PLC Playground: Hands-On Industrial Control Systems Attacks

This briefing, presentation, or document is for information only.
No US Government commitment to sell, loan, lease, co-develop
or co-product defense articles or provide defense services is implied or intended

Introduction to Cyber-Physical Systems

The AFIT of Today is the Air Force of Tomorrow.

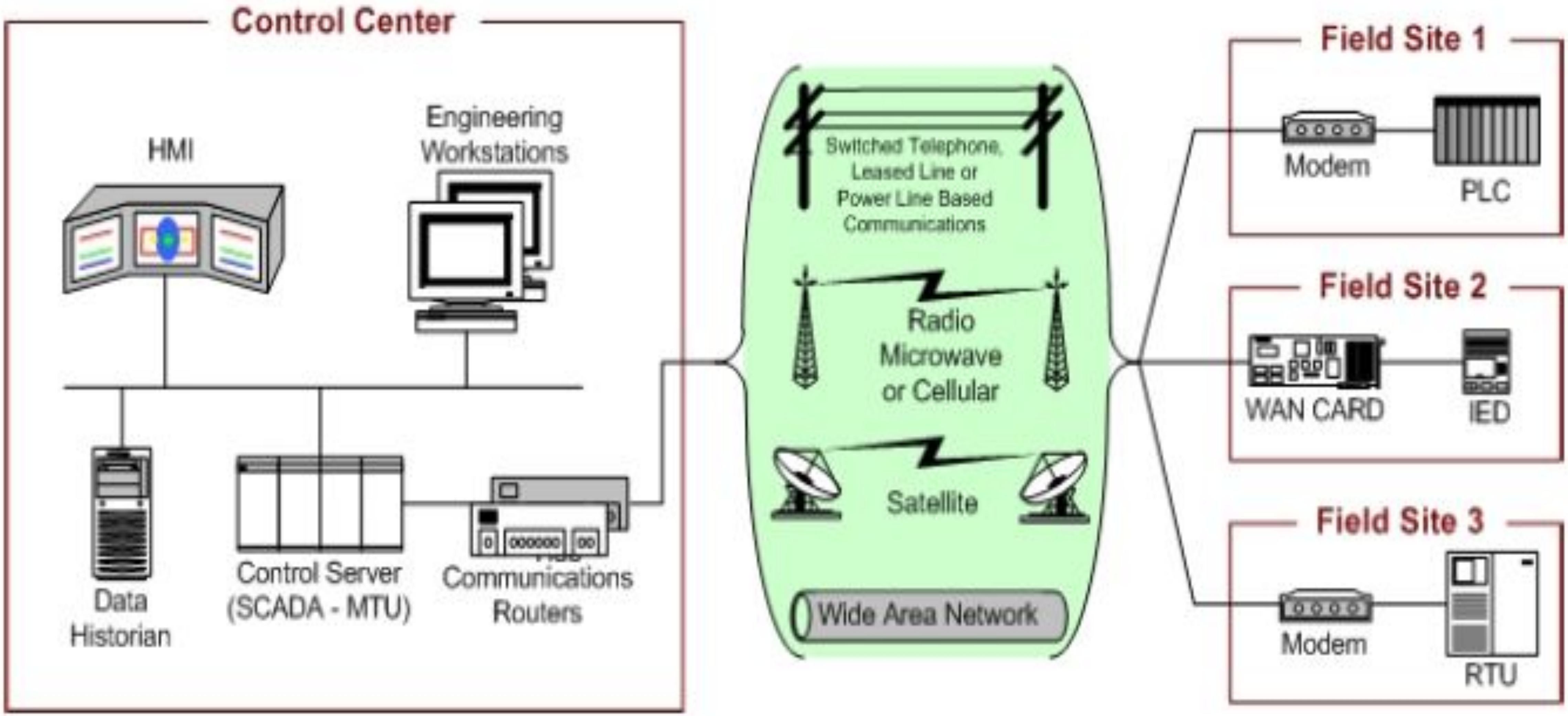
- Cyber-Physical Systems are integrations of computing, networking, and physical processes.
- Software controls physical components like motors, sensors, valves, and pumps.
- Real-time responsiveness is critical: delays can lead to safety or mission failure

Industrial Robots
GPS
GPS Receivers
Digital Cameras
DVD Players
Wireless Routers
Embedded Systems
MP3 Players
Set top Boxes
Gaming Consoles
Photocopiers
Microwave Ovens

What are Industrial Control Systems?

- Industrial Control Systems (ICS) are systems that integrate computation, networking, and physical processes to monitor and control industrial operations.Examples: Power grids, water treatment plants, manufacturing assembly lines.

Industrial Control Systems



Source: NIST Special Publication 800-82 r2, Guide to Industrial Control Systems (ICS) Security.

Key Components of ICS

- Sensors: Measure physical parameters (e.g., temperature, pressure).
- Actuators: Respond to control signals (e.g., motors, valves).
- Controllers: Devices like Programmable Logic Controllers (PLCs) or Distributed Control Systems (DCS) that process inputs and adjust processes.
- Human-Machine Interface (HMI): Enables operators to monitor and interact with the system.

Why ICS is Important?

- Supports essential services like energy, water, transportation, and manufacturing.
- Plays a vital role in ensuring efficiency, safety, and reliability in industrial operations.

Common Examples of ICS

- Energy Sector: Supervisory Control and Data Acquisition (SCADA) systems in power plants.
- Transportation: Automated signaling in railway systems.
- Manufacturing: Assembly line automation in car production.
- Utilities: Water distribution and sewage treatment systems.

Operational Technology

Source: https://commons.wikimedia.org/wiki/File:Transfer_Pump_Station.jpg

What is CI?

- Chemical
- Commercial Facilities
- Communications
- Crit. Manufacturing
- Dams
- Defense Industrial
- Emergency Services
- Energy

- Financial Services
- Food & Agriculture
- Govt. Facilities
- Healthcare
- Information Tech
- Nuclear
- Transportation
- Water & Wastewater

Public or private?

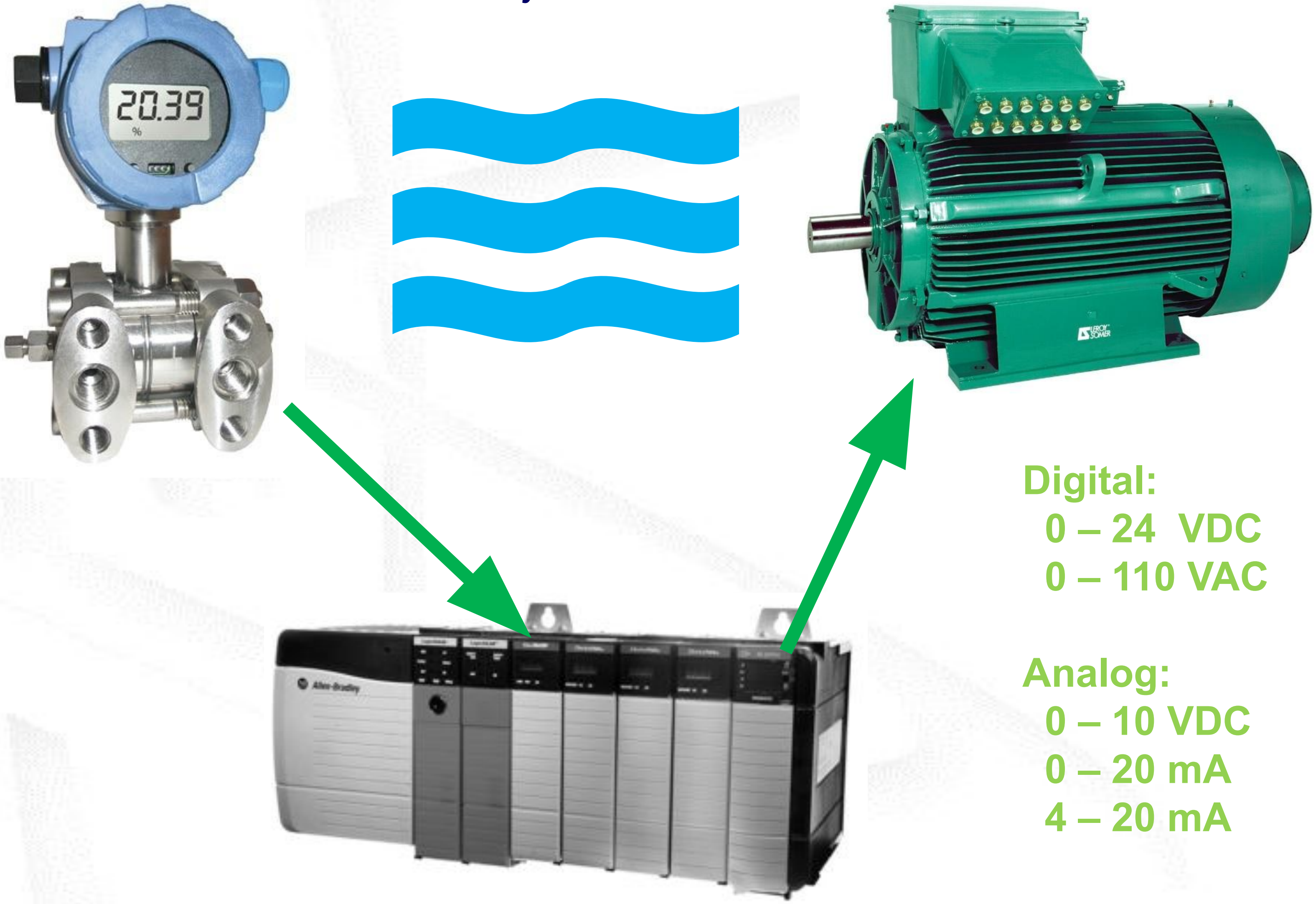
Components

- Building Automation – HVAC, access control
- Power – distribution, backup generation, conservation
- Water – treatment and waste
- Security – perimeter defenses, cameras
- Transportation – traffic lights, street lights
- Emergency Services – police, fire, EMS
- Flight Line – lights, communications
- Weapon Systems
- Fueling Systems

Field Sites

Image: https://www.reeng.com.au/products/control-systems/

Field Sites

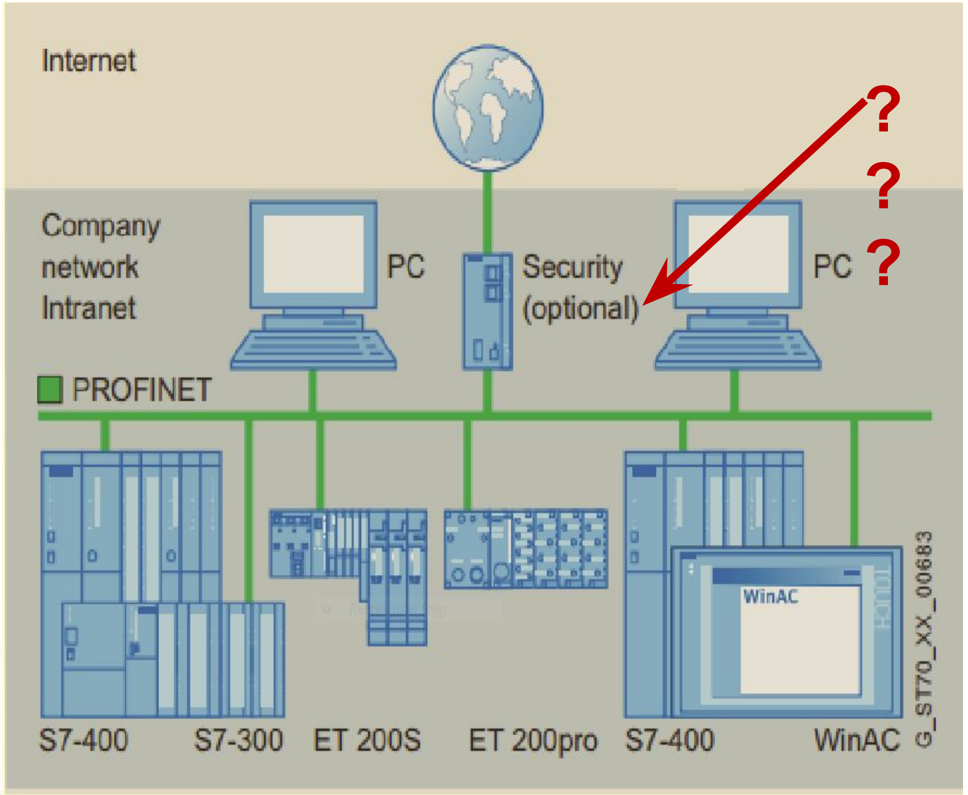


Digital:
- 0 – 24 VDC
- 0 – 110 VAC

Analog:
- 0 – 10 VDC
- 0 – 20 mA
- 4 – 20 mA

ICS and Internet Connectivity

- Modernization of ICS:
  - Increasing integration of Industrial Control Systems (ICS) with IT networks and the internet.
  - Adoption of protocols like PROFINET and Ethernet/IP for communication.
- Unintended Consequences:
  - Direct or indirect internet access introduces significant vulnerabilities.
  - Legacy ICS systems often lack built-in security measures.



Access via Industrial Ethernet network to PN CPU with web server

Key Challenges

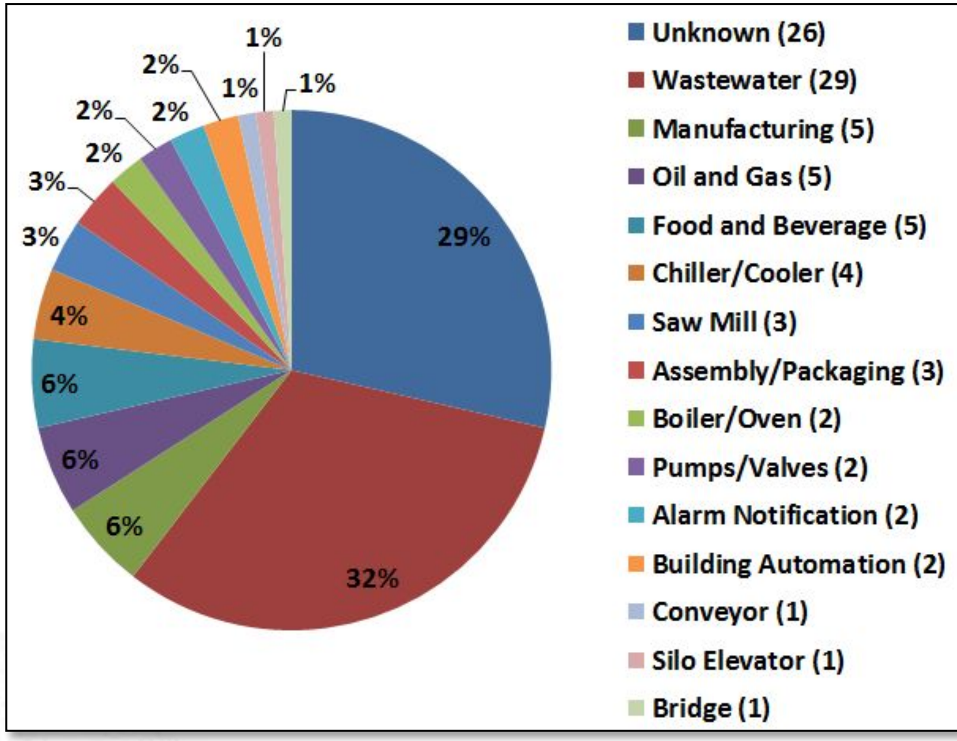
- Weak or Optional Security
  - Security mechanisms are often not prioritized or are optional in ICS setups.
  - Example: Firewalls or intrusion detection systems are frequently omitted.
- Legacy Systems
  - Many ICS were not designed with internet connectivity in mind.
  - Patching and updating older systems can be difficult without downtime.
- Attack Surface Expansion
  - Direct exposure of ICS devices to the internet increases the risk of:
    - Unauthorized Access via poorly secured remote connections.
    - Cyber Attacks like ransomware or data exfiltration.

EMCS

Source: Max Cornelisse

The Challenge of Internet-Exposed Devices

- Internet-facing devices are ICS components that are directly accessible from the internet without adequate security controls.
- A significant number of critical devices (e.g., wastewater, manufacturing) are exposed.
- Many are listed as "Unknown," indicating poor inventory or security practices.



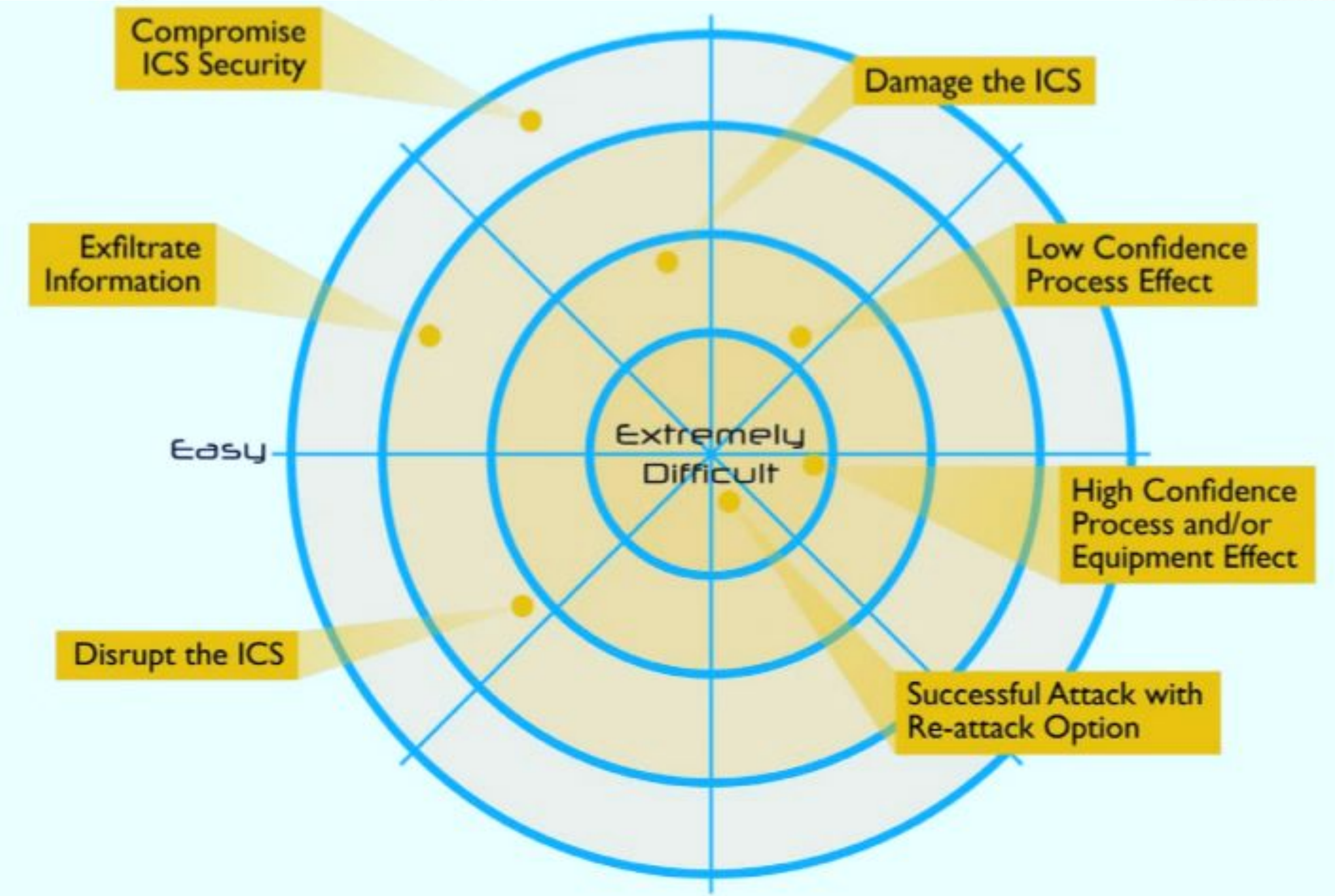
Internet Facing Devices

Bridge PLC

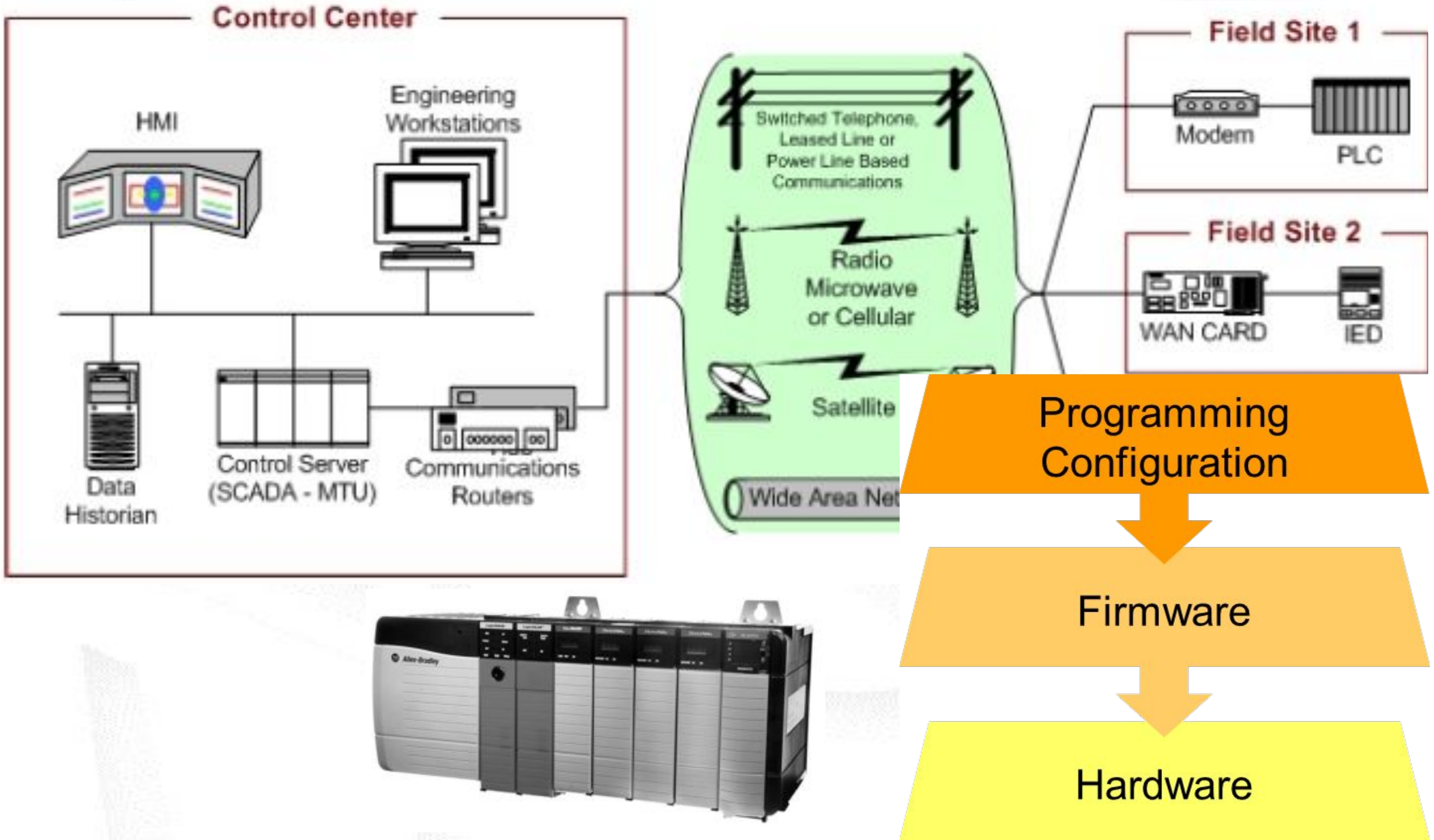
<u>Source</u>: Max Cornelisse

ICS Attack Difficulty

The AFIT of Today is the Air Force of Tomorrow.


Compromise ICS Security
Damage the ICS
Exfiltrate Information
Low Confidence Process Effect
Easy
Extremely Difficult
High Confidence Process and/or Equipment Effect
Disrupt the ICS
Successful Attack with Re-attack Option

Targets



Programming Configuration

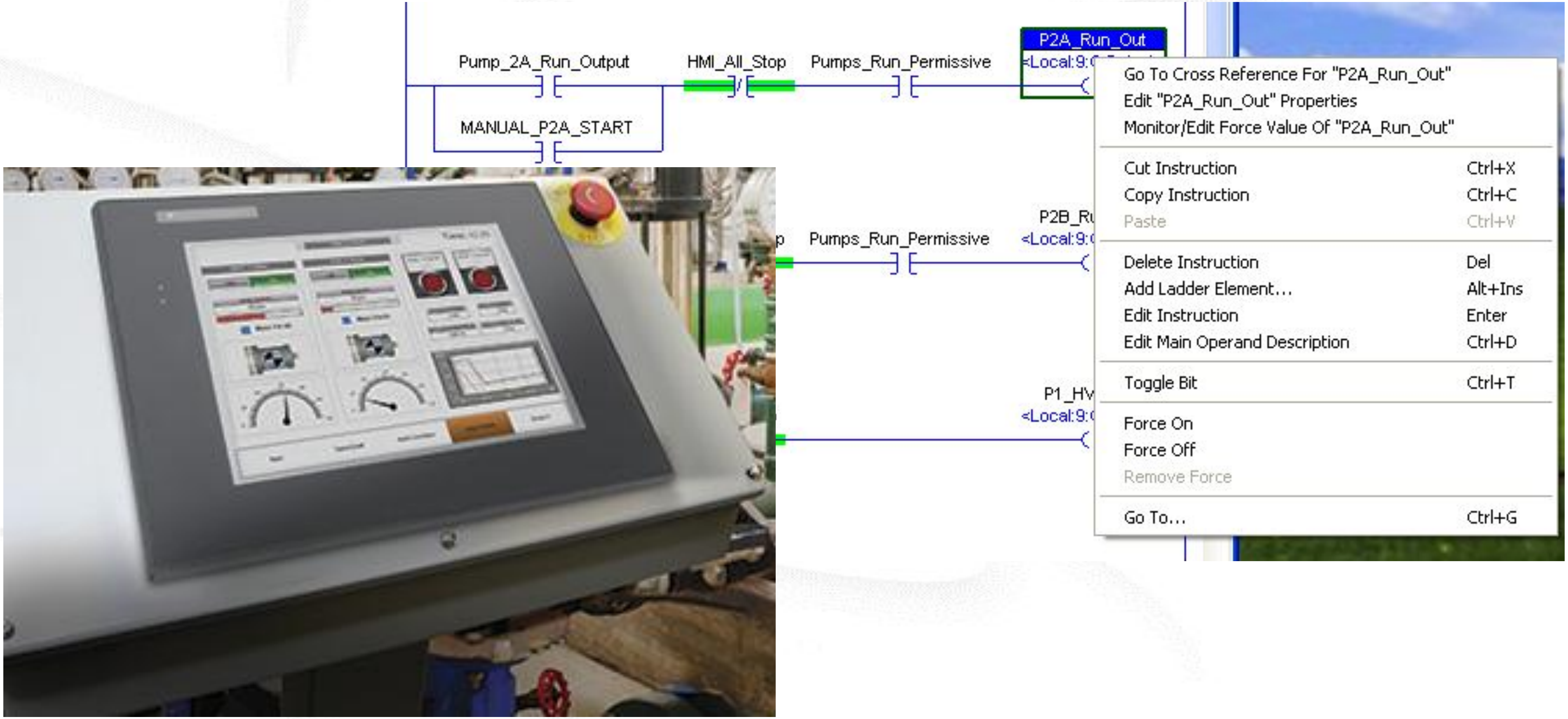
Firmware

Hardware

Source: NIST Special Publication 800-82 r2, Guide to Industrial Control Systems (ICS) Security.

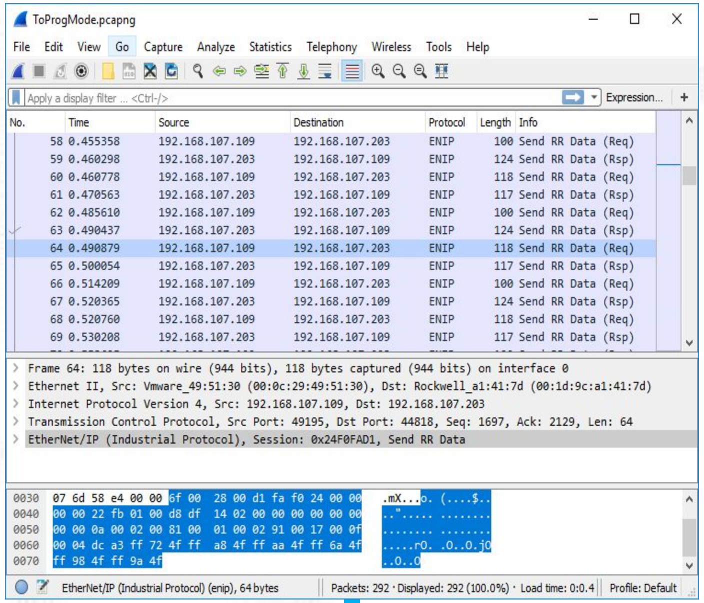
Vendor Tools

The AFIT of Today is the Air Force of Tomorrow.



Easy Defense

Build Your Own Tools

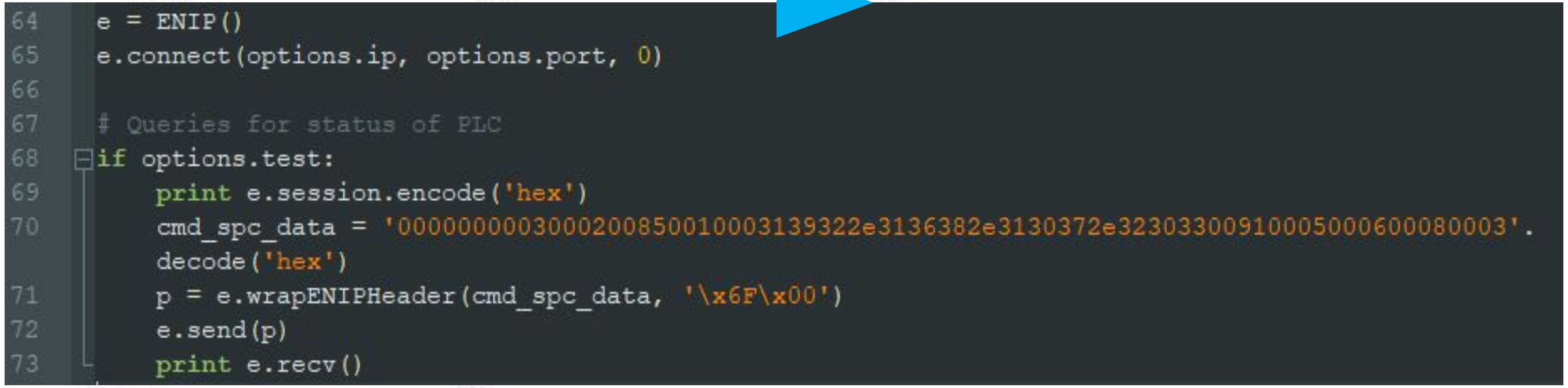


No.	Time	Source	Destination	Protocol	Length	Info
58	0.455358	192.168.107.109	192.168.107.203	ENIP	100	Send RR Data (Req)
59	0.460298	192.168.107.203	192.168.107.109	ENIP	124	Send RR Data (Rsp)
60	0.460778	192.168.107.109	192.168.107.203	ENIP	118	Send RR Data (Req)
61	0.470563	192.168.107.203	192.168.107.109	ENIP	117	Send RR Data (Rsp)
62	0.485610	192.168.107.109	192.168.107.203	ENIP	100	Send RR Data (Req)
63	0.490437	192.168.107.203	192.168.107.109	ENIP	124	Send RR Data (Rsp)
64	0.490879	192.168.107.109	192.168.107.203	ENIP	118	Send RR Data (Req)
65	0.500054	192.168.107.203	192.168.107.109	ENIP	117	Send RR Data (Rsp)
66	0.514209	192.168.107.109	192.168.107.203	ENIP	100	Send RR Data (Req)
67	0.520365	192.168.107.203	192.168.107.109	ENIP	124	Send RR Data (Rsp)
68	0.520760	192.168.107.109	192.168.107.203	ENIP	118	Send RR Data (Req)
69	0.530208	192.168.107.203	192.168.107.109	ENIP	117	Send RR Data (Rsp)

```
> Frame 64: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
> Ethernet II, Src: Vmware_49:51:30 (00:0c:29:49:51:30), Dst: Rockwell_a1:41:7d (00:1d:9c:a1:41:7d)
> Internet Protocol Version 4, Src: 192.168.107.109, Dst: 192.168.107.203
> Transmission Control Protocol, Src Port: 49195, Dst Port: 44818, Seq: 1697, Ack: 2129, Len: 64
> EtherNet/IP (Industrial Protocol), Session: 0x24F0FAD1, Send RR Data
```

```
0030  07 6d 58 e4 00 00 6f 00  28 00 d1 fa f0 24 00 00   .mX...o. (....$..
0040  00 00 22 fb 01 00 d8 df  14 02 00 00 00 00 00 00   ..".... ........
0050  00 00 0a 00 02 00 81 00  01 00 02 91 00 17 00 0f   ........ ........
0060  00 04 dc a3 ff 72 4f ff  a8 4f ff aa 4f ff 6a 4f   .....rO. .O..O.jO
0070  ff 98 4f ff 9a 4f                                  ..O..O
```

EtherNet/IP (Industrial Protocol) (enip), 64 bytes | Packets: 292 · Displayed: 292 (100.0%) · Load time: 0:0.4 | Profile: Default



```
e = ENIP()
e.connect(options.ip, options.port, 0)

# Queries for status of PLC
if options.test:
    print e.session.encode('hex')
    cmd_spc_data = '0000000003000200850010003139322e3136382e3130372e32303300910005000600080003'.
    decode('hex')
    p = e.wrapENIPHeader(cmd_spc_data, '\x6F\x00')
    e.send(p)
    print e.recv()
```

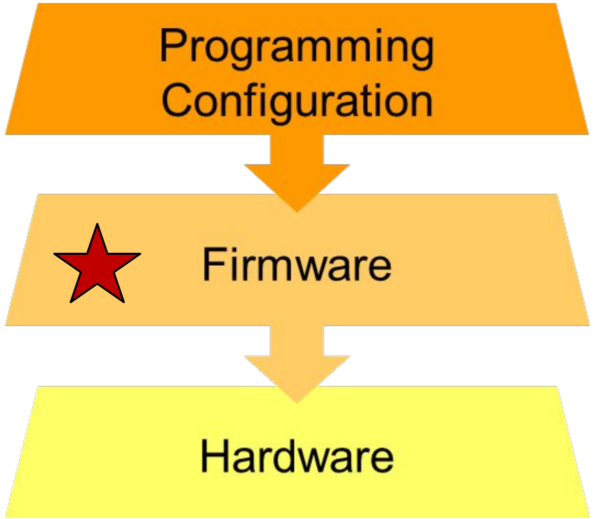
Firmware Implants

© UPS, 2003

Deployment

Payloads

Triggers



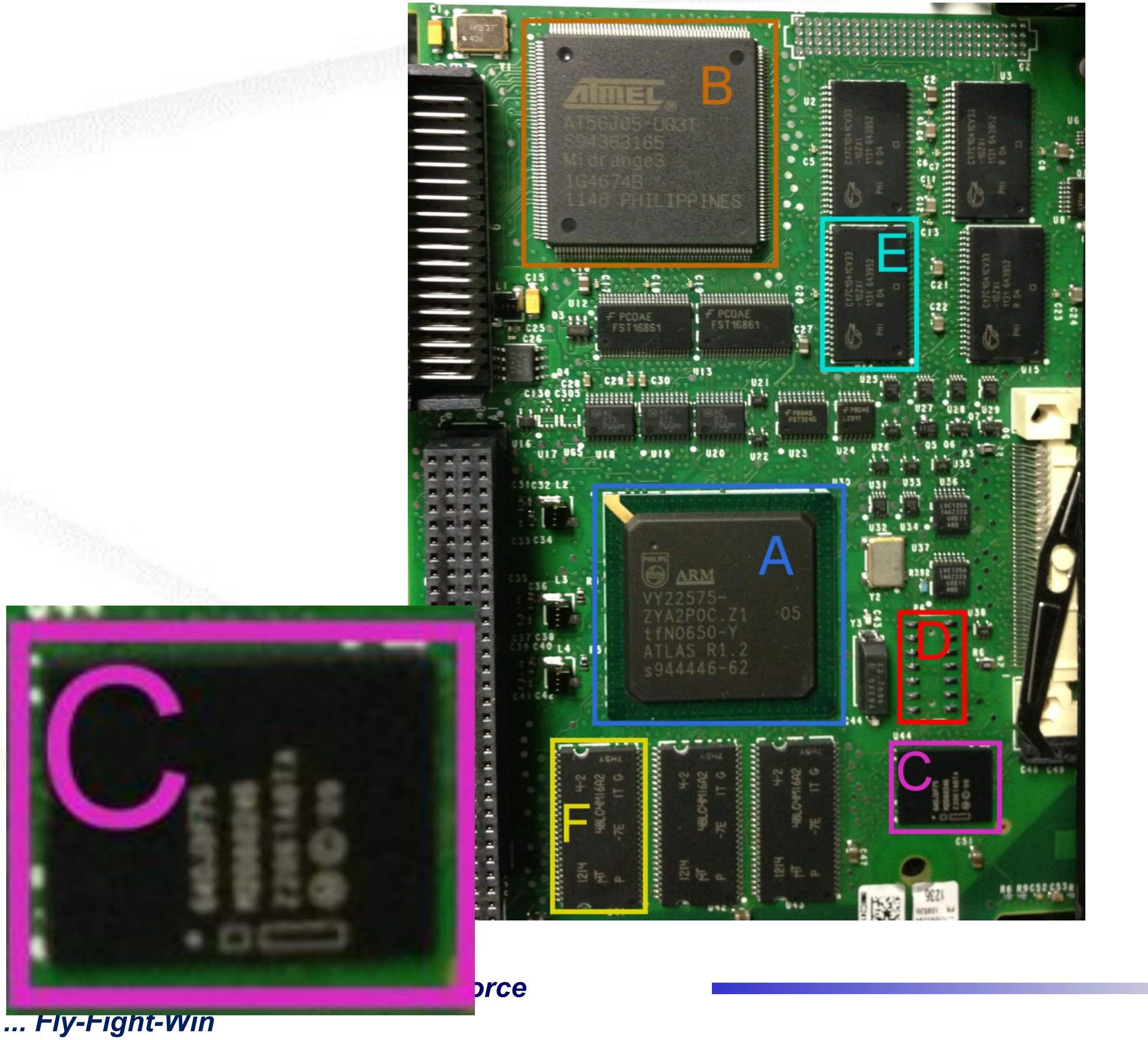
Programming Configuration

★ Firmware

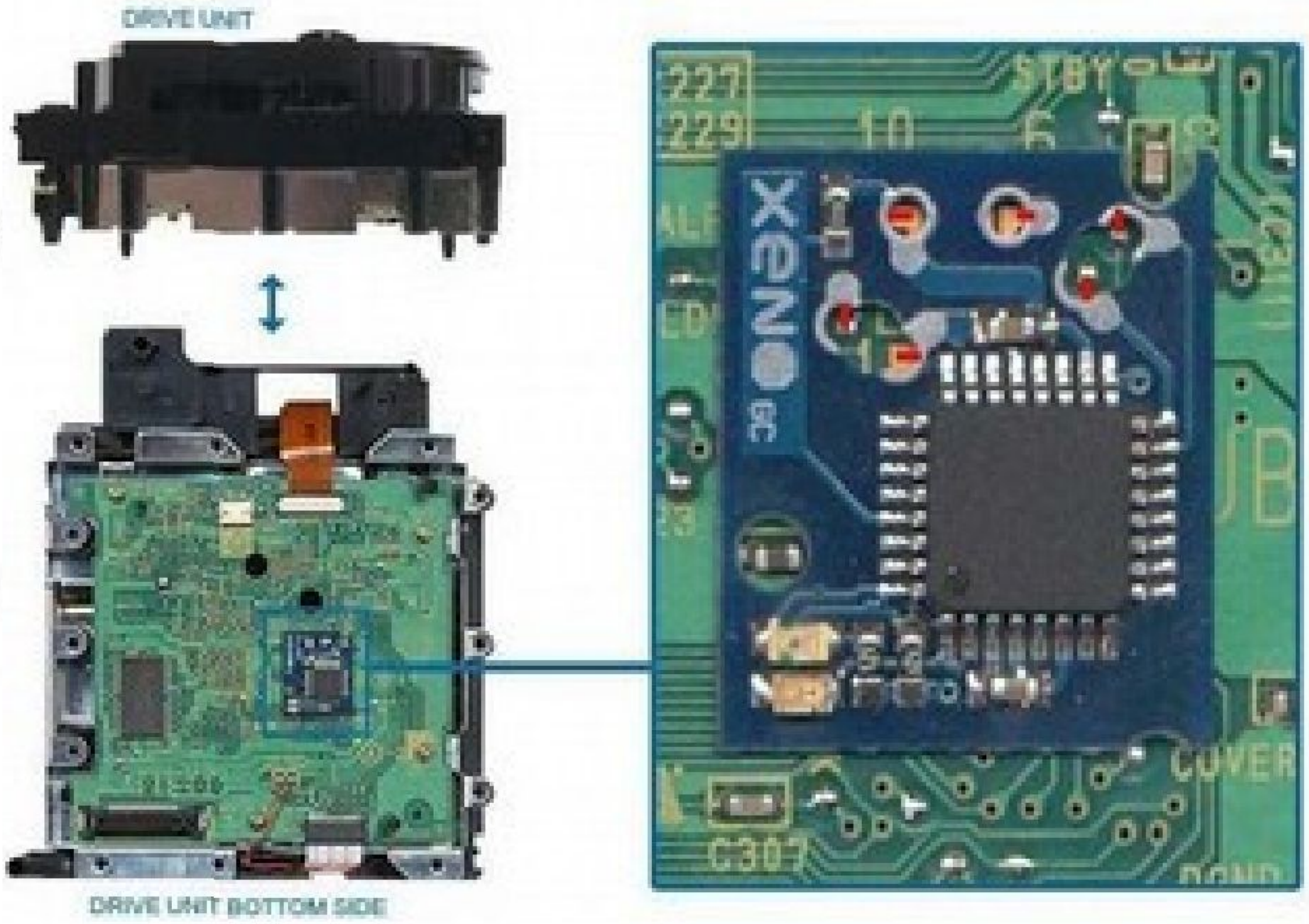
Hardware

Why Firmware Implants

- Full control over device
- Bypass security mechanisms
- Include backdoors
- Self propagation
- Impossible to detect
- Impossible to clean device
- Unless you use physical access



Hardware

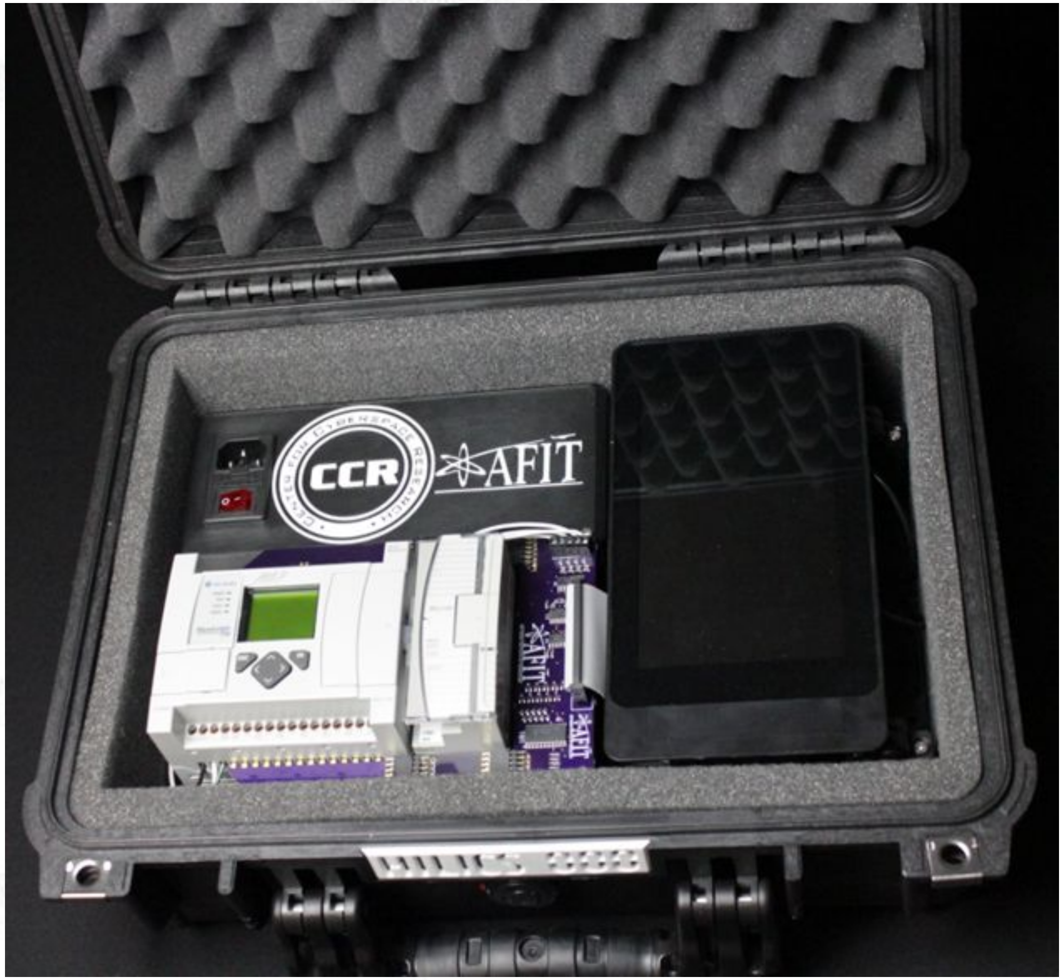

DRIVE UNIT
DRIVE UNIT BOTTOM SIDE
227
229
STBY
10
6
xeno
COVER
C303

Defense – NIST Framework

- Identify – Passive monitoring
- Protect – Isolation/segmentation
- Detect – Deep packet inspection
- Respond – Manual operation
- Recover – Bring back automation

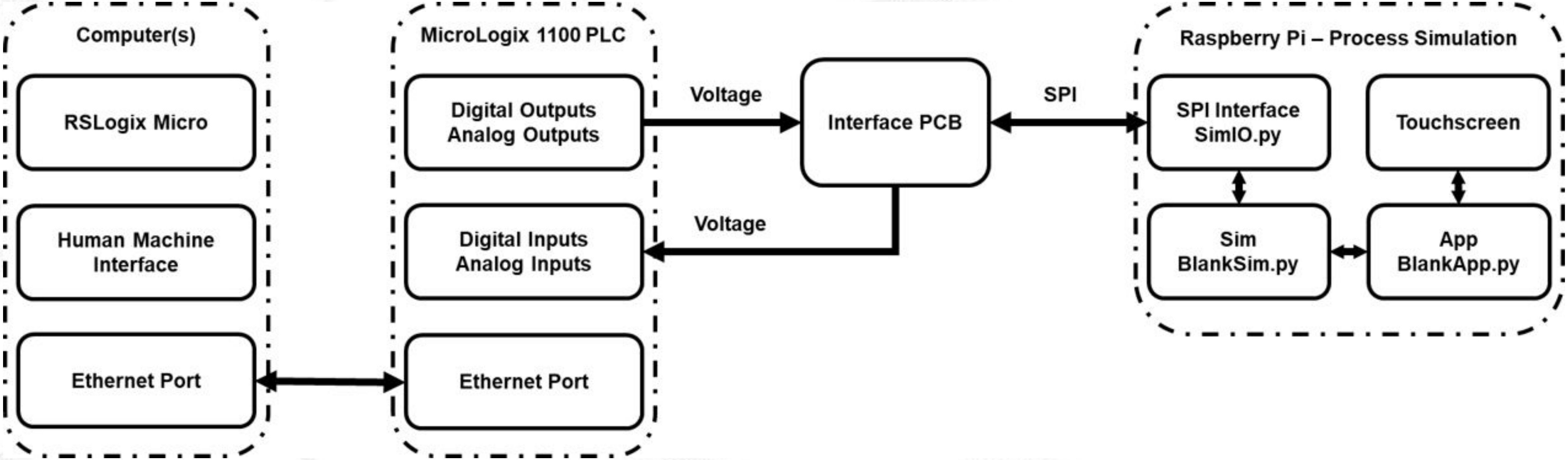
The HILICS Platform

- Hardware-in-the-Loop ICS
- Real ICS equipment is expensive, large, and difficult to scale.
  - Water tanks, compressors, and valves are impractical for classrooms.
  - One physical trainer can’t support 30+ students simultaneously.
- Emulation alone isn’t realistic, real PLC hardware matters
- As far as the PLC knows, it's controlling a real industrial process.



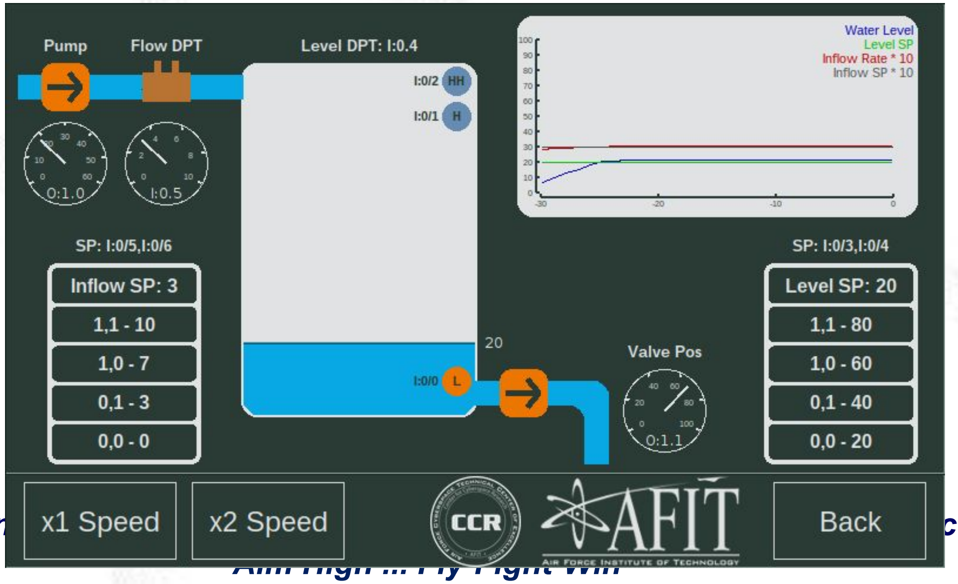
https://github.com/sdunlap-afit/hilics

HILICS Architecture



HILICS Architecture

- Raspberry Pi acts as the physical process simulation (e.g., door, tank).
- MicroLogix 1100 is the real PLC you're attacking or defending.
- All traffic (VNC + PLC) is routed via the Pi’s IP using port forwarding.
- Students access their kits remotely using web browser + VPN.
- The setup mimics a NATed industrial environment with remote access.



Initial Setup Instructions

- Open noVNC in Browser
  - VNC gives you visual access to the Raspberry Pi simulation.
  - All tools run in this environment.
- Access PLC Web Interface
  - Navigate to http://<kit_ip> to confirm PLC is online.
- Configure RSLinx
  - Set up Ethernet/IP driver to talk to the MicroLogix 1100.
- Launch RSLogix 500
  - Upload/download the PLC logic.
  - Go online to observe or modify the ladder logic.

HILICS Toolchain

Tool	Purpose
noVNC	Browser-based remote desktop for Raspberry Pi GUI
PLC Web UI	Verify connectivity and PLC identity
RSLinx Classic	Communication driver setup (Ethernet/IP) for RSLogix
RSLogix 500	Upload/download logic, modify ladder diagram, go online
Wireshark	(Optional) Packet capture to see ICS traffic

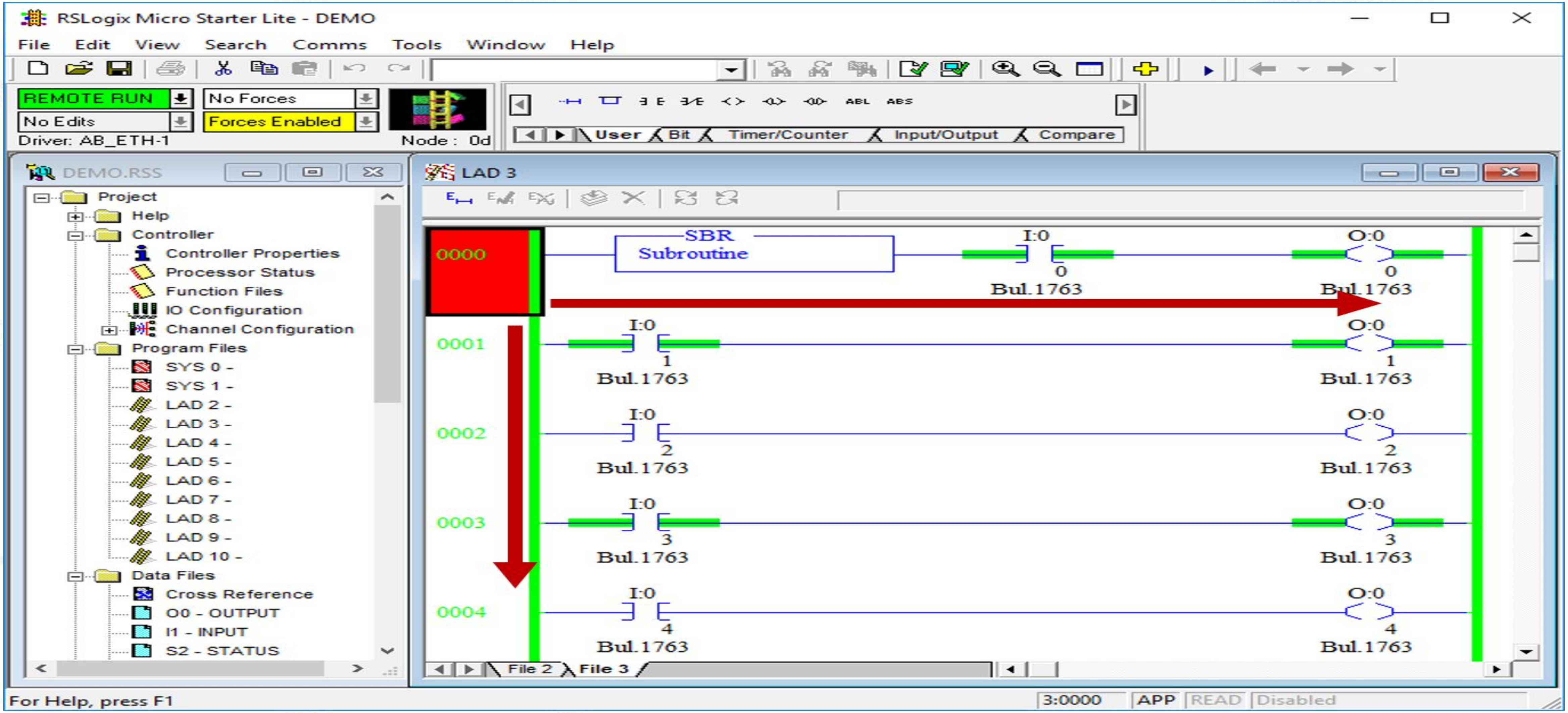
What is Ladder Logic?

- Ladder Logic is the only language supported by the MicroLogix 1100.
- Visual, circuit-like programming language designed for reliability and uptime.
- If you come from C++ or Python: it will feel alien.
- If you've used AND/OR gates or FPGAs: it'll feel familiar.
- Main subroutine (LAD 2) runs in an infinite loop — designed to run 24/7.

Anatomy of a Ladder Program

- Ladders = Subroutines or files (e.g., LAD 2)
- Rungs = Think of them like circuits
- Logic flow: Left → Right, Top → Bottom
- Input logic (left side) controls outputs (right side)
- Logic "flows" across the rung like electricity:
  - Series (AND): All must be true
  - Parallel (OR): One path must be true

Anatomy of a Ladder Program



RSLogix Micro Starter Lite - DEMO

REMOTE RUN

No Edits

No Forces

Forces Enabled

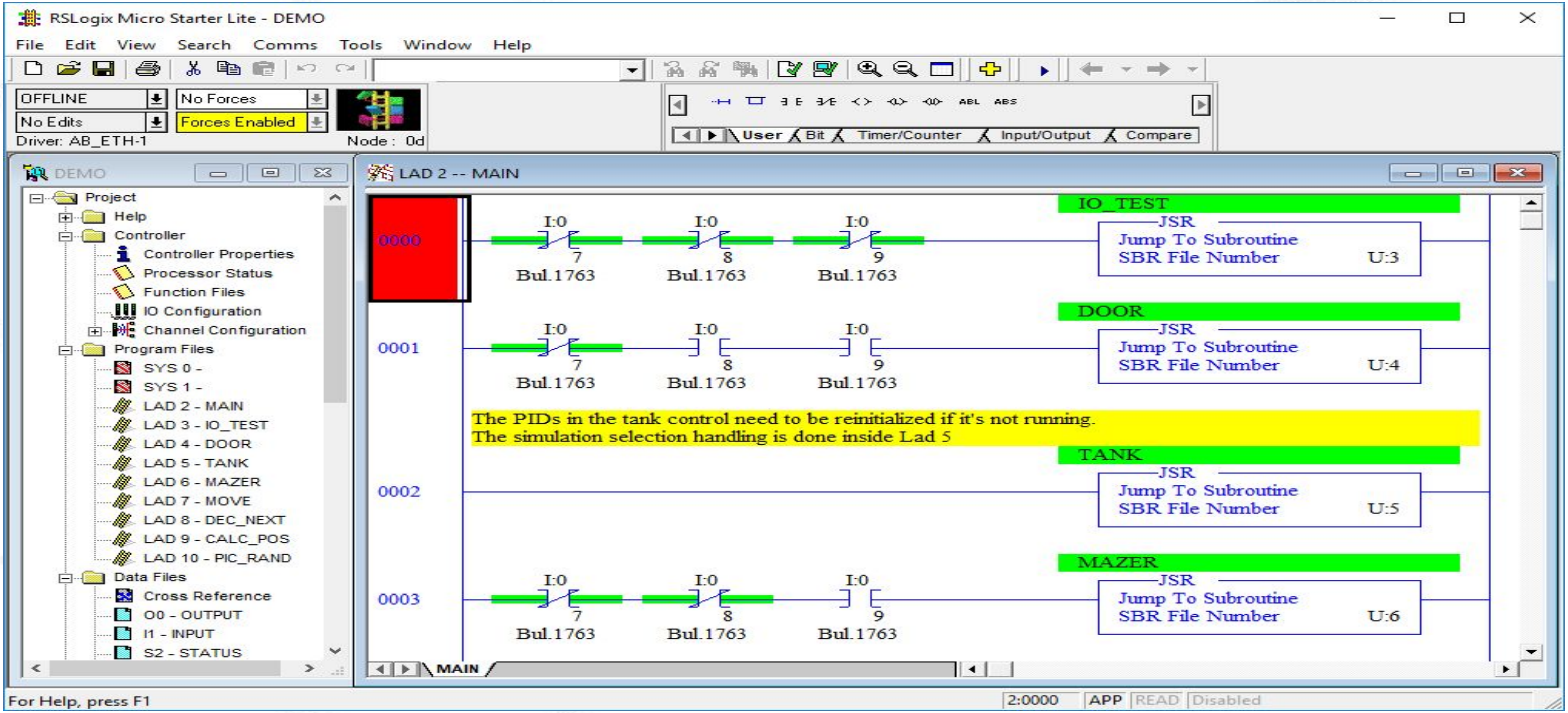
Driver: AB_ETH-1

Node : 0d

For Help, press F1

3:0000 APP READ Disabled

Ladders



RSLogix Micro Starter Lite - DEMO

OFFLINE
No Forces
No Edits
Forces Enabled
Driver: AB_ETH-1
Node : 0d

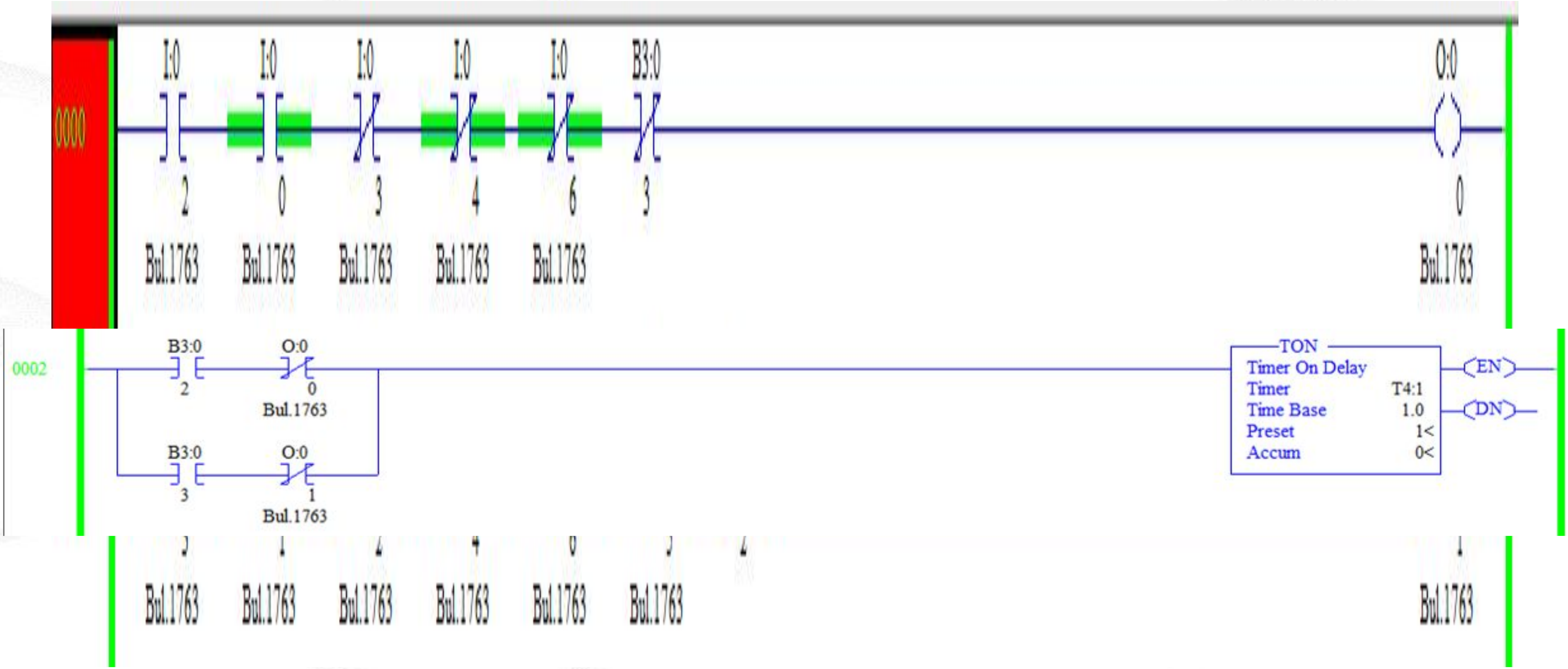
LAD 2 -- MAIN

The PIDs in the tank control need to be reinitialized if it's not running.
The simulation selection handling is done inside Lad 5

2:0000 APP READ Disabled

For Help, press F1

Rungs



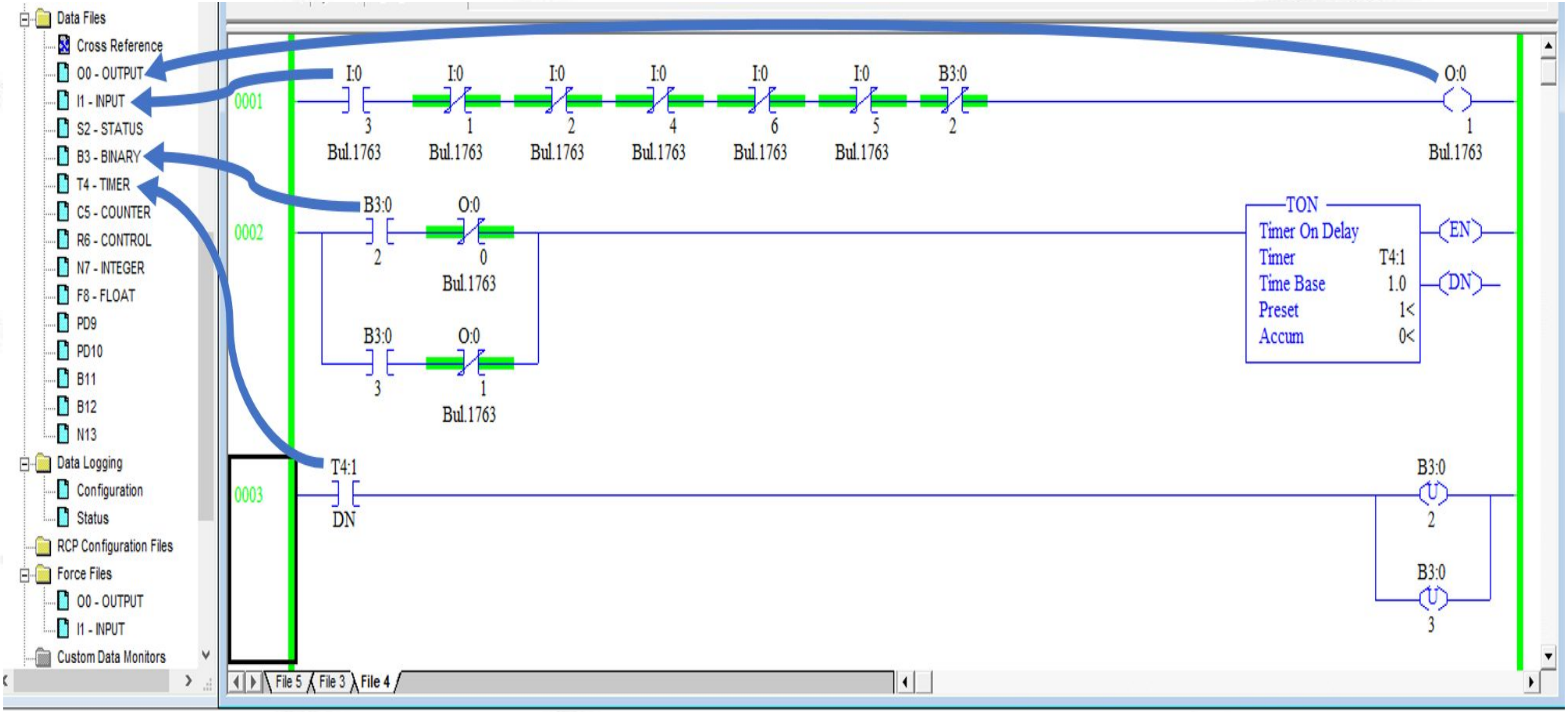
TON
Timer On Delay
Timer T4:1
Time Base 1.0
Preset 1<
Accum 0<

PLC Variables – Data Files

- Data stored in typed files:
  - Inputs: I:0/3, Outputs: O:0/2, Binary: B3:1/0, Integer: N7:0
- Format:
  - I:0/3 → Input file 0, bit 3
  - B3:1/5 → Binary file 3, row 1, bit 5

Type	File	Access	Example
Input	I	Read-only	I:0/3
Output	O	Write-only	O:0/2
Binary	B3	R/W	B3:1/0
Integer	N7	R/W	N7:0

PLC Variables – Data Files



Instruction Types and Flow

- Examine If Closed (XIC) – True if input is HIGH (e.g., I:0/3)
- Examine If Open (XIO) – True if input is LOW (inverted logic)
- Output Energize (OTE) – Turns on an output if rung is true
- JSR – Jump to Subroutine (e.g., call LAD 4, 5, or 6)

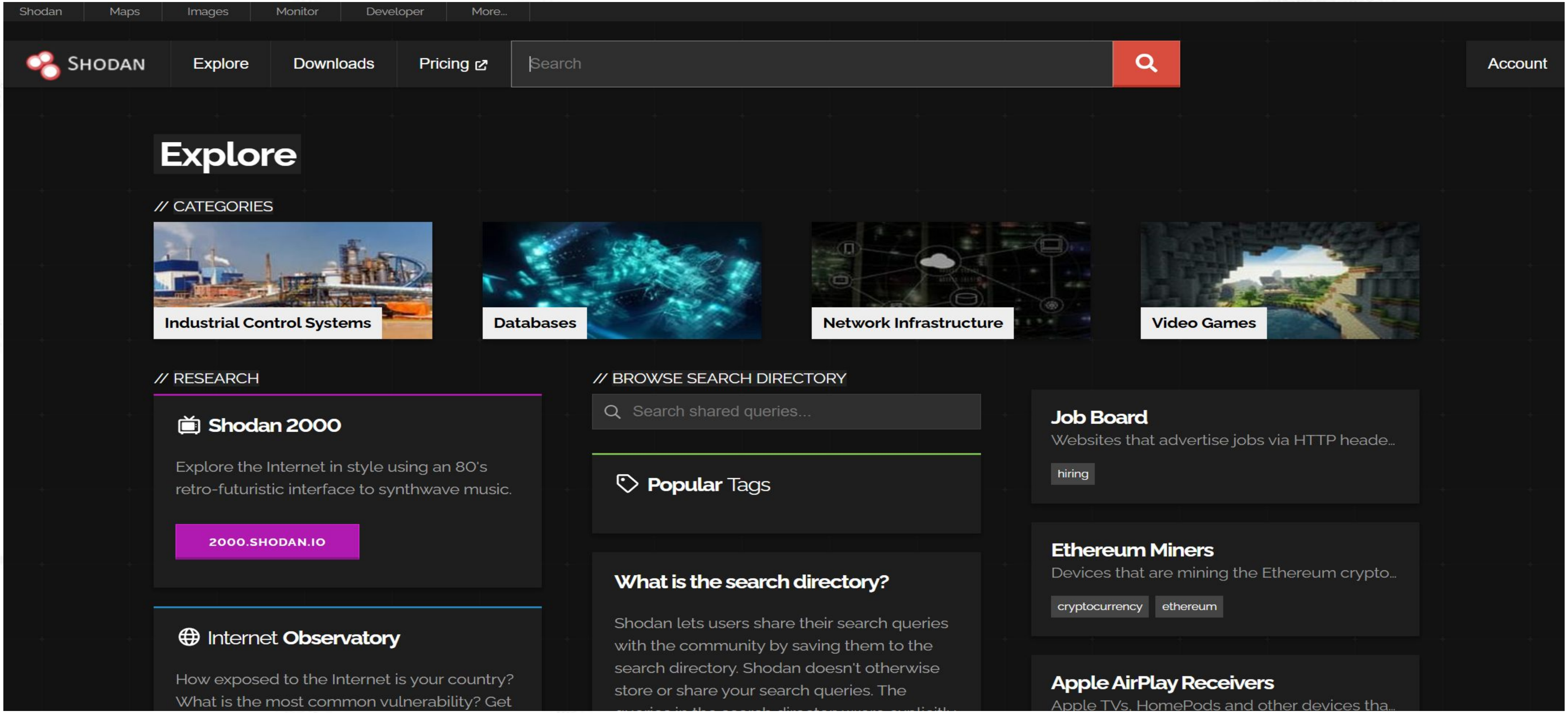
Exercise 1 – Familiarization

Exercise 2 – Door Simulation Attacks

Exercise 3 – Fluid Tank Simulation Attacks

Shodan & ICS Exposure

The AFIT of Today is the Air Force of Tomorrow.



Explore

// CATEGORIES

Industrial Control Systems

Databases

Network Infrastructure

Video Games

// RESEARCH

Shodan 2000

Explore the Internet in style using an 80's retro-futuristic interface to synthwave music.

2000.SHODAN.IO

Internet Observatory

How exposed to the Internet is your country? What is the most common vulnerability? Get

// BROWSE SEARCH DIRECTORY

Search shared queries...

Popular Tags

What is the search directory?

Shodan lets users share their search queries with the community by saving them to the search directory. Shodan doesn't otherwise store or share your search queries. The

Job Board

Websites that advertise jobs via HTTP heade...

hiring

Ethereum Miners

Devices that are mining the Ethereum crypto...

cryptocurrency
ethereum

Apple AirPlay Receivers

Apple TVs, HomePods and other devices tha...

Exercise 4 – Custom Exploit Development

Questions