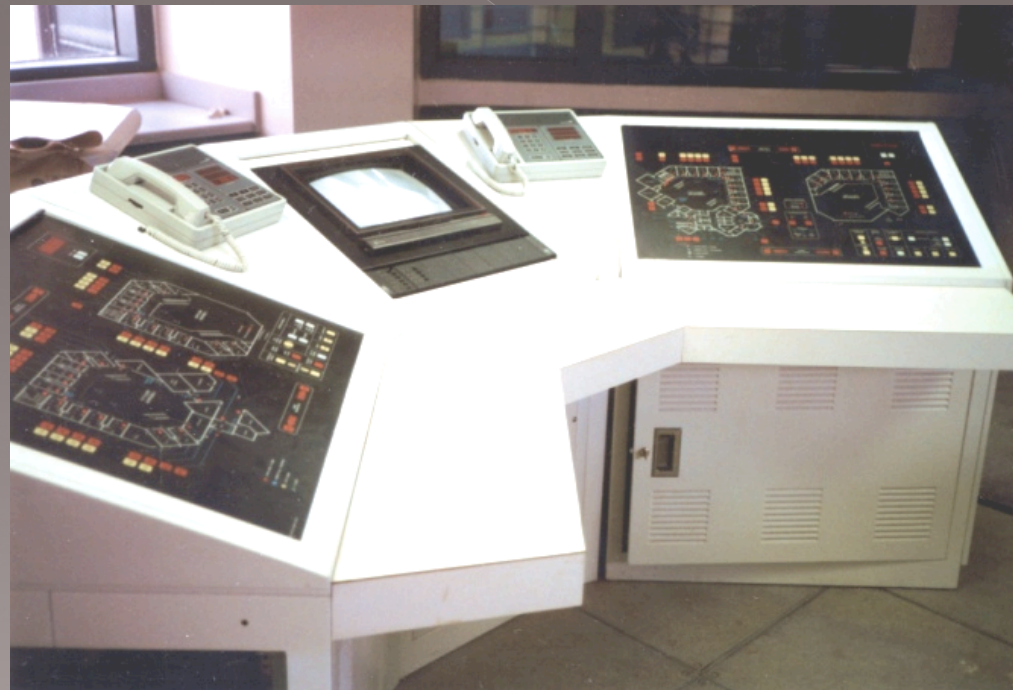
Monitor



**Server**

**Control  
Center**

**It starts with a  
control center...  
the master “brain”  
for the system**





Server



Lock solenoids or motors



Lock sensors or limit switches

Its reason for being is all about door control



CCTV

Server

Duress  
alarms



Control  
Center



Intercom

Lock solenoids or  
motors



Lock sensors or limit  
switches

It also monitors  
and controls many  
security  
systems...among

# It monitors high security perimeter fences

On-board graphic panels for perimeter patrols



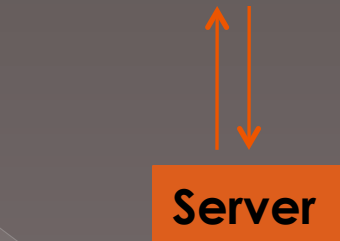
**Rf Link**



Fence sensors



Lock sensors or limit switches



CCTV



Duress alarms

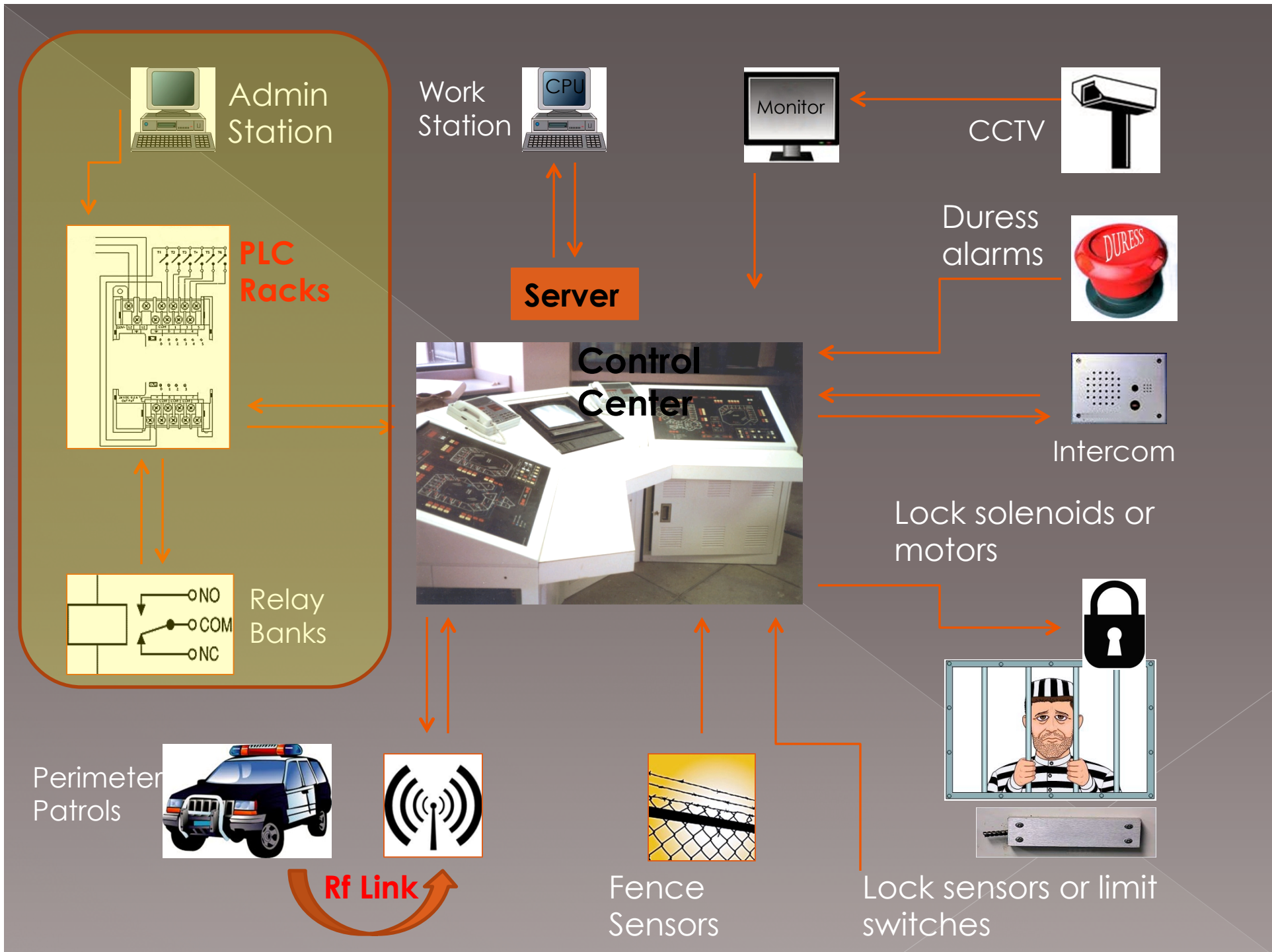


Intercom

Lock solenoids or motors



All of these functions are  
monitored and/or  
controlled by rack-  
mounted PLCs and relay  
banks!



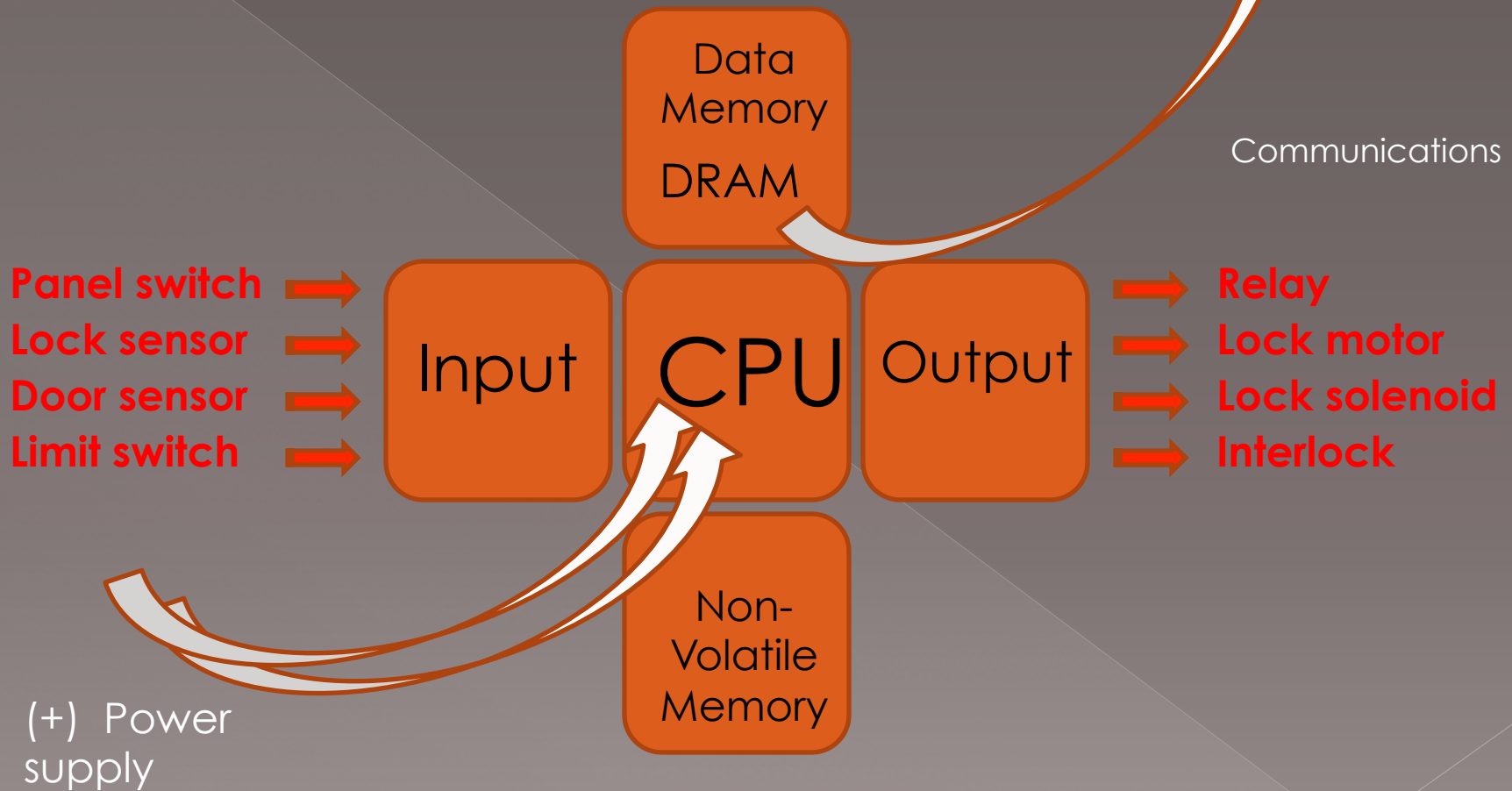


# Prison system functions could also include controls for:

- Public telephone
- Dayroom TV
- Lighting
- Showers
- Water

# Block diagram of PLC

[Programmable Logic Controller]



Programming device

## Door control

# PLC Manufacturers

- There are from 40 to 50 manufacturers. The PLCs most commonly used in corrections are:
  - > Allen-Bradley
  - > GE Fanuc
  - > Hitachi
  - > Mitsubishi
  - > Panasonic
  - > Rockwell Automation
  - > Samsung
  - > Siemens
  - > Square-D

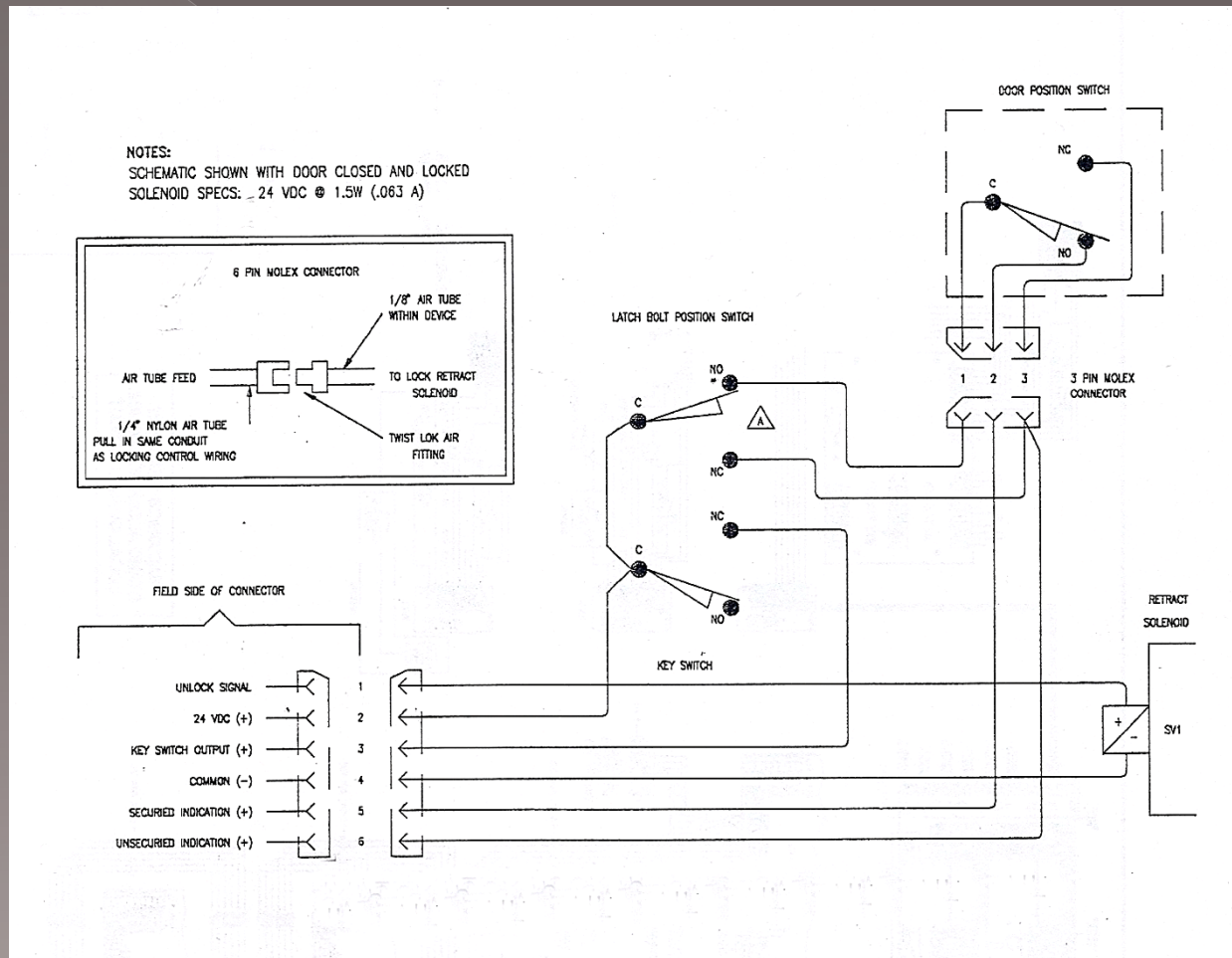
# PLC Facts

- Usually 9-pin RS-232 or EIA-485 or Ethernet
- Protocols
  - > Modbus
  - > LonWorks (**Most common**)
  - > BACnet
  - > DF1
  - > others
- Programming
  - > Ladder Logic
    - **Most common, esp. for older systems**
    - **Weak**
  - > FBD (Function block diagram)
  - > SFC (Sequential function chart)
  - > ST (Structured text; viz. Pascal)
  - > IL (Instruction list)
  - > BASIC
  - > C++

# PLC Facts

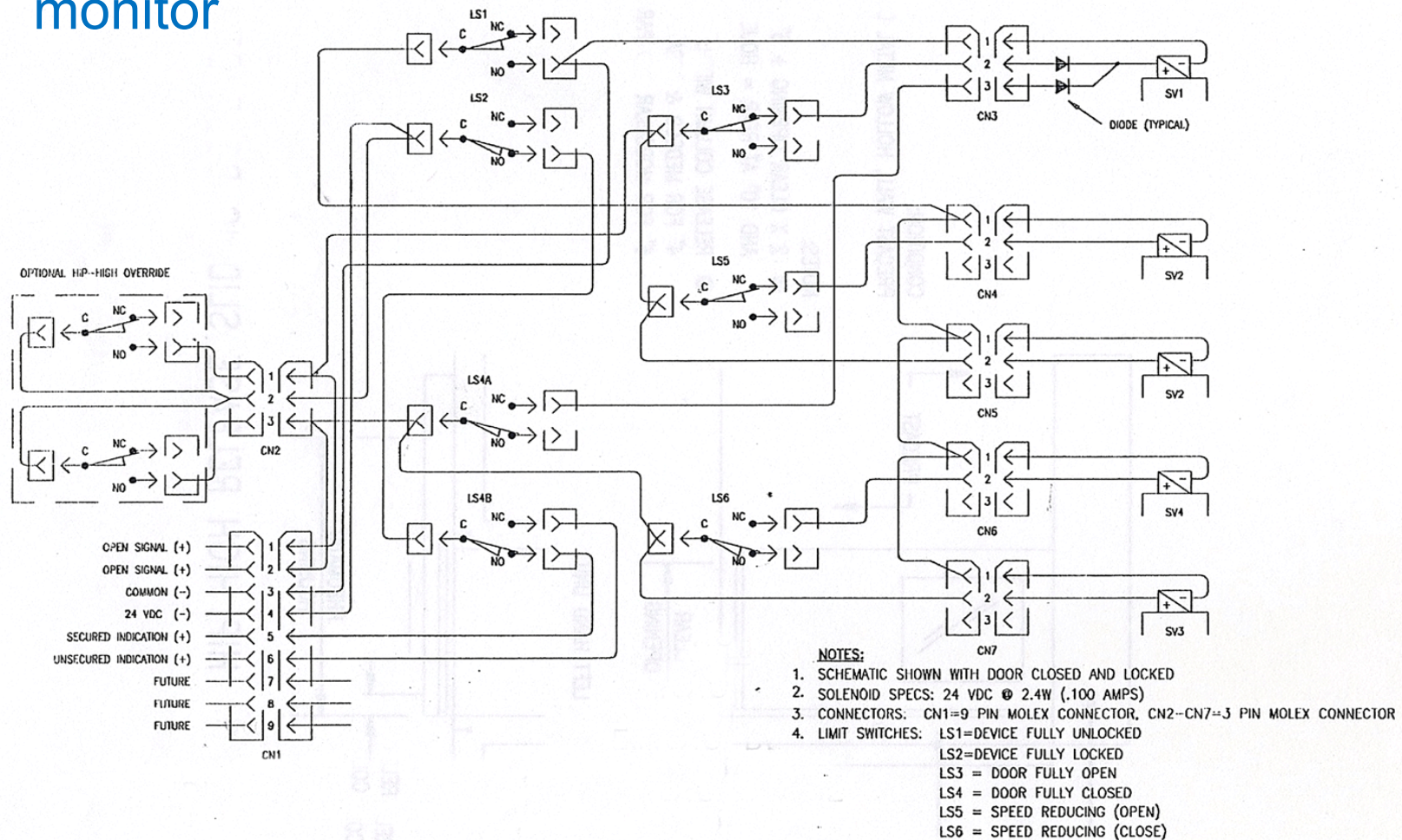
- In large facilities PLCs monitor many thousands of points (mostly contact closures) and control hundreds of devices (mostly motors and solenoids)

# Pneumatic sliding door schematic detail

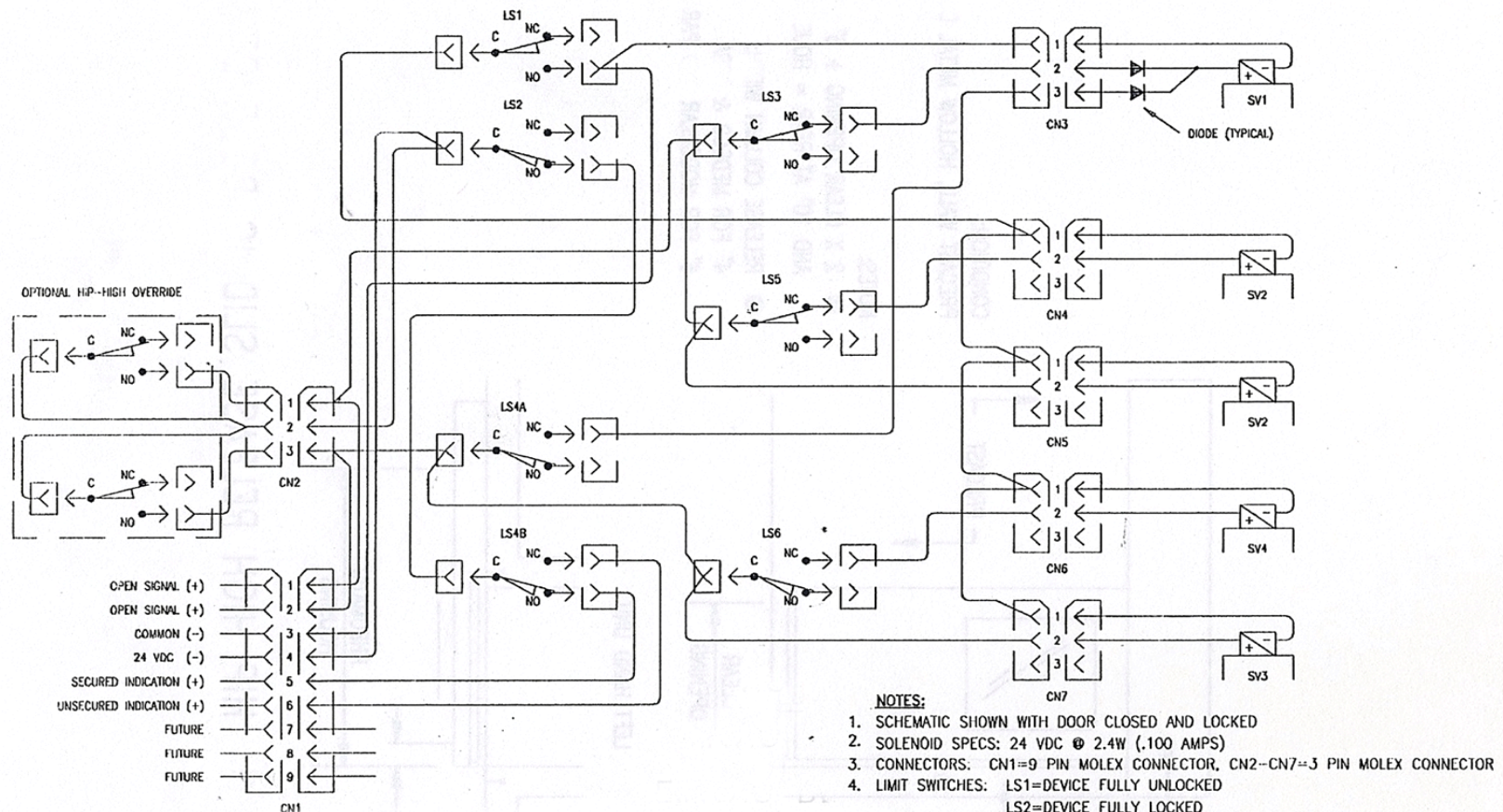


# Pneumatic lock wiring

This one door could have as many as 34 points to monitor



# Pneumatic lock wiring

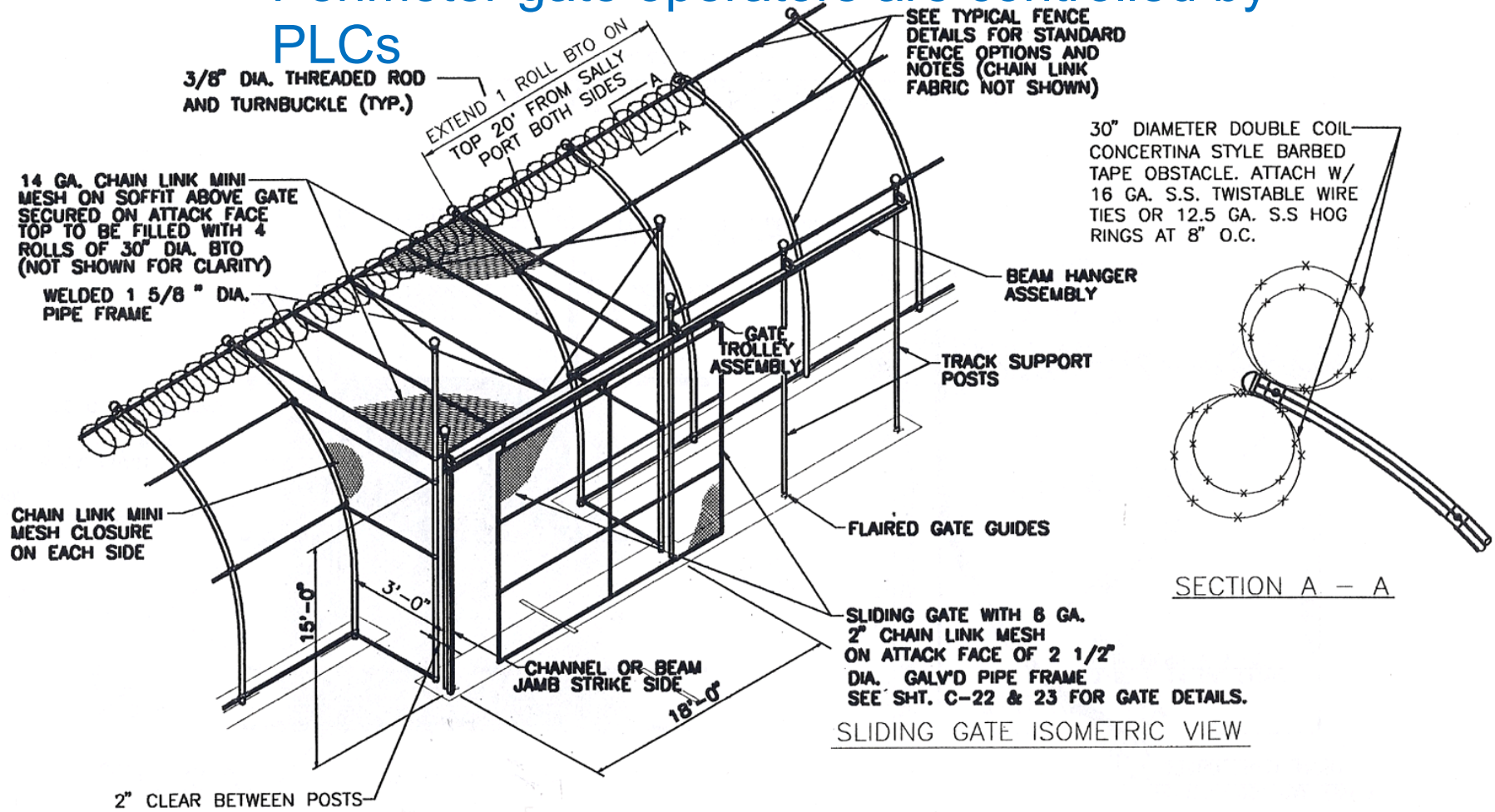


**Note** →



# Fence sally port gate detail

Perimeter gate operators are controlled by PLCs



# Vulnerabilities

- **Open doors and gates**
  - > Especially in a.m. hours when controls may have shifted to Central Control because of staffing shortages.
- **Cause phased locks (sliders) to go out of phase**
- **Prevent doors or gates from opening**
  - > Especially during a fire evacuation when “slam-lock” doors (without remote latch holdback) can only be unlocked manually with a key. Guards may not have the key.

# Vulnerabilities

- **Emergency release of entire cell blocks or entire facility**
  - > Prevent “cascading release” and massive power in-rush may cause severe damage
- **Activate door motors and solenoids**
  - > Accelerating high-speed activation of solenoids
  - > Make them fire off like machine guns
- **Radio signal-linked graphic panels in patrol vehicles**
  - > Weak encryption or no encryption

# Vulnerabilities

- **Perimeter fence intrusion detection systems (FIDS) often have high rates of nuisance (NAR) and false (FAR) alarm rates**
  - > Rates can be elevated until zones are shut down by Central Control
  - > Exception would be “taut-wire” systems, but those systems are infrequent

# Vulnerabilities

- **Belief that PLCs are invulnerable because they are not connected to the Internet**
  - > Operating system software requires installing patches and updates
  - > Correctional facilities need to send and receive information to and from federal, state, or local data bases
  - > Facility operations often require off-site support from vendors and suppliers (i.e. food service)

# Vulnerabilities

- **Belief that PLCs are invulnerable because they are not connected to the Internet**
  - > Some facilities provide Internet access for inmates
    - Granted, they aren't connected to facility networks
    - But, Charles Manson smuggled a cell phone into his cell twice in two years
  - > Perimeter patrol vehicles have wireless connections to the fence intrusion detection system
  - > Prison intercom systems often have a "patch" to connect to public telephone (PBX) system

# Vulnerabilities

- **Belief that PLCs are invulnerable because they are not connected to the Internet**
  - > After a correctional facility's electronic security systems have been designed and installed, the owner's IT people show up to add network connections
  - > AND...corrections officers sometimes "break the rules"

# What could an exploit do?

- You could wreak widespread pandemonium by severely damaging door systems and shutting down security, communications, and video surveillance
  - As only one example, a very large prison cannot instantly, simultaneously open or close all doors. The power in-rush would be massive, destroying the electronics and possibly physically damaging door components. Doors are gradually “cascaded” open or closed, group-by-group. You could override the “cascade” program.



# Infection Vectors

## From Within

- Technicians access the Equipment Room
  - > We were there when techs were in Equipment room; with permission, we followed them down under Central Control
- Central Control infected with a USB drive
- Internet access being used by guards for personal usage
  - > Policies against this exist, but we witnessed this being abused

## From Without

- Software updates
- Straight-forward malicious attacks from outside the facility
- Malicious attacks from outside the “sanitized” zone, but at a point at which the Internet connects to the outside

# Is Internet Access Isolated?

- Prison design shows that there may be multiple places where internet access from the control computers in Central Control touch buildings in which there is Internet access reachable from the outside
  - > An example is the Commissary
  - > Where there are financial exchanges, we traced some connections shared with Central Control

# Christmas Eve Nightmares

What kind of badness is possible?

# Scenario 1: Open Doors

- > Goal is to open doors
  - To either cause chaos for a murder, bring an item into the prison or release someone from the facility
  - Potential to open:
    - All cell doors
    - Doors to the yard
    - Gates into/out of the facility
  - Most doors, in event of fire, have own separate controls
    - But emergency controls for those gates that are wired into the Central Control over-ride

# Result: Release from Prison

- Unlikely...yes, but in the past 30 years helicopters have been used for a prison escape 8 times, of which 6 were initially successful. Which event is more unlikely?
- Attack via Internet Access
  - Devices do updates via the Internet
    - Unsigned software manufacturer/vendor updates?
  - The guards in Central Control and Housing Control are not supposed to use computers for personal usage
    - We witnessed guards in Central Control on personal Gmail accounts
    - Had discussion with guards; they admitted a lot of malware on control computer because of viewing of images and movies

# Scenario 2: Close Doors

- > Prisoners sometimes want to target someone within the prison.
- > Example: During a fire evacuation
  - Prisoners in high security prisons often do not evacuate into the yard, but use horizontal exiting, such as through a one-hour rated partition
  - In process, prisoners have slammed doors (called “slam locks”) shut behind them, trapping those behind in areas that cannot be manually re-opened once the fire alarm activated. Those behind the door have died.

# Result: Prisoners Locked In

- > Lock a Housing Unit Down
  - A gang in one Housing Unit wants to eliminate members of another gang in a separate Housing Unit.
    - Lock down a Housing Unit, no manual over-rides
    - Set a mattress fire
    - Result is everyone, including guards, in locked down housing unit, perish

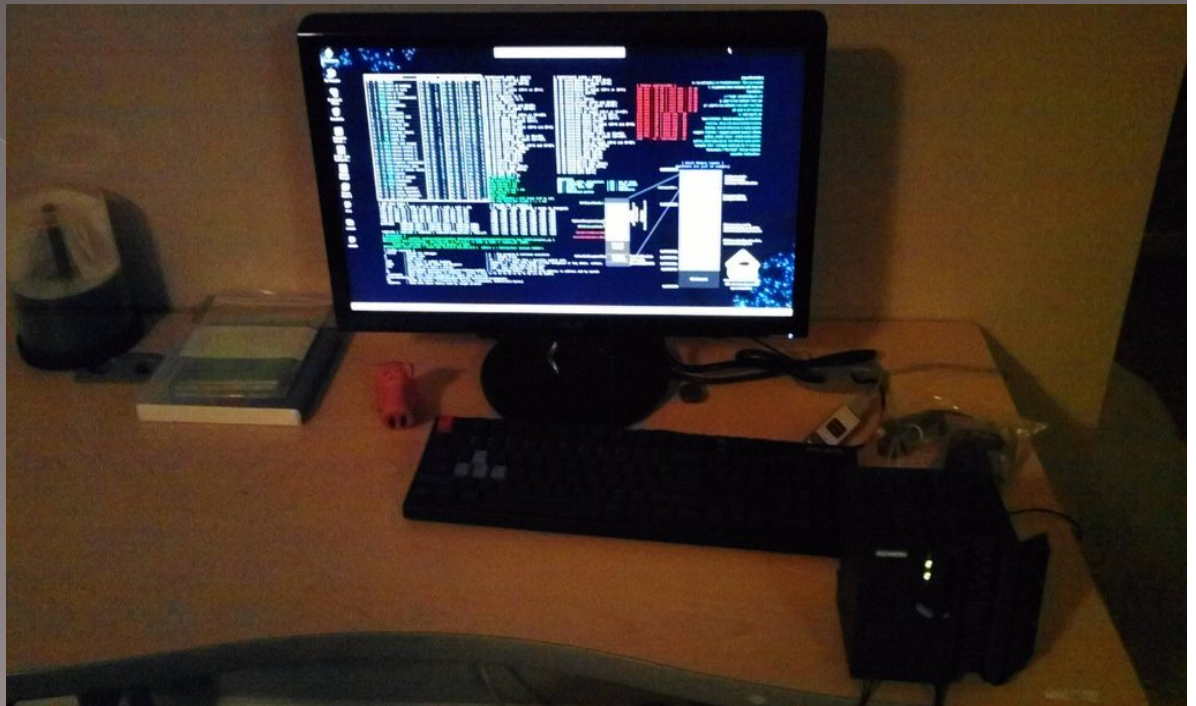
# How Much Does PLC Research Cost?

- It cost us only \$2500 (mostly in legit licenses)
- Bought licensed products from the vendor
- Wrote exploits for the Siemens S7-300, the same one exploited by Stuxnet
- There are exploits that are simple-to-write
  - Buffer overflow on a stack, about 30 lines of code



# The Basement Lab

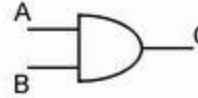
- Programming PLCs is easy
- Ladder Logic
- In <3 hours & no prior ladder logic experience, we simulated jail's system



# Ladder Logic

- Logic AND

A	B	O
0	0	0
0	1	0
1	0	0
1	1	1

A standard AND gate symbol with two inputs labeled 'A' and 'B' on the left and one output labeled 'O' on the right.


- In Ladder Logic



# Ladder Logic

- Logic OR

A	B	O
0	0	0
0	1	1
1	0	1
1	1	1



A logic OR gate symbol with two inputs labeled A and B, and one output labeled O.

- In Ladder Logic



# Attack Vectors

- There exist many publically available exploits...
- Luigi Auriemma
  - > 34 exploits released in 1 day (Mar 21, 2011)
  - > <http://aluigi.org/adv.htm>
- Metasploit
- Exploit-DB

# Our attack vector

- ◉ Similar to Stuxnet
- ◉ Directly call PLC functions
- ◉ Suppress alarms/notifications

# DEMO

- Video on YouTube



SIEMENS

CPU 313

SF  
BATF  
DC5V  
FRCE  
RUN  
STOP

RUN-P  
RUN  
STOP  
MRES

SIMATIC  
S7-300

313-1AD00-6AB0

16  
16

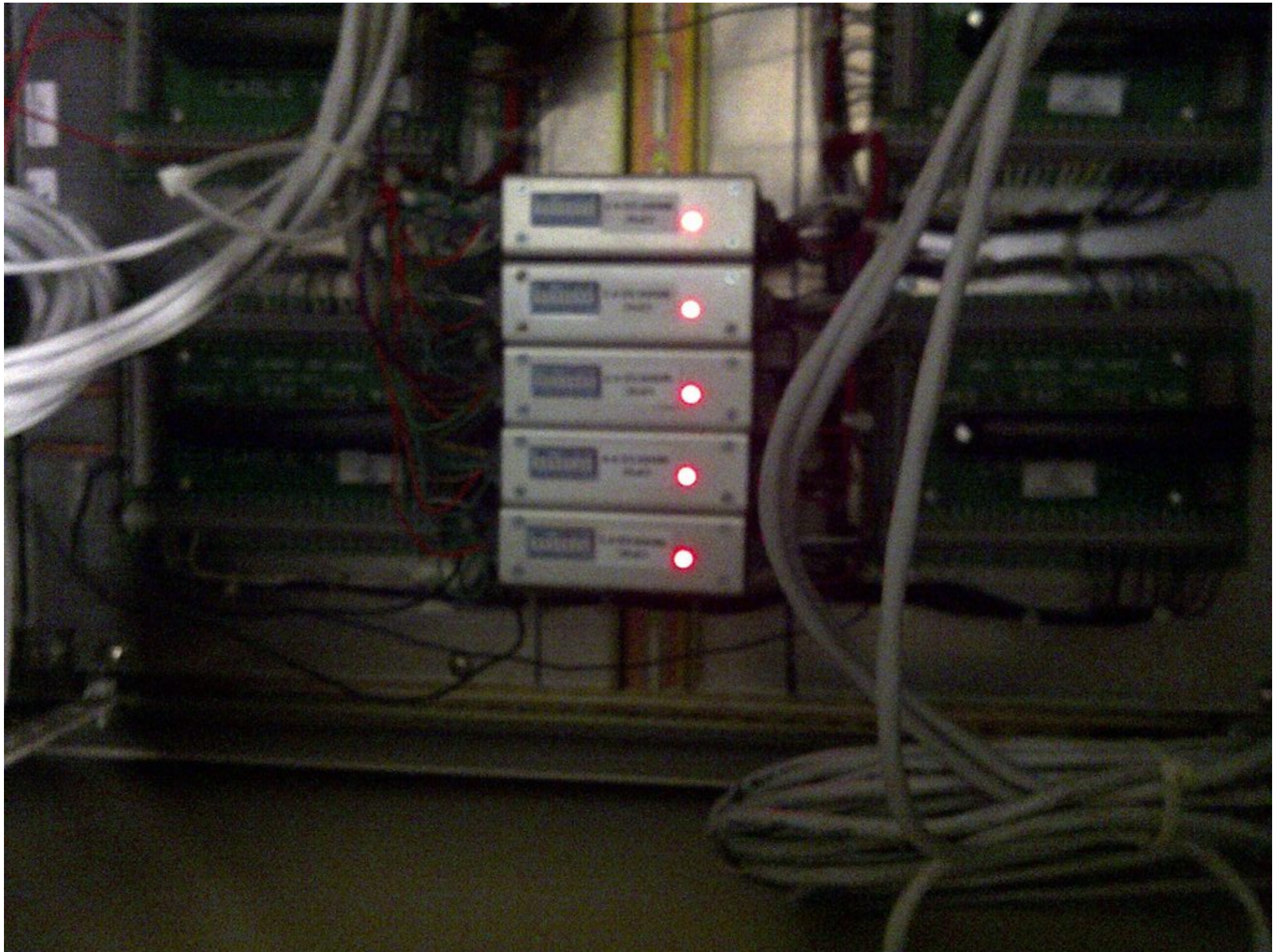
0 1 2 3 4 5 6 7  
0 1 2 3 4 5 6 7

5x Input  
16x Output  
5x Input  
16x Output

# Newman & Rad Tour a Correctional Facility







# Remediation

- Use a device for its intended purpose
- Proper network segmentation
- Restrict physical media
- Restrict physical access
- Follow acceptable use policies regarding accessing the Internet from locations like the Control or Equipment Rooms

# Conclusion

- Many modern prisons/jails were designed 10 years ago before these attacks were known
- Improved communication/interaction between IT and physical security
- Enforcing and updating procedures and policies regarding acceptable use of facility computers
- Patch PLC and controlling computer's software
- When PLCs are in use in secured areas, use heightened security procedures

# Acknowledgments

- The CISO of a State in the U.S. who is cognizant about computer security and is working to improve security in correctional facilities
- The Feds who invited us for a briefing on our research
- Law Enforcement Officers who provided us with a tour and discussed their concerns about the current state of the correctional system

# Special Thanks



CORE Security Technologies for publishing our work and teaming with us for correctional facility pen test projects

# Contact Us

- **Tiffany Rad**
  - > [Tiffany@elcnetworks.com](mailto:Tiffany@elcnetworks.com)
- **Teague Newman**
  - > [Teague@day0.net](mailto:Teague@day0.net)
- **John Strauchs**
  - > [John.Strauchs@strauchs-llc.com](mailto:John.Strauchs@strauchs-llc.com)

For questions or inquiries about penetration tests of correctional facilities, contact us or [cjohanson@coresecurity.com](mailto:cjohanson@coresecurity.com)