11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Stealth Low-Level Manipulation of Programmable Logic Controllers I/O by Pin Control Exploitation

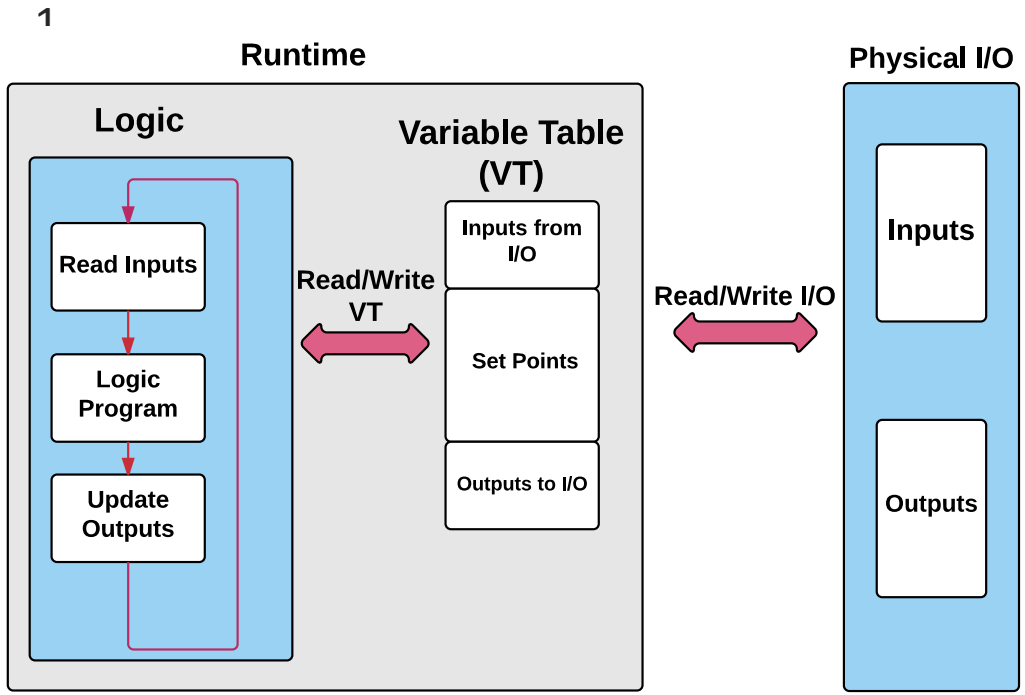
Ali Abbasi[a], Majid Hashemi[b], Emmanuele Zambon[a,c], and Sandro Etalle[a, d]

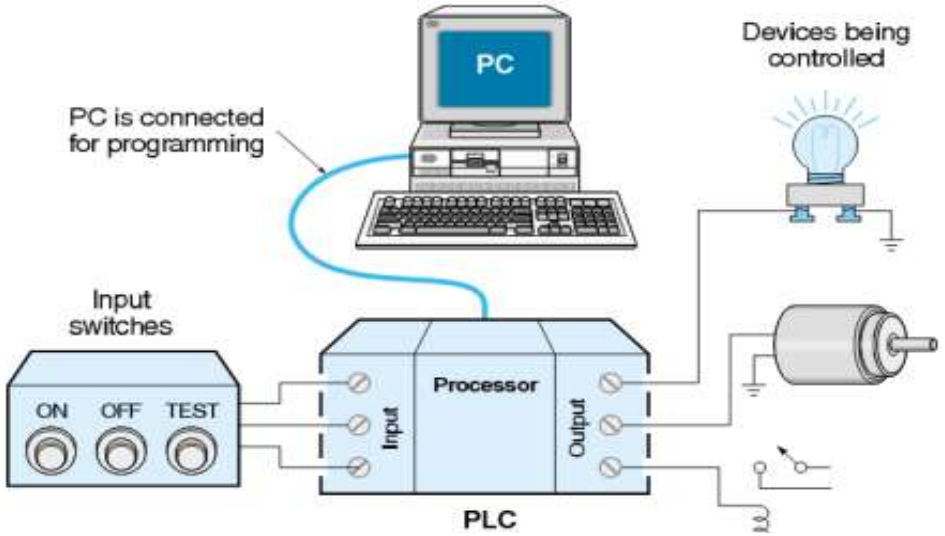
[a] *University of Twente, Services, Cyber Security and Safety Group*
[b] *Quarkslab*
[c] *SecurityMatters B.V.*
[d] *Eindhoven University of Technology*

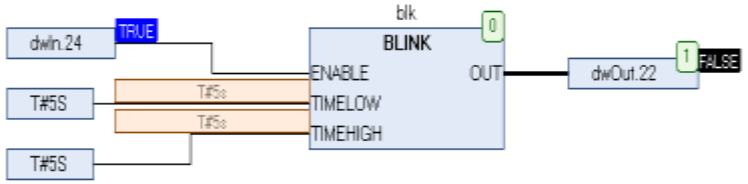
UNIVERSITY OF TWENTE.

PREEMPTIVE

Programmable Logic Controller







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

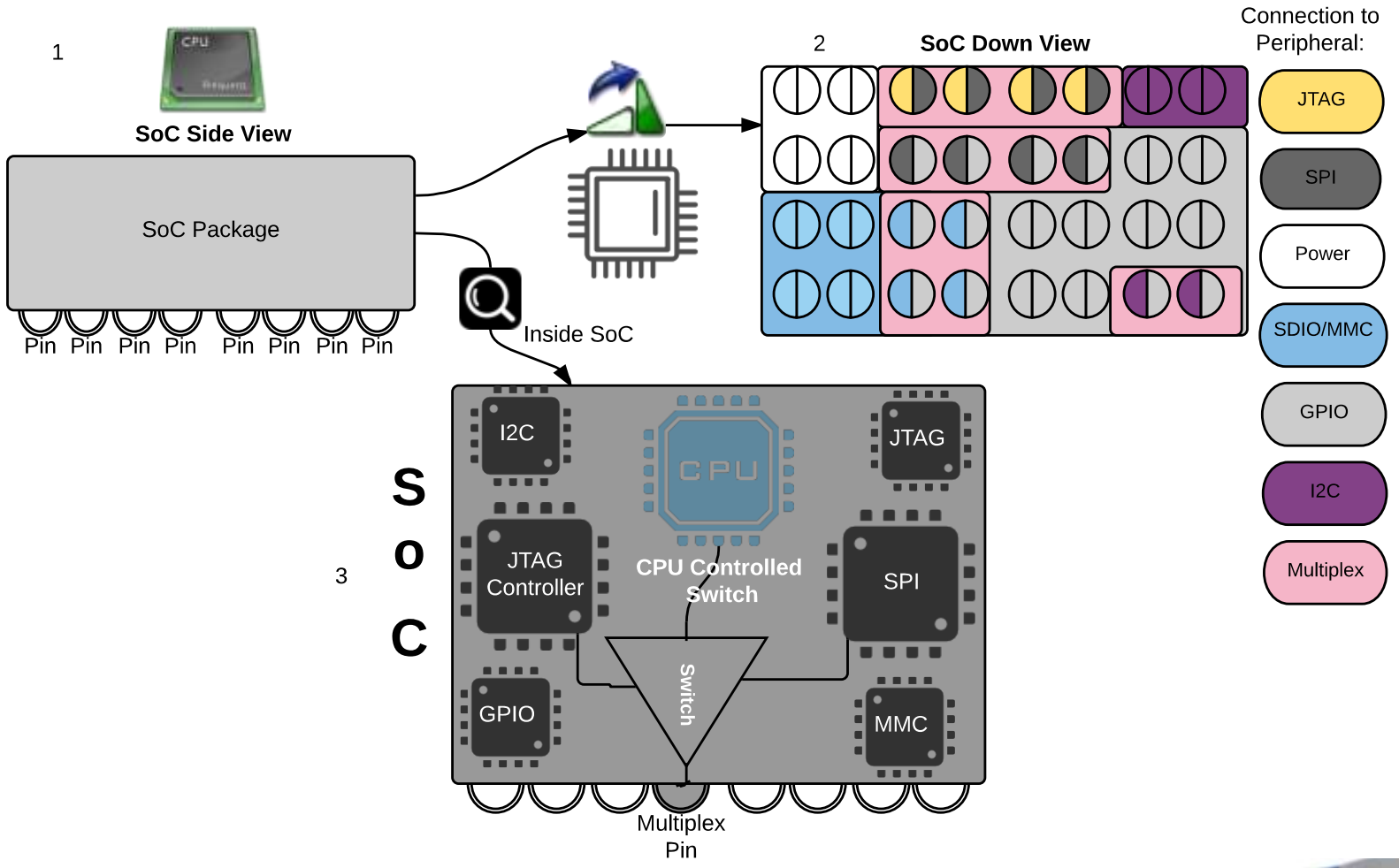
Background on Attacks and Defenses in PLCs

- Attacks:
  - Firmware modification attacks
  - Configuration manipulation attacks
  - Control Flow attacks
  - Authentication bypass
- Defenses:
  - Attestation
  - Control flow integrity
  - Firmware integrity verification
  - Logic checksum

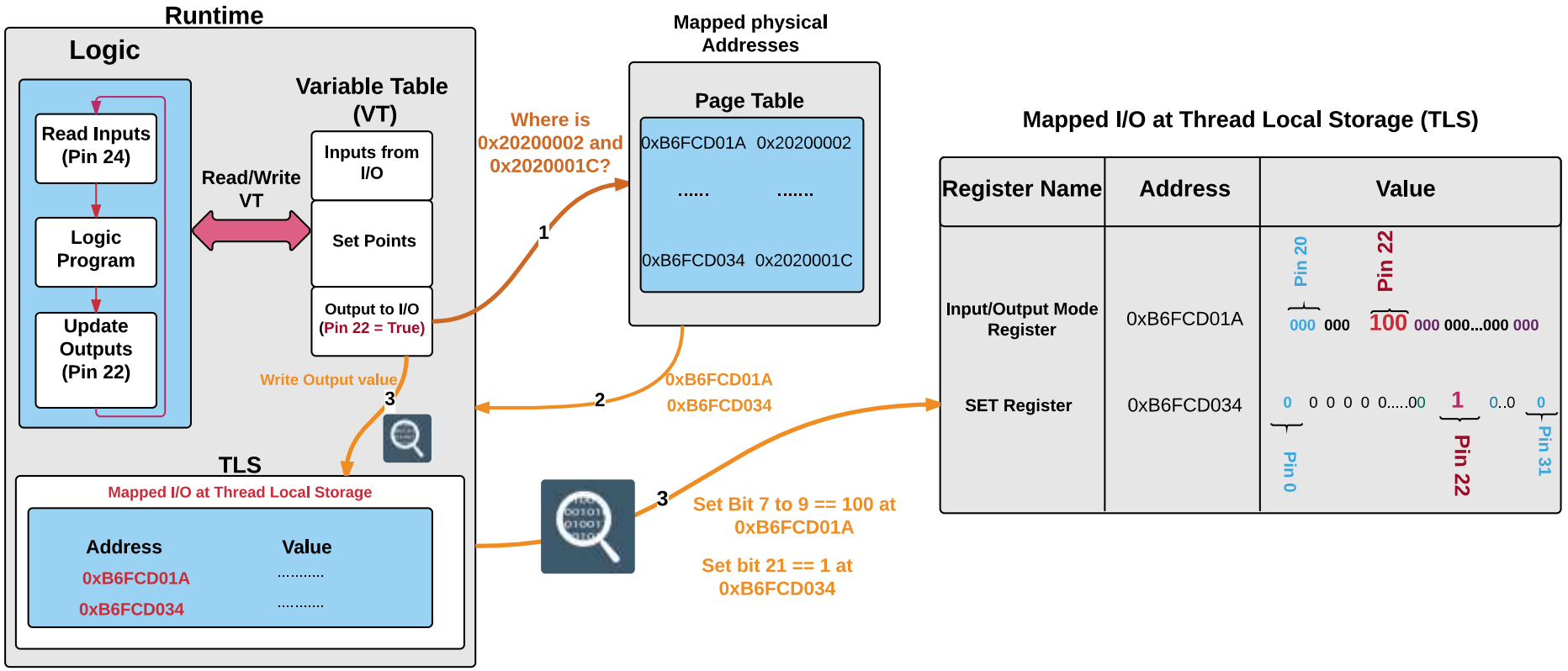
Background on Pin Control

Pin Control Subsystem

- Pin Configuration
- Pin Multiplexing



How PLC Control the I/O



Security concerns regarding Pin Control

CRITIS 2016

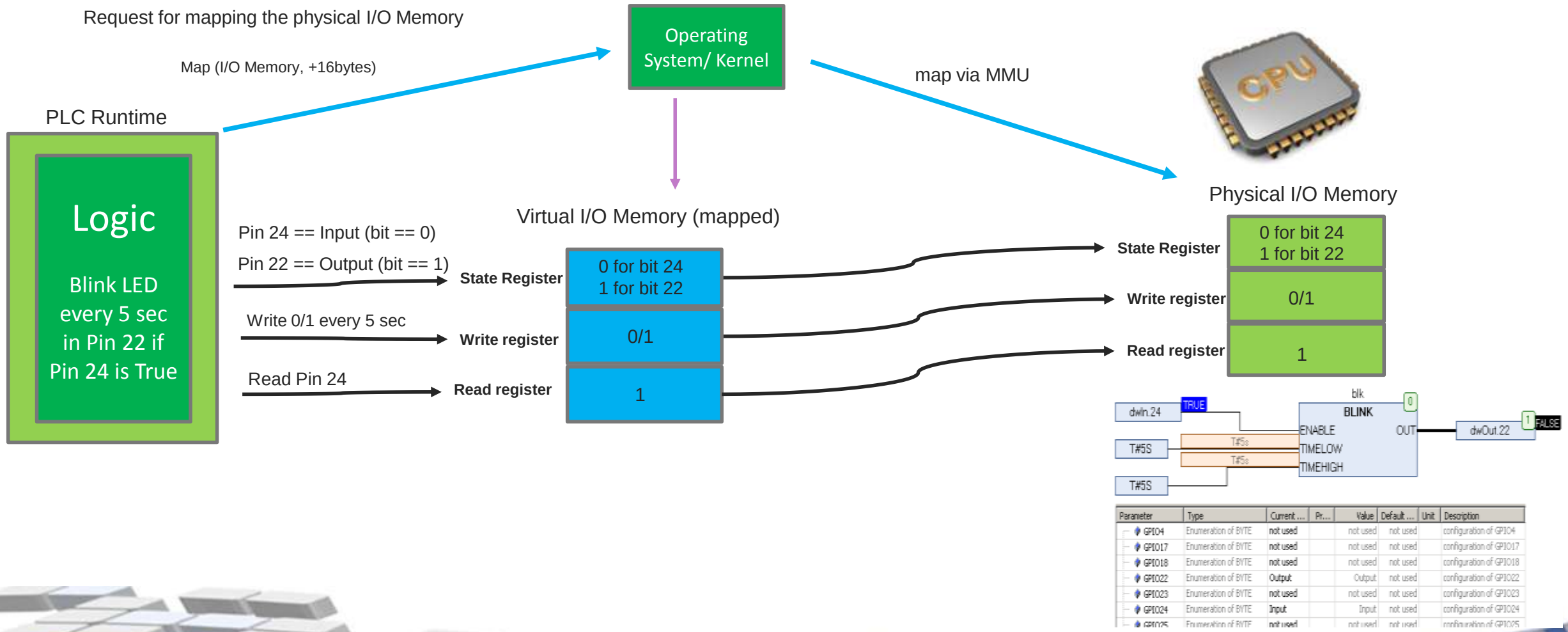
No Interrupt for Pin Configuration

- How the OS knows about the modification of pin configuration?
- What if somebody modify configuration of Pin at runtime?

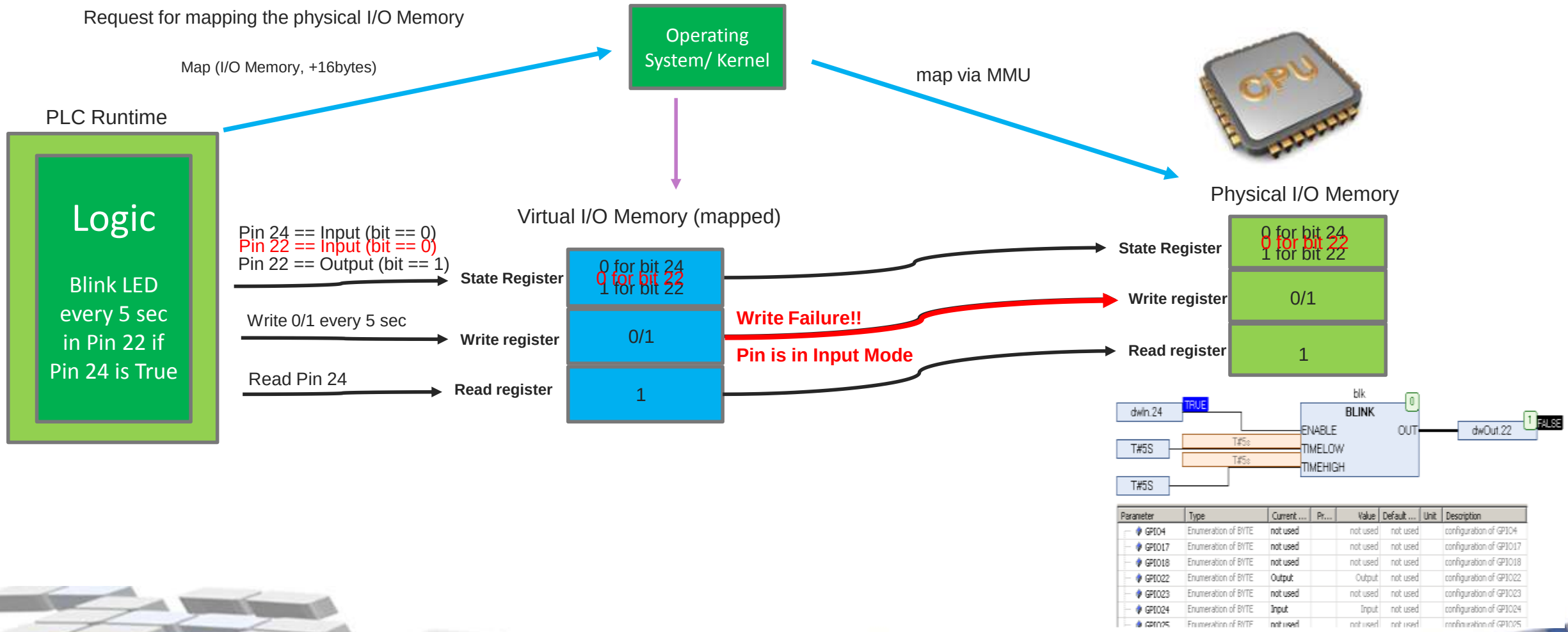
No Interrupt for Pin Multiplexing

- How OS knows about the of pin multiplexing?
- What if somebody multiplex a Pin at runtime?

Security Concerns

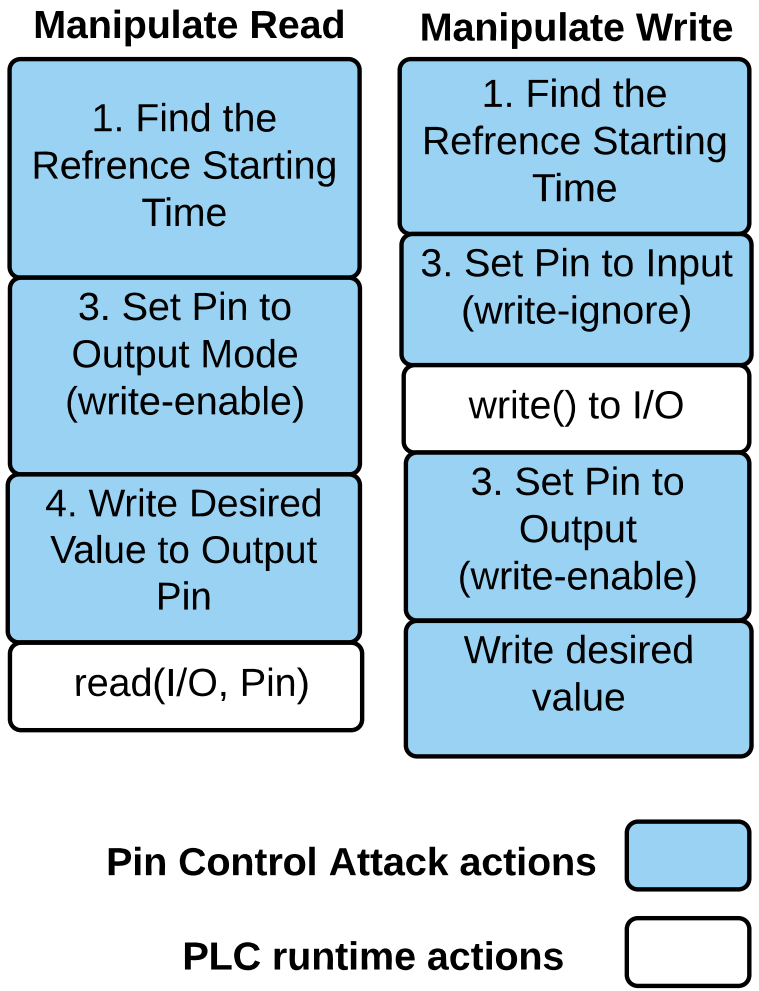


Security Concerns



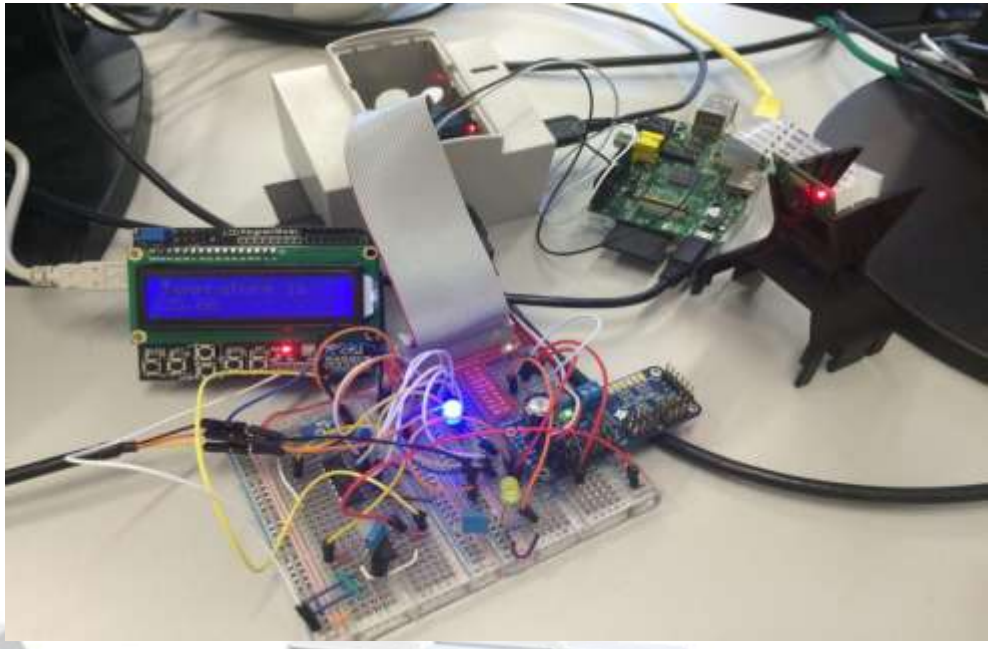
Pin Control Attack

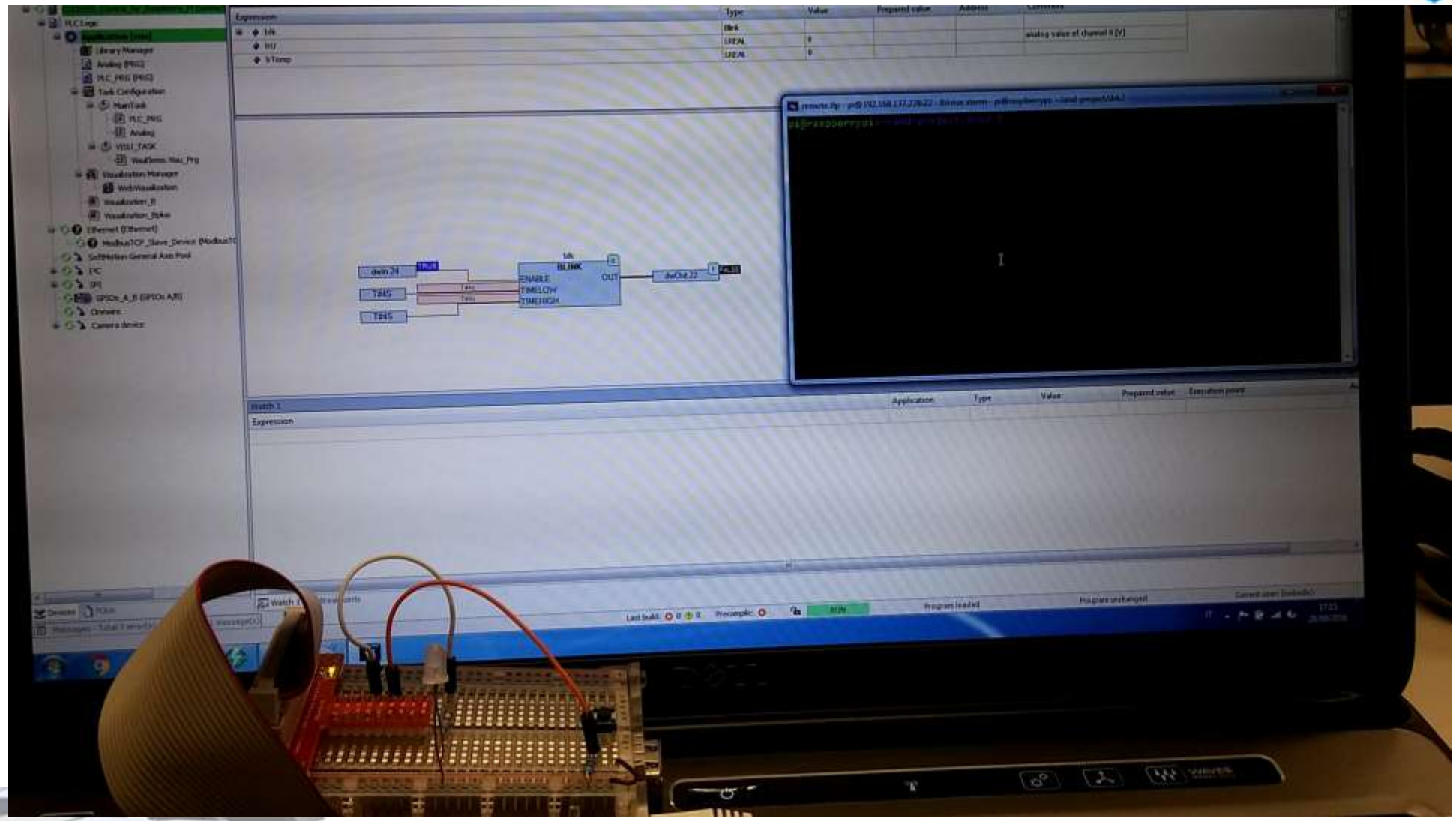
- We can disable write to the PLC I/O outputs
  - Virtual memory have different value since CPU will ignore write operations.
- We can enable write to the PLC input I/O as well.
- Pin Control Attack: manipulate the I/O configuration of the PLC
  - PLC OS never knows about it.



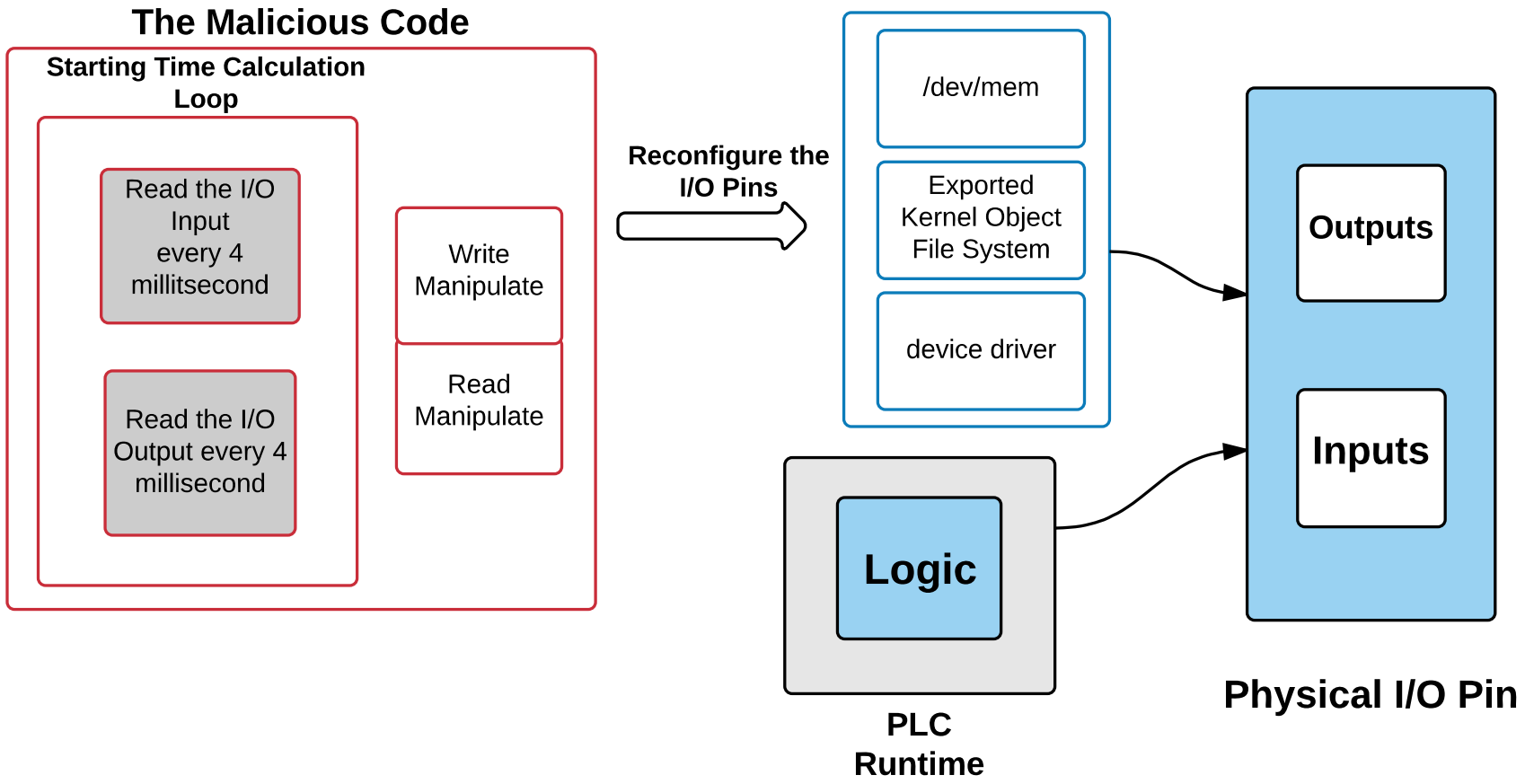
Threat Model & Attack Implementation

- PLC runtime privilege
- Knowledge of the physical process
- Knowledge of mapping between I/O pins and the logic



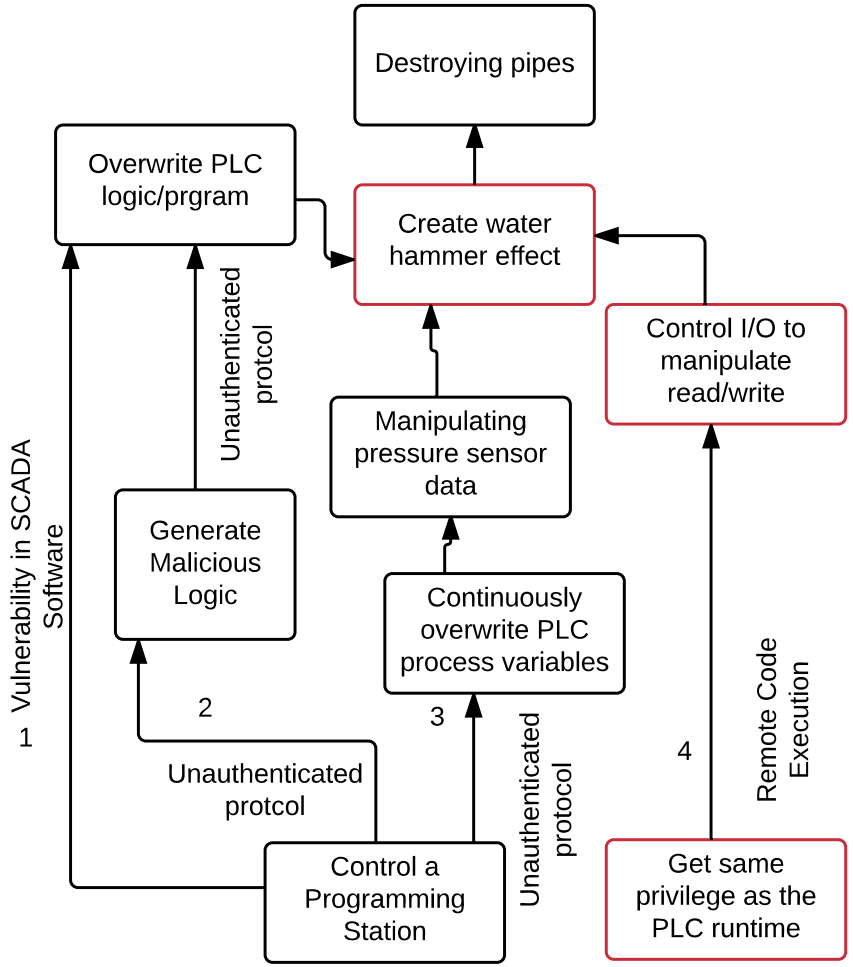

BLINK
ENABLE
OUT
TIMELOW
TIMEHIGH
T#45
T#45

Practical Implementation of the Attack



Implication of the attack on the ICS

- Taxonomy of Utilities
  - Water Utilities
- What can happen?:
  - Attacker can change the I/O
  - PLC is unaware of it.
  - Even if we deploy some kind of detection mechanisms



Implication of Attack in the ICS

- For now attacker can:
  - Simply change the logic
  - Modify PLC Runtime executable
- Fixing this attacks are trivial:
  - Proper Authentication
  - Proper Logic Checksum
  - PLC Runtime integrity verification
- Next Step for attackers:
  - Achieve its goal without actually modifying the Logic or Runtime or hooking functions

Conclusions

- Need to focus on system level security of control devices In future more sophisticated techniques come that evade defenses.
  - Pin Control attack is an example of such attacks.
- Pin Control Attack:
  - lack of interrupt for I/O configuration registers
  - Significant consequences on protected PLCs and other control devices such as IEDs.
- Solution:
- It is hard to handle I/O interrupts with existing real-time constraints.
- Monitoring I/O Configuration Pins for anomalies.
- User/Kernel space separation for I/O memory.

Questions?

Looking for more technical detail?

Attend our talk at Black Hat EU 2016, London, UK.
or
SCADA Security Scientific Symposium (S4x17) at Miami, USA.
Or
ZeroNights 2016, Moscow, Russia.

Contact:
a.abbasi@utwente.nl