Ghost in the PLC – Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack

Written by Ali Abbasi
Research is done in Twente University

Ali Abbasi:

Page: wwwhome.cs.utwente.nl/~abbasia/
E-Mail: a.abbasi@utwente.nl
Twitter: www.twitter.com/bl4ckic3

Ph.D. candidate of Distributed and Embedded System Security group at University of Twente, Netherlands since November 2013. His research interests involve Embedded Systems Security mostly related to Industrial Control Systems and Real-Time Operating Systems.

Ghost in the PLC
Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack

Ali Abbasi[1] and Majid Hashemi[2]

[1] Distributed and Embedded Systems Security Group, University of Twente, The Netherlands,
{a.abbasi}@utwente.nl
[2] QuarksLab, France
mhashemi@quarkslab.com

Abstract. Input/Output is the mechanisms through which embedded systems interact and control the outside world. Particularly when employed in mission critical systems, the I/O of embedded systems has to be both reliable and secure. Embedded system's I/O is controlled by a pin based approach. In this paper, we investigate the security implications of embedded system's pin control. In particular, we show how an attacker can tamper with the integrity and availability of an embedded system's I/O by exploiting cerain pin control operations and the lack of hardware interrupts associated to them.

Keywords: Pin, SoC, Exploit, Attack, PLC, Rootkit

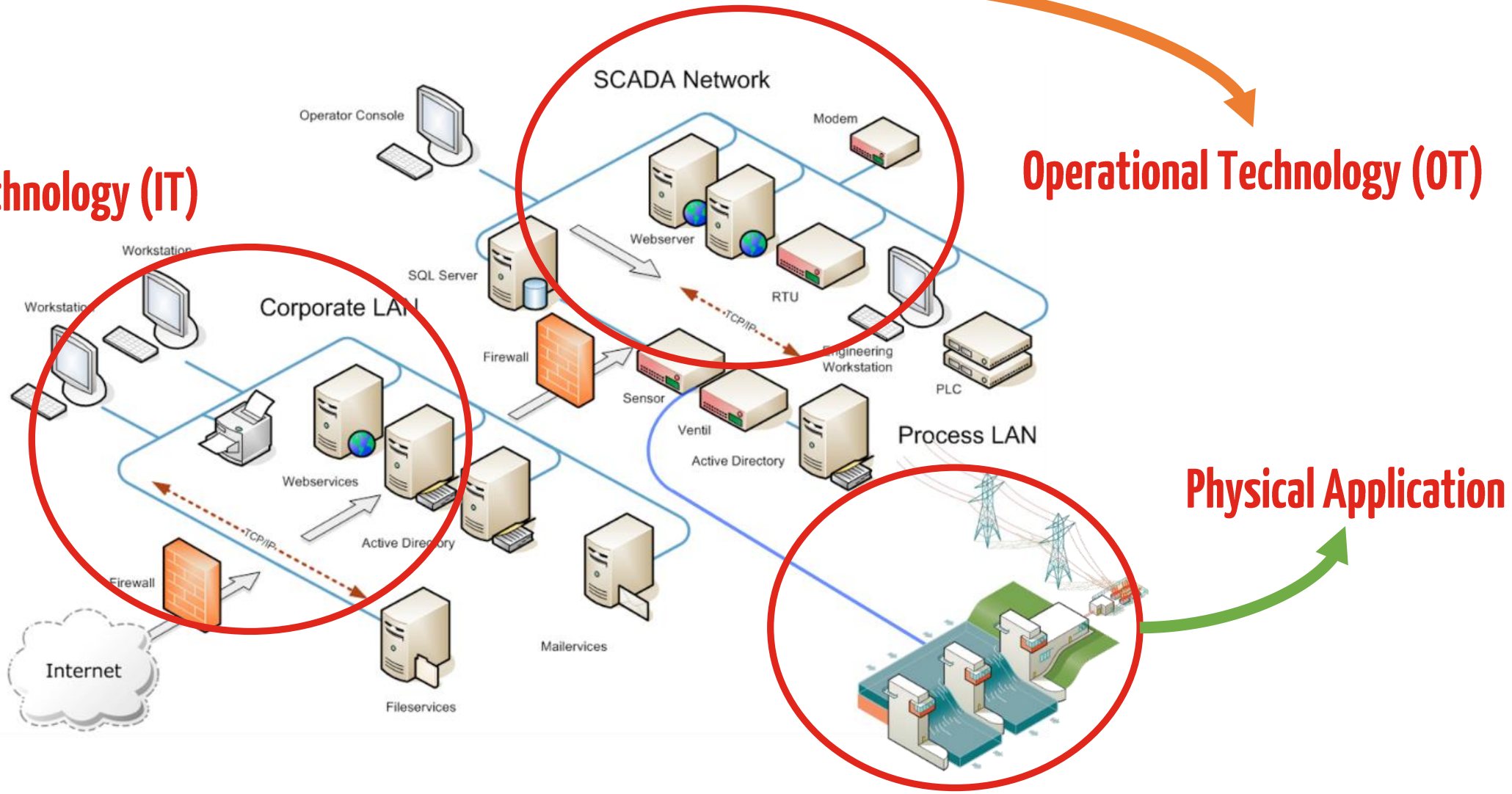
Industrial Control Systems

Industrial Control Systems

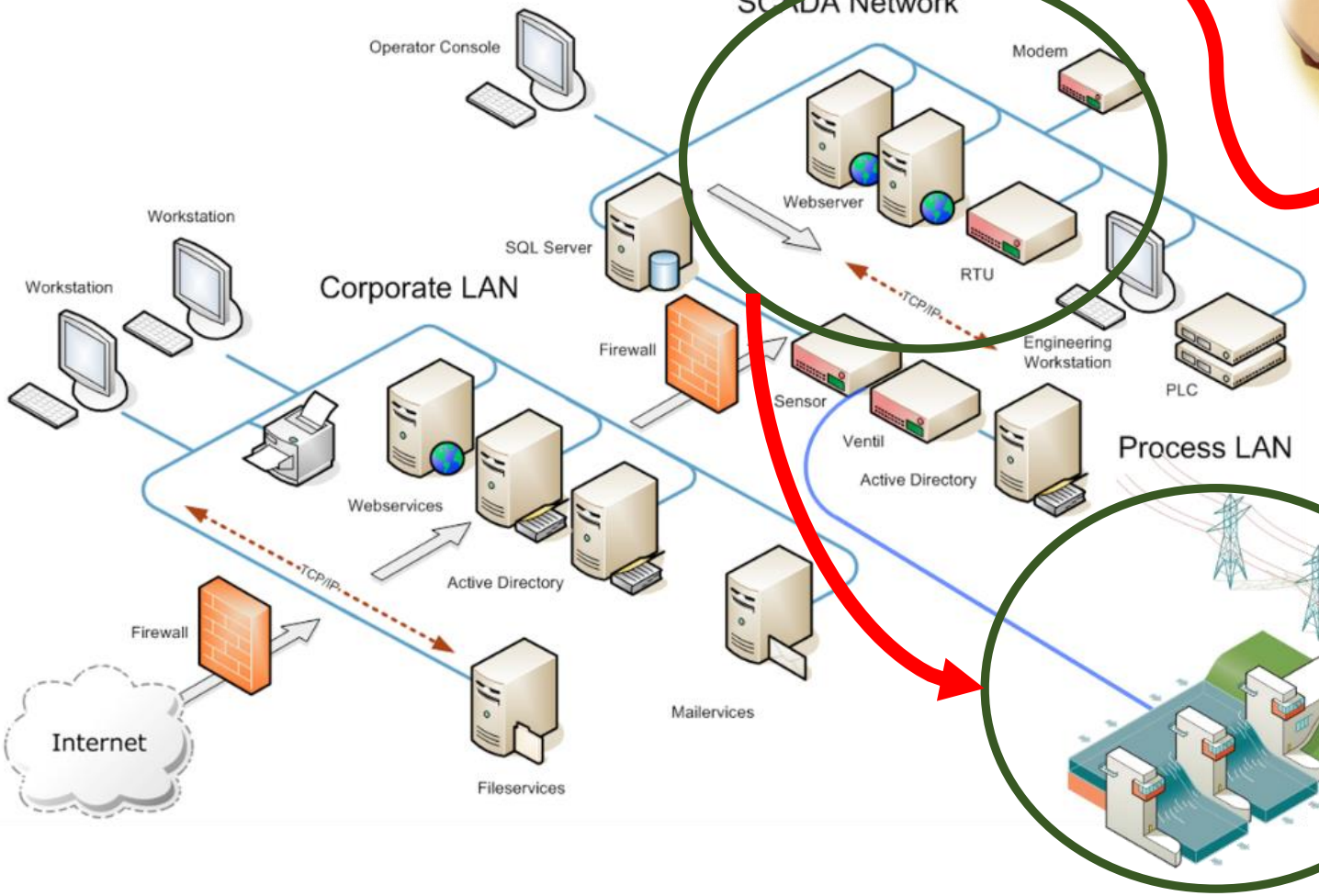
Information Technology (IT)

Operational Technology (OT)

Physical Application



Industrial Control Systems Hacking



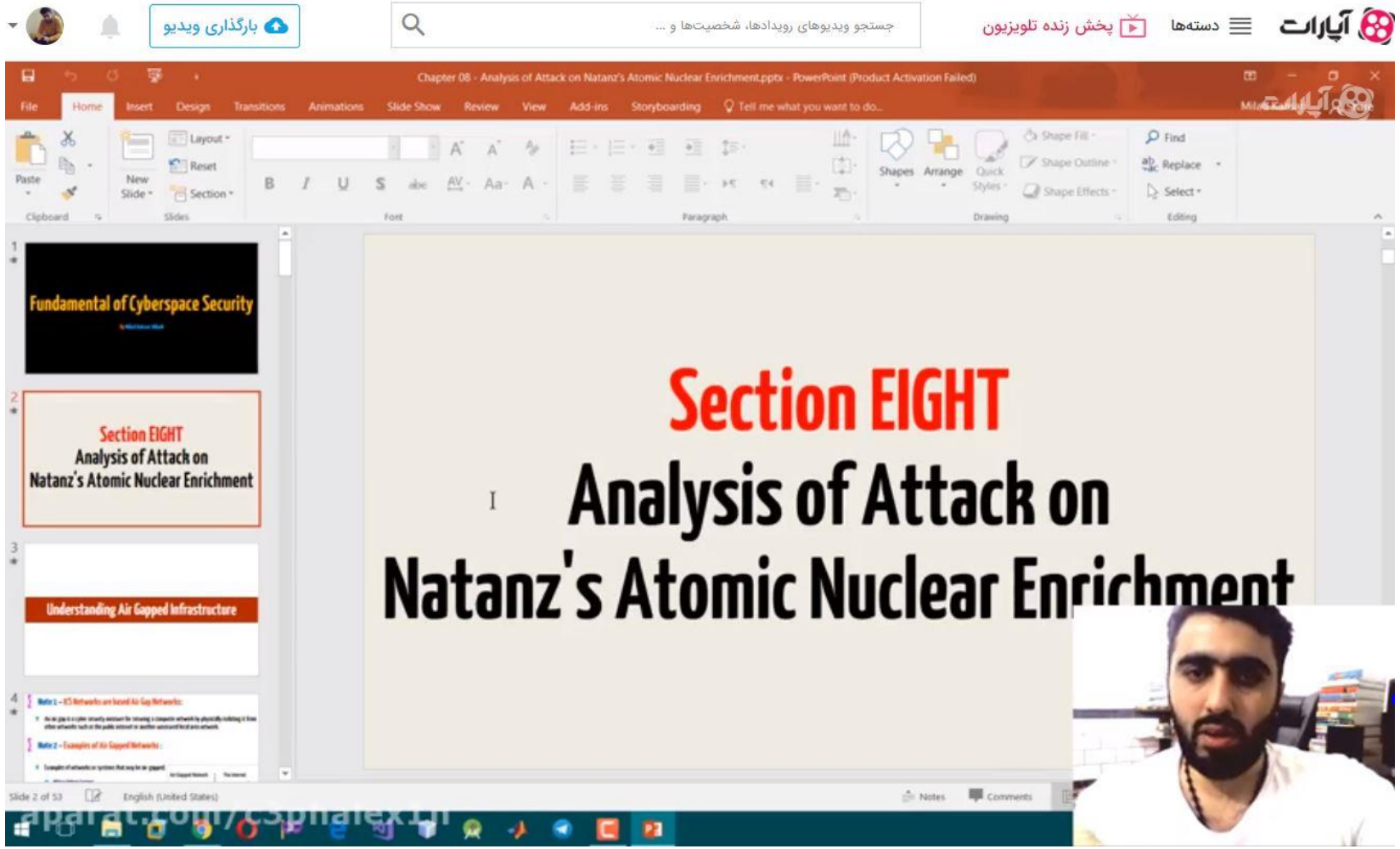
ICS Infrastructure

ICS Infrastructure:

- ≈ Air Gap Infrastructure
- ≈ Air Gap Attacks

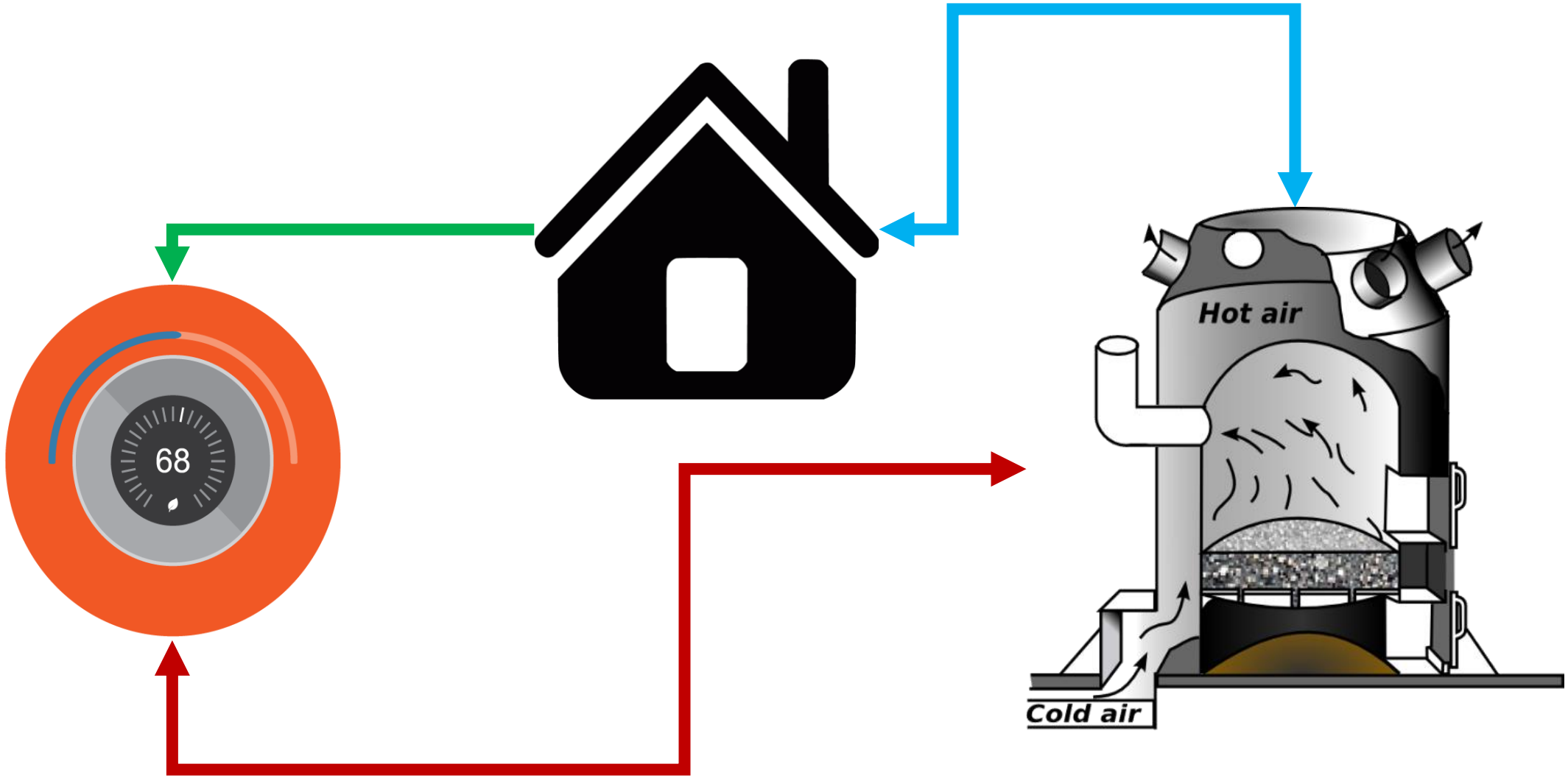
More Information:

http://www.aparat.com/v/lbjJl

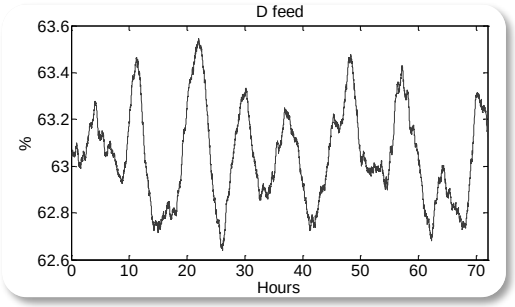


Process Control

Process Control 101



Control Loop

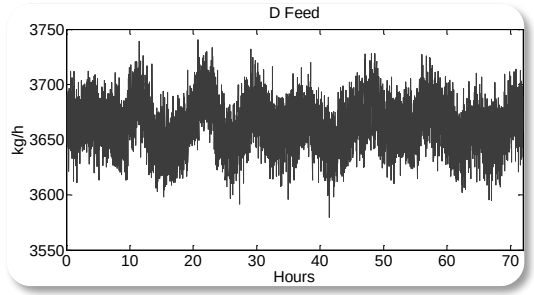


Actuators

Physical Process

Sensors

Control System

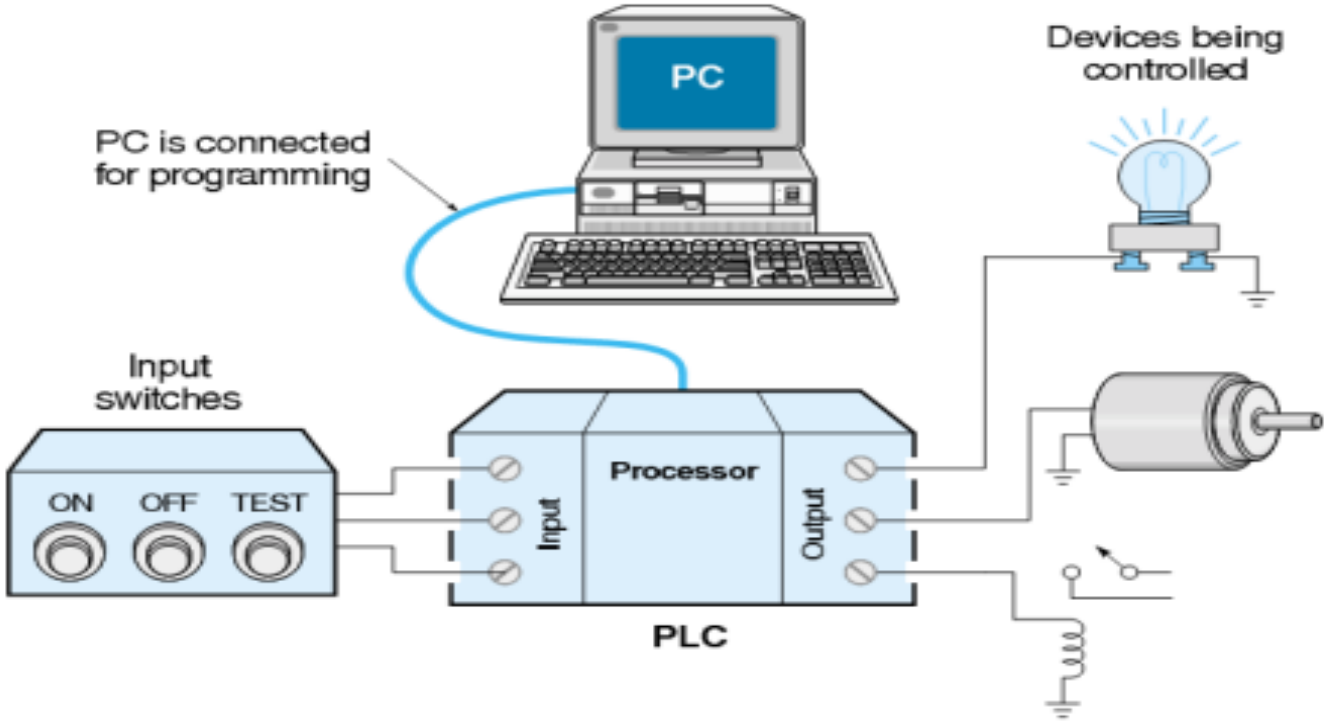


Control Equipment

1. In large scale operations control logic gets more complex than a thermostat.
2. One would need something bigger than a thermostat to handle it.
3. Most of the time this is a programmable logic controller (PLC).

What is a PLC?

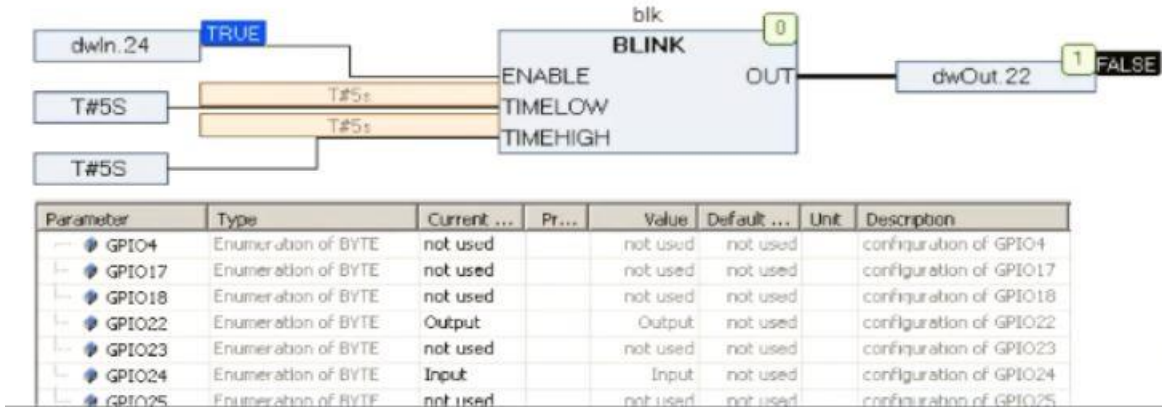
An Embedded system with Real Time Operating Systems like VxWorks and QNX running logic.



Control Logic

- It is programmed graphically most of the time
- Define what should/should not hapen
  - Under which conditions
  - At what time
  - Yes or No proposition

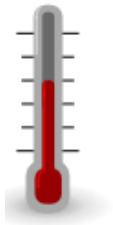
- IEC 61131-3
  - Ladder diagram (LD)
  - Function block diagram (FBD)
  - Structured text (ST)
  - Instruction list (IL)
  - Sequential function chart (SFC)



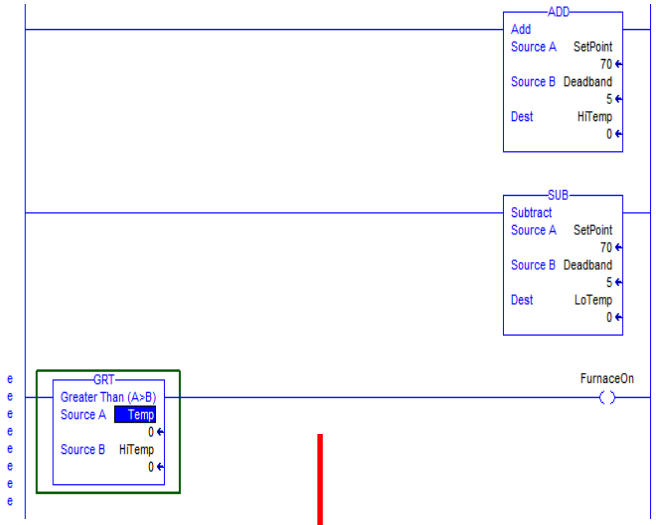
PLC Internals

1. Copy data from inputs to temporary storage
2. Run the logic
3. Copy from temporary storage to outputs

Sensors

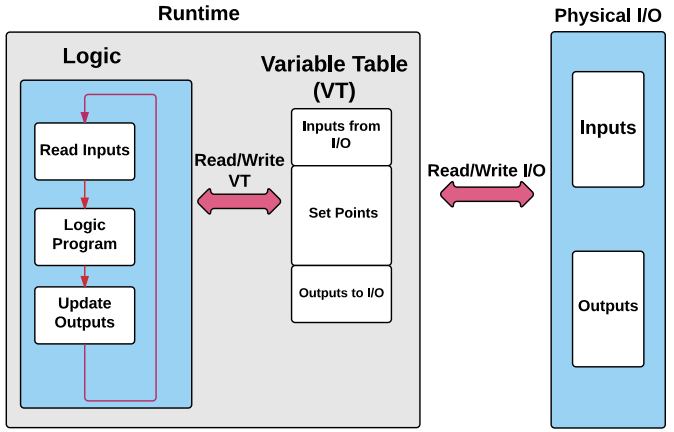


Inputs



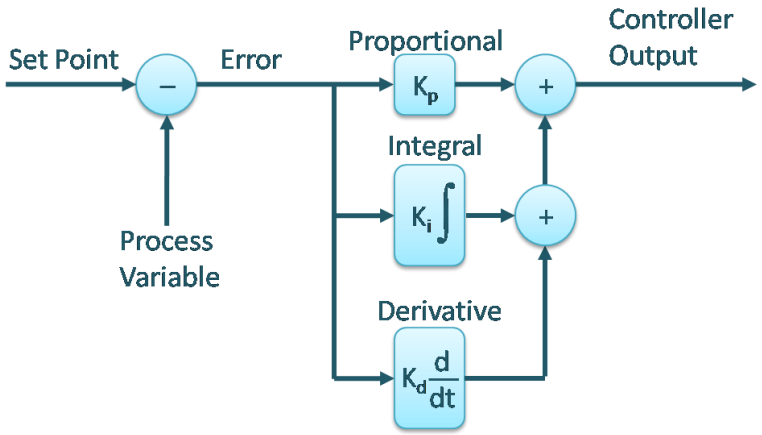
Outputs

Actuators

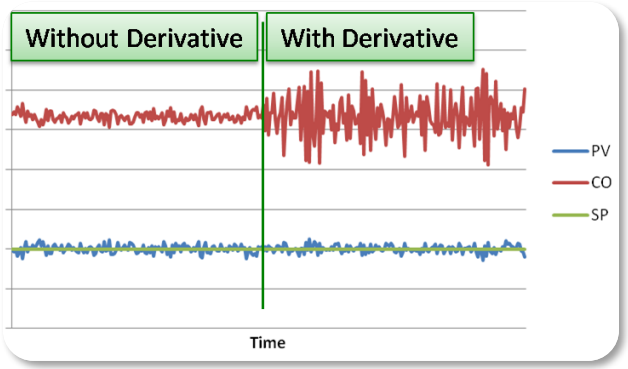


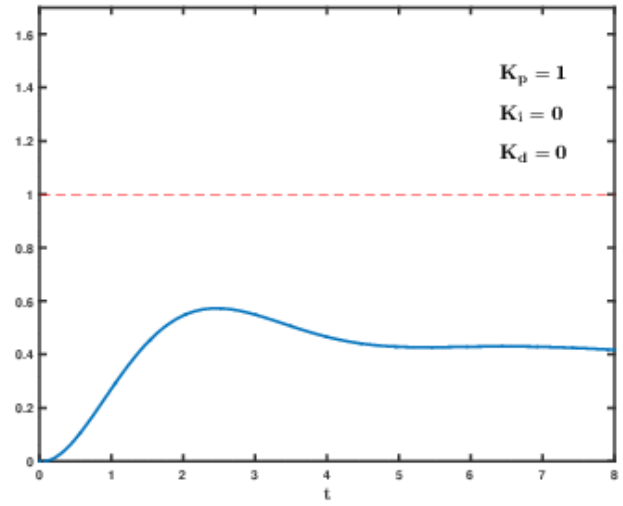
Control Algorithms

- **Used to compute output based on inputs received from control logic**
- **PID: proportional, integral, derivative –** most widely used control algorithm on the planet
- PI controllers are most often used



$$u(t) = K\left(e(t) + \frac{1}{T_i}\int_0^t e(\tau)d\tau + T_d\frac{de(t)}{dt}\right)$$





Why Control Loop is Important for Industry?

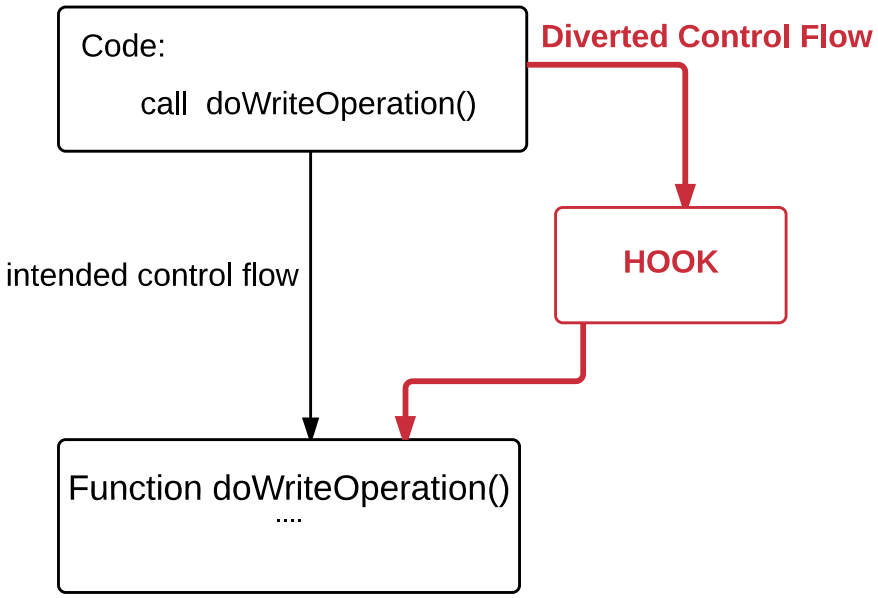
Existing Attacks and Defenses for Embedded Systems Applicable to the PLCs

Current Attacks against Embedded Systems:

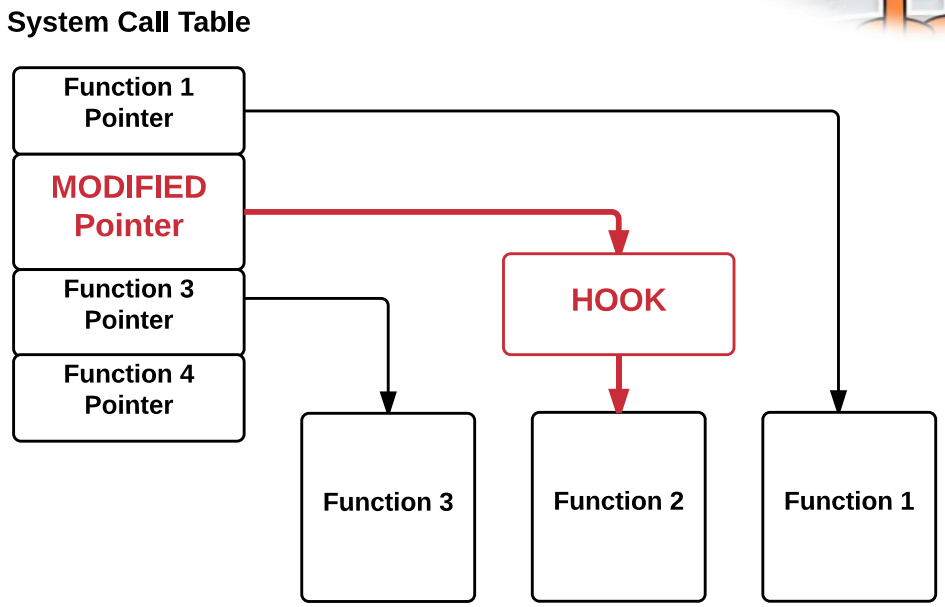
- Authentication bypass
  - Attacker find a backdoor password in the PLC.
- Firmware modification attacks
  - Attacker upload new firmware to the PLC
- Configuration manipulation attacks
  - Attacker modify the logic
- Control Flow attacks
  - Attacker find a buffer overflow or RCE in the PLC
- Hooking functions for ICS malwares

Function Hooking

Code Hook



Data Hook



Demo Function Hooking

Stuxnet – It wasn't a cyber toy.

Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant. Stuxnet final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes :

- Zero-day exploits
- Windows rootkit
- Antivirus Evasion Techniques
- Complex Process Injection and Hooking Code
- Network Infection Routines
- Peer-to-Peer Updates
- Command and Control Interface.

Current Defense for PLCs

- Attestation
  - memory attestation
- Firmware integrity verification
  - Verify the integrity of firmware before its being uploaded
- Hook detection
  - Code hooking detection
    - α Detect code hooking
  - Data hooking detection
    - μ Detect data hooking

System-level protection for PLCs

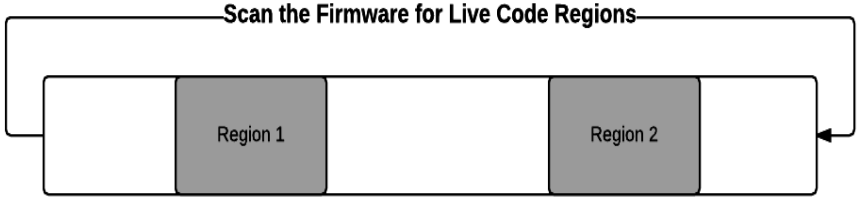
- Trivial Defenses:
  - Logic Checksum
  - Firmware integrity verification

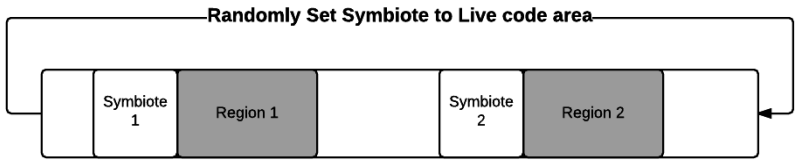
- Non-trivial software-based HIDS applicable to PLCs
  - **Doppelganger (Symbiote Defense):** an implementation for software symbiotes for embedded devices

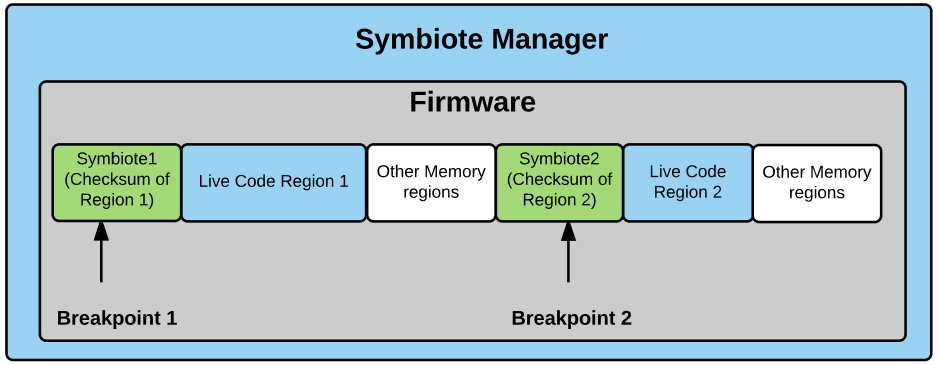
  - **Autoscopy JR:** A host based intrusion detection which is designed to detect kernel rootkits for embedded control systems

How Doppelganger Works

- Scan the firmware of the device for live code regions and insert symbiotes randomly.

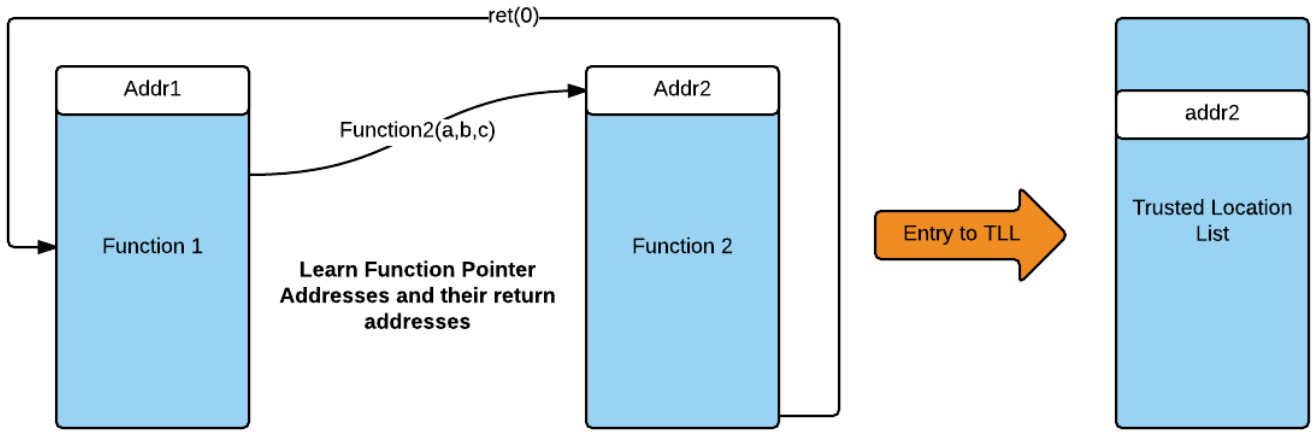






How Autoscopy Jr works

- Tries to Detects function hooking by learning
- Verifies the destination function address and returns with the values and addresses in TLL (Trusted Location List)

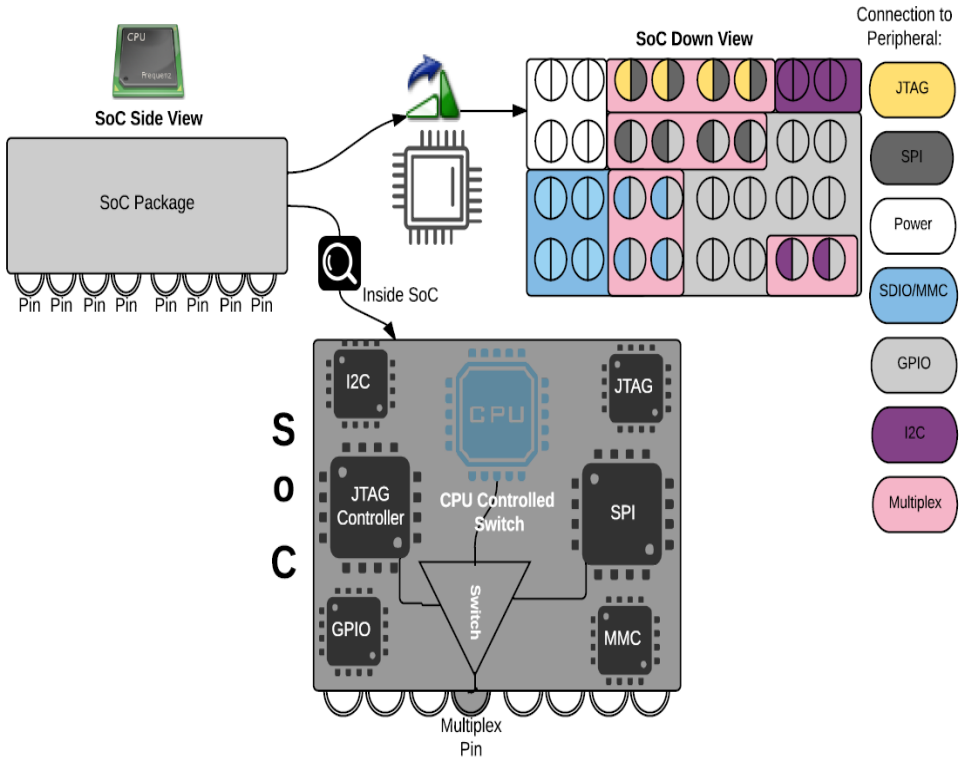


Some Background about Pin Control

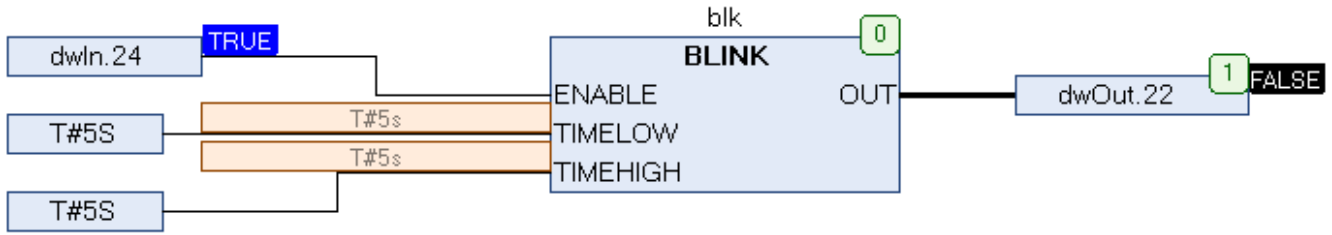
Pin Control Subsystem

Pin Multiplexing: Reusing the same pin for different purposes

Pin Configuration: Configuring electronic properties of pins

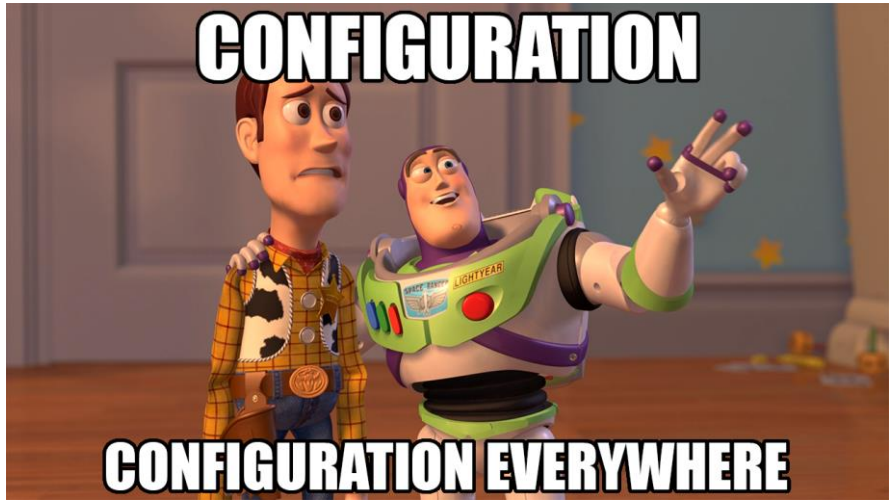


Pin Configuration

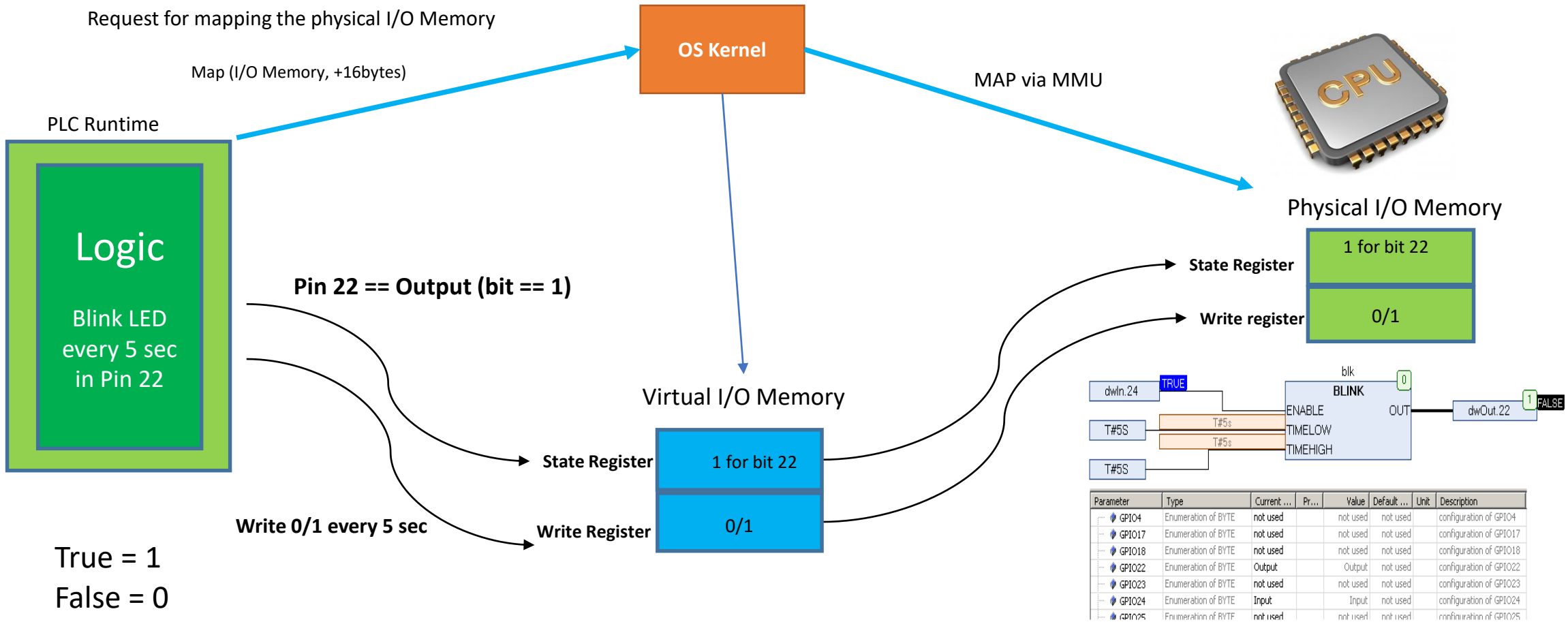


Parameter	Type	Current ...	Pr...	Value	Default ...	Unit	Description
GPIO4	Enumeration of BYTE	not used		not used	not used		configuration of GPIO4
GPIO17	Enumeration of BYTE	not used		not used	not used		configuration of GPIO17
GPIO18	Enumeration of BYTE	not used		not used	not used		configuration of GPIO18
GPIO22	Enumeration of BYTE	Output		Output	not used		configuration of GPIO22
GPIO23	Enumeration of BYTE	not used		not used	not used		configuration of GPIO23
GPIO24	Enumeration of BYTE	Input		Input	not used		configuration of GPIO24
GPIO25	Enumeration of BYTE	not used		not used	not used		configuration of GPIO25

- Input Pin
  - **readable** but not writeable
- Output Pin
  - **readable** and writeable



Introducing Pin Control Attack: A Memory Illusion



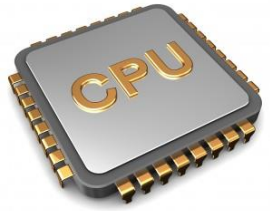
Introducing Pin Control Attack: A Memory Illusion

Request for mapping the physical I/O Memory

Map (I/O Memory, +16bytes)

OS Kernel

MAP via MMU



Physical I/O Memory

PLC Runtime

Logic

Blink LED every 5 sec in Pin 22

Pin 22 == Input (bit == 0)

Virtual I/O Memory

State Register

1 for bit 22

Write register

0/1

Write 0/1 every 5 sec

State Register

1 for bit 22

Write Register

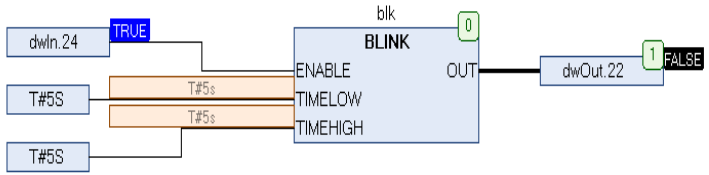
0/1

Write Failure!!

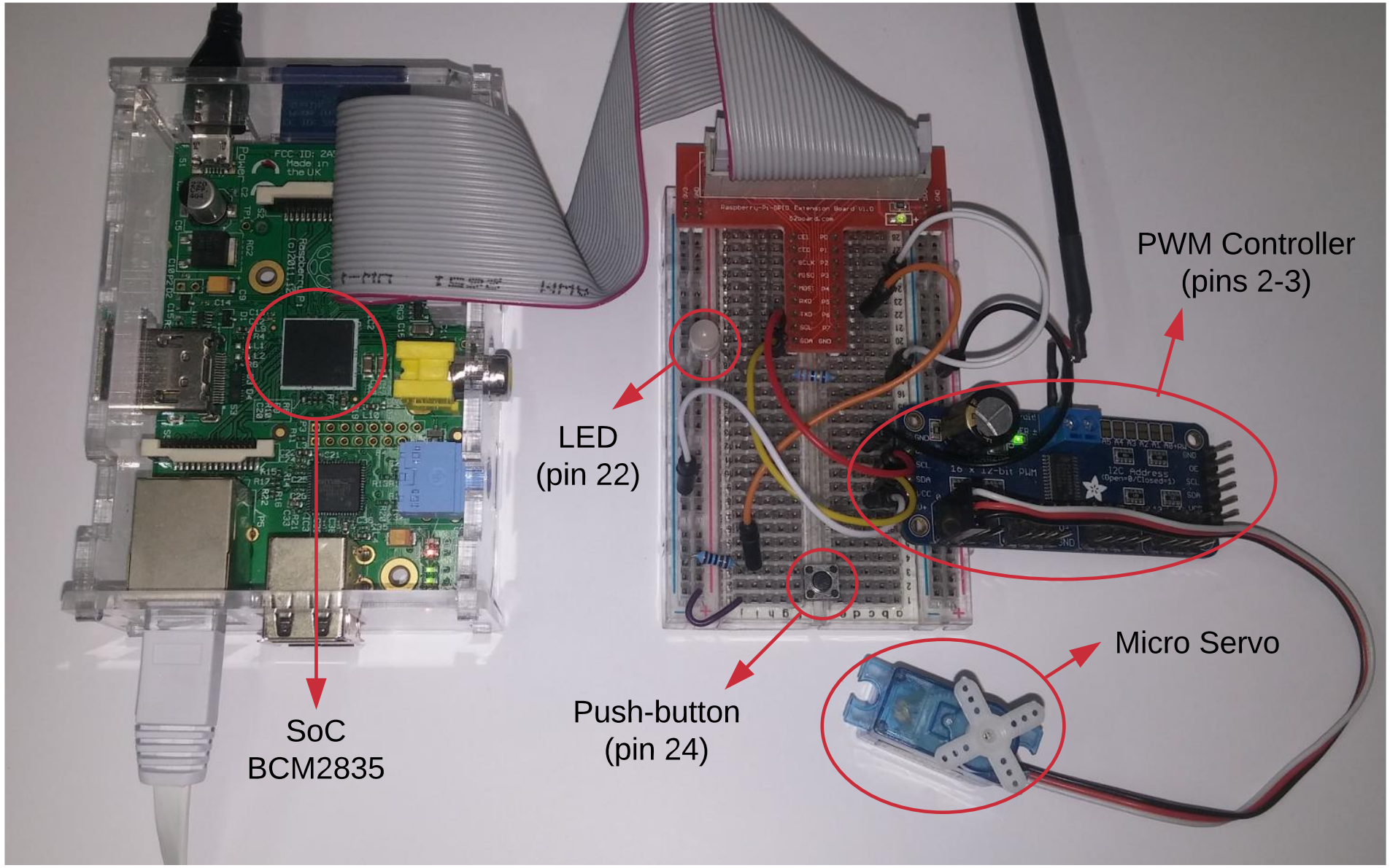
Pin is in Input Mode

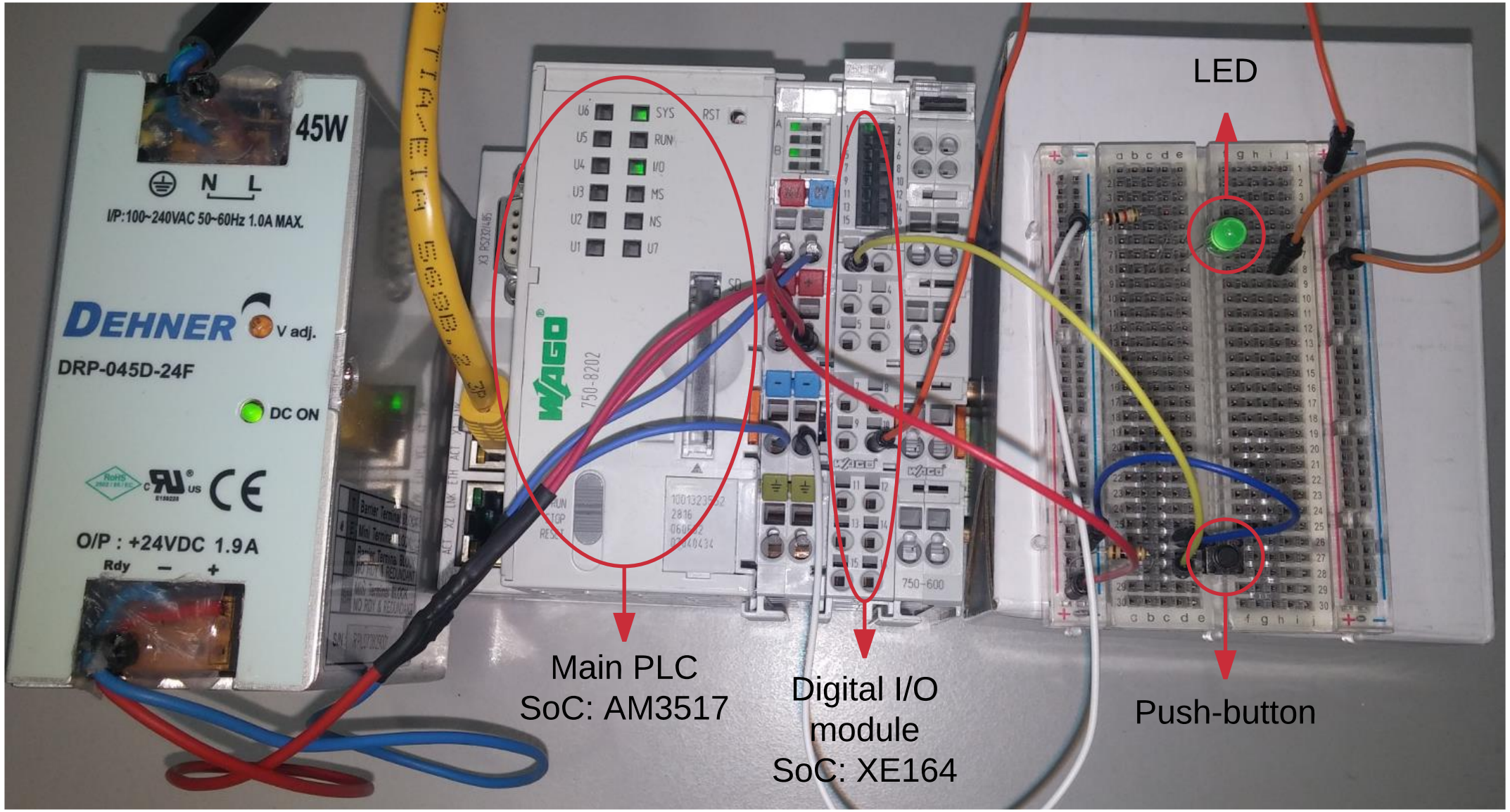
True = 1

False = 0



Parameter	Type	Current ...	Pr...	Value	Default ...	Unit	Description
GPIO4	Enumeration of BYTE	not used		not used	not used		configuration of GPIO4
GPIO17	Enumeration of BYTE	not used		not used	not used		configuration of GPIO17
GPIO18	Enumeration of BYTE	not used		not used	not used		configuration of GPIO18
GPIO22	Enumeration of BYTE	Output		Output	not used		configuration of GPIO22
GPIO23	Enumeration of BYTE	not used		not used	not used		configuration of GPIO23
GPIO24	Enumeration of BYTE	Input		Input	not used		configuration of GPIO24
GPIO25	Enumeration of BYTE	not used		not used	not used		configuration of GPIO25


PWM Controller
(pins 2-3)
LED
(pin 22)
SoC
BCM2835
Push-button
(pin 24)
Micro Servo


LED
Main PLC
SoC: AM3517
Digital I/O
module
SoC: XE164
Push-button
45W
I/P:100~240VAC 50~60Hz 1.0A MAX.
DEHNER
V adj.
DRP-045D-24F
DC ON
O/P : +24VDC 1.9A
Rdy
WAGO
750-8202
750-600
SYS
RUN
I/O
MS
NS
RST

Demo

Everything that has a beginning has an end.

— The Matrix Revolution