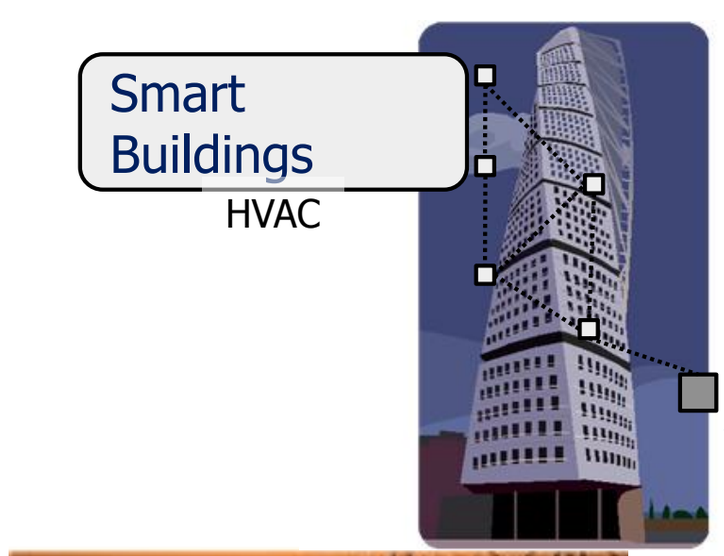
Cyber-Physical Systems Security

Alvaro A. Cárdenas
Department of Computer Science
University of Texas at Dallas

Modernization of our Physical Infrastructures

Physical Systems are Being Modernized with New Technologies



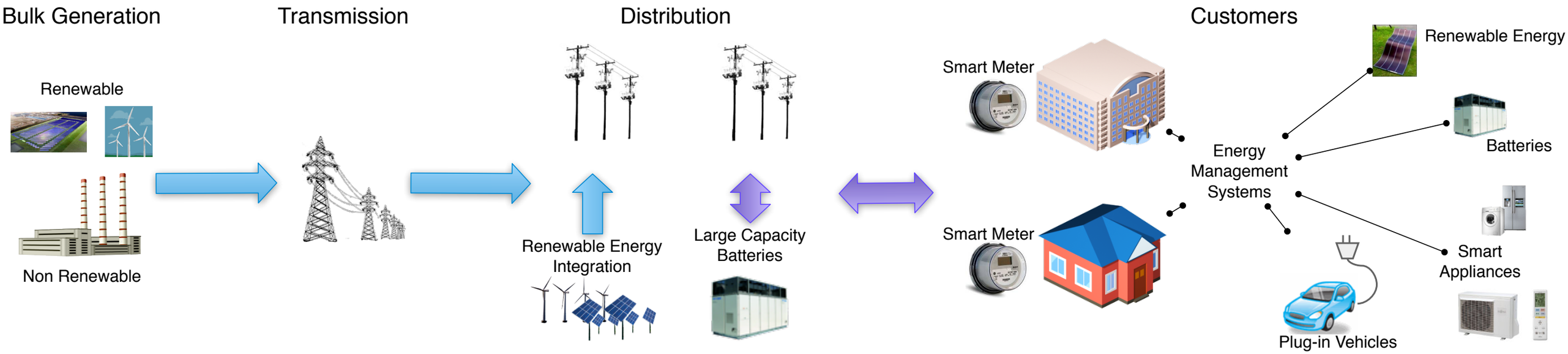
Smart Infrastructures

Intelligent Transportation Systems

Operations Center.

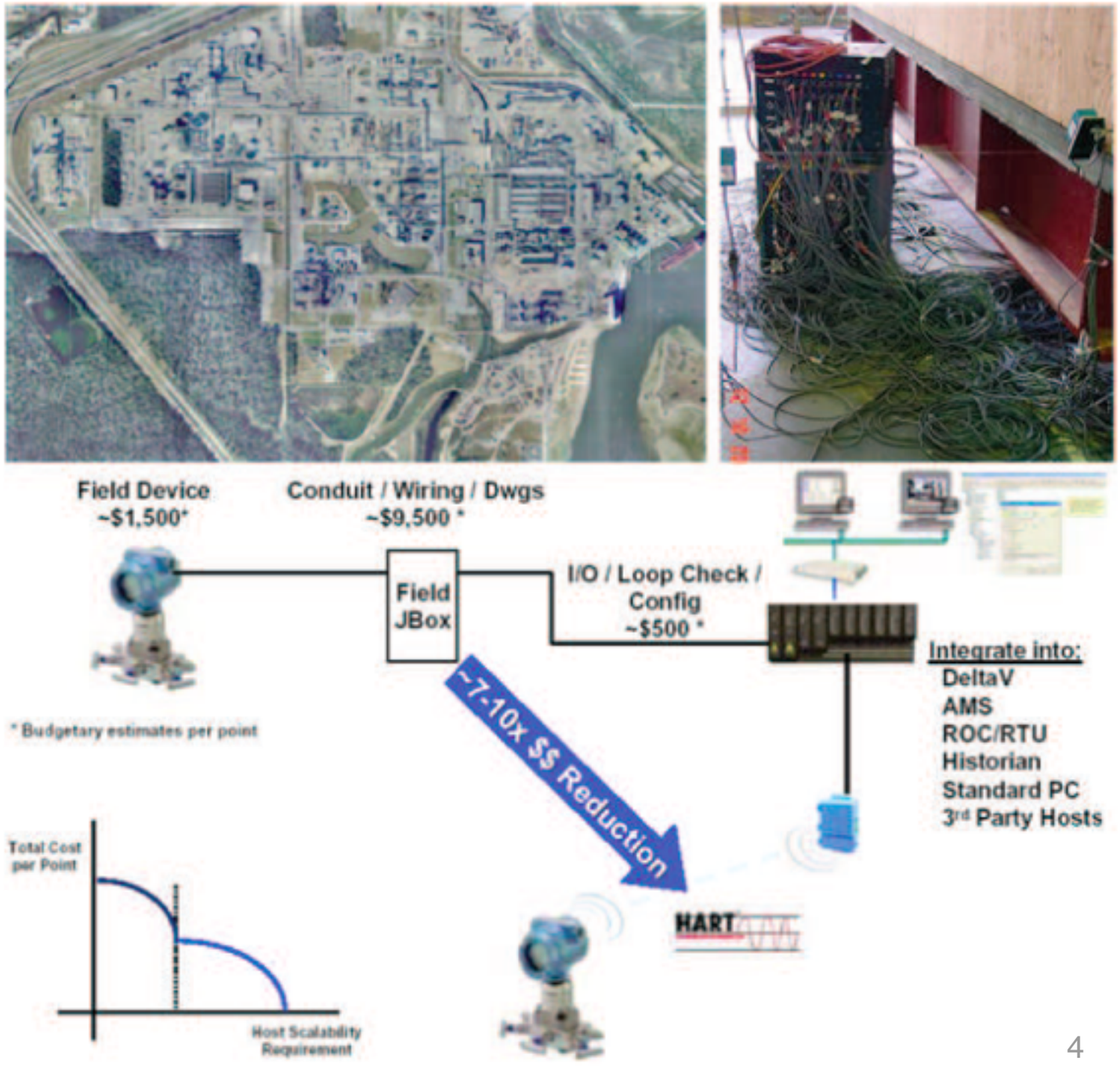
Standards: Wireless HART (IEC), ISA SP 100.11a, IETF 6LoWPAN, ROLL, CoRE, Eman, LWIP, IRTF IoT, W3C EIX, IEEE 802.15.4 (g), 802.15.5, etc.

Typical Example: Smart Grid



First Success Story of Sensor Networks

- SCADA systems:
  - Improve monitoring
  - Situational awareness
- Cost-effective solution



Devices are becoming smarter,

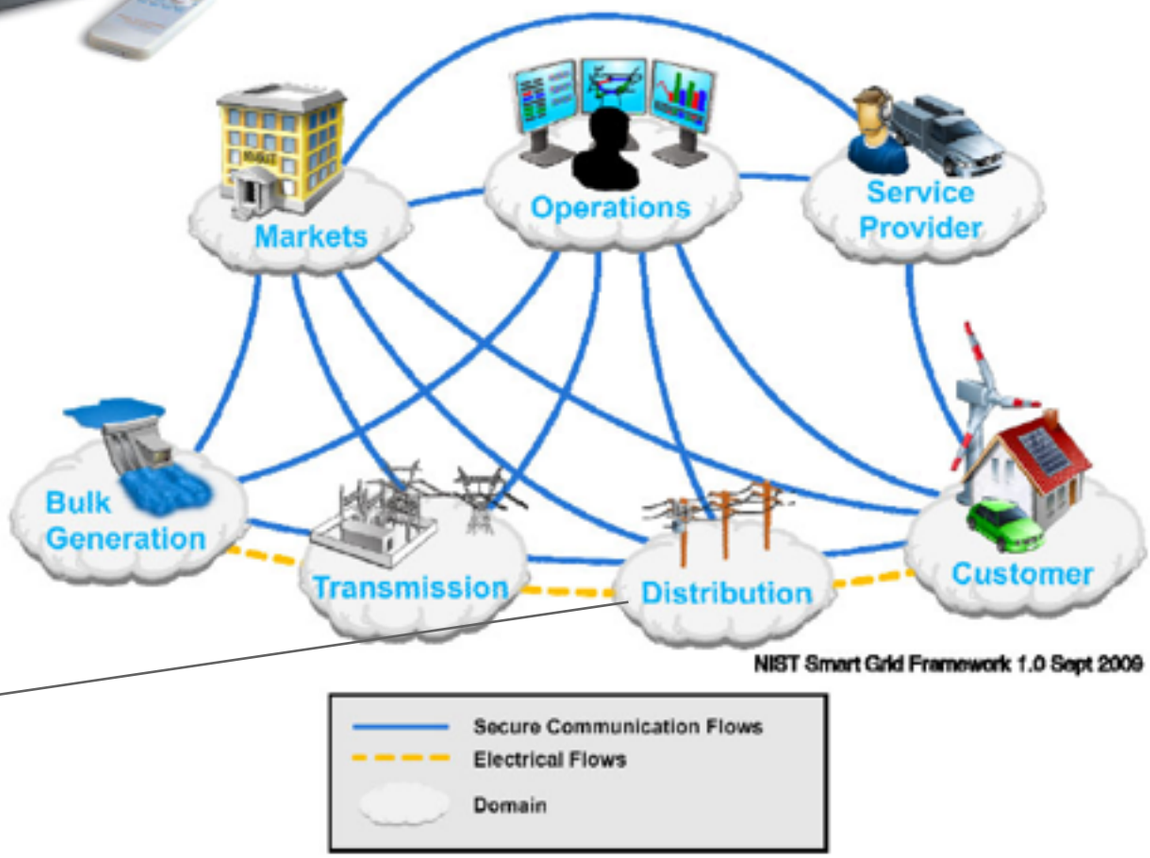


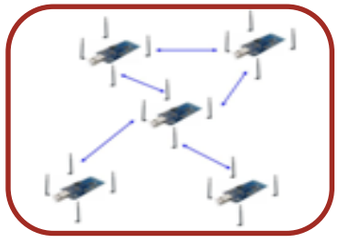
Figure 2. Smart Grid Domains

Cyber-Physical Systems

- By embedding instrumentation in buildings, vehicles, factories, power grid, we are creating Cyber-Physical Systems (CPS):
  - Smart sensing + actuation
  - CPS systems are IT systems that interact with the physical world

Physical System

Actuators
RTUs



Sensors

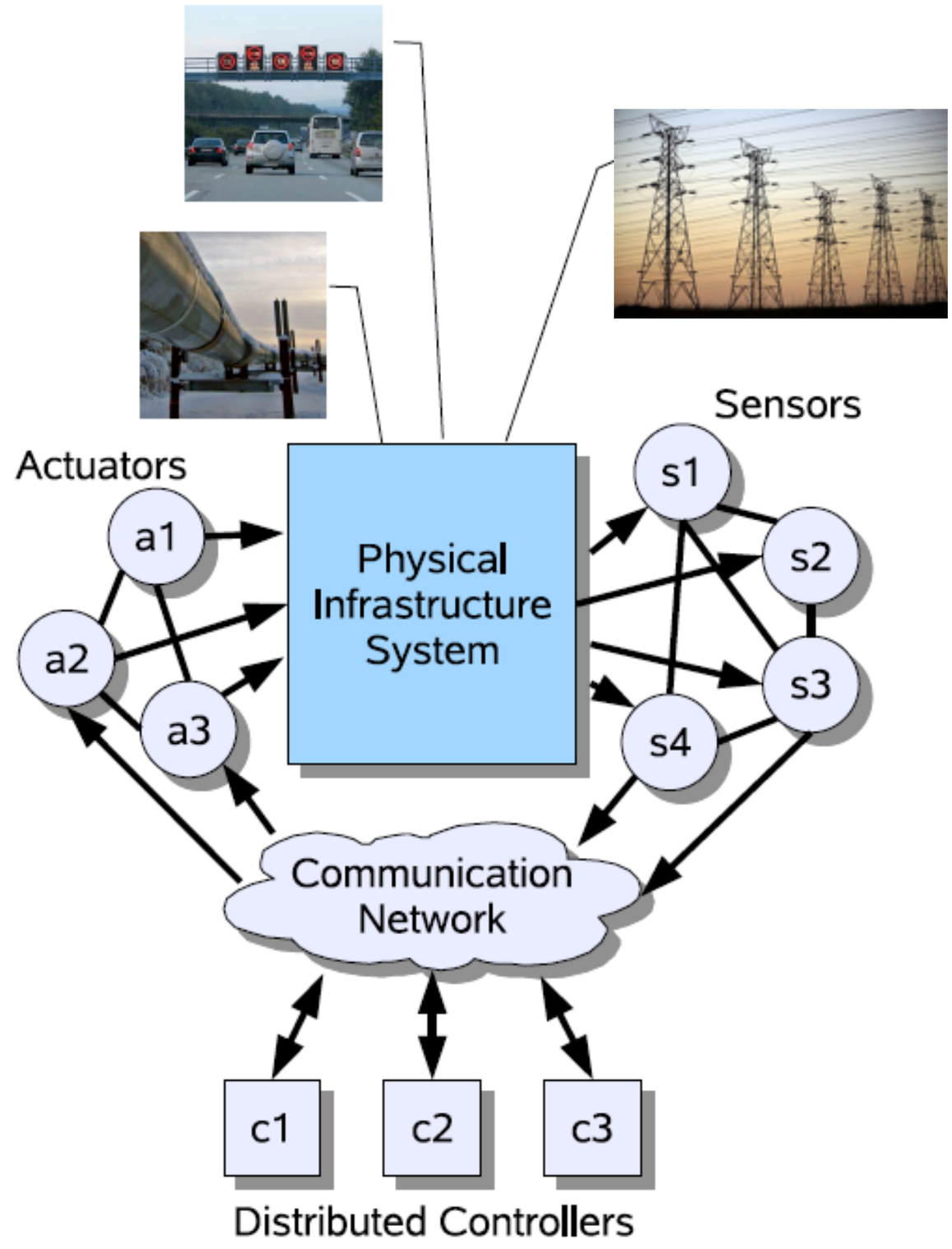
Control

Data Processing
State Estimation

Cyber-physical systems

- Control
- Computation
- Communication

- Interdisciplinary Research!



Why is Security Important Now? New Vulnerabilities & Threats

- Controllers are computers (from Relays to MCUs)
  - Can be programmed to do anything!
- Networked
  - Sensors and actuators can be accessed remotely
- Commodity IT solutions
  - Well known generic vulnerabilities are widely available
  - Some technologies are even insecure by design!
- New functionalities
  - New vulnerabilities (e.g. privacy problems with fine-grained monitoring)
- More devices (IoT)
  - Easier to find a vulnerable device
- Highly skilled IT global workforce
  - Creating exploits (and using them) is now easier than ever!

Vulnerabilities can be Exploited

2000 Maroochy Shire sewage control system.

2011 HVAC

2012 Smart Meters

Cyberattack on German steel factory causes 'massive damage'

By Loek Essers

IDG News Service | December 19, 2014

MORE GOOD READS

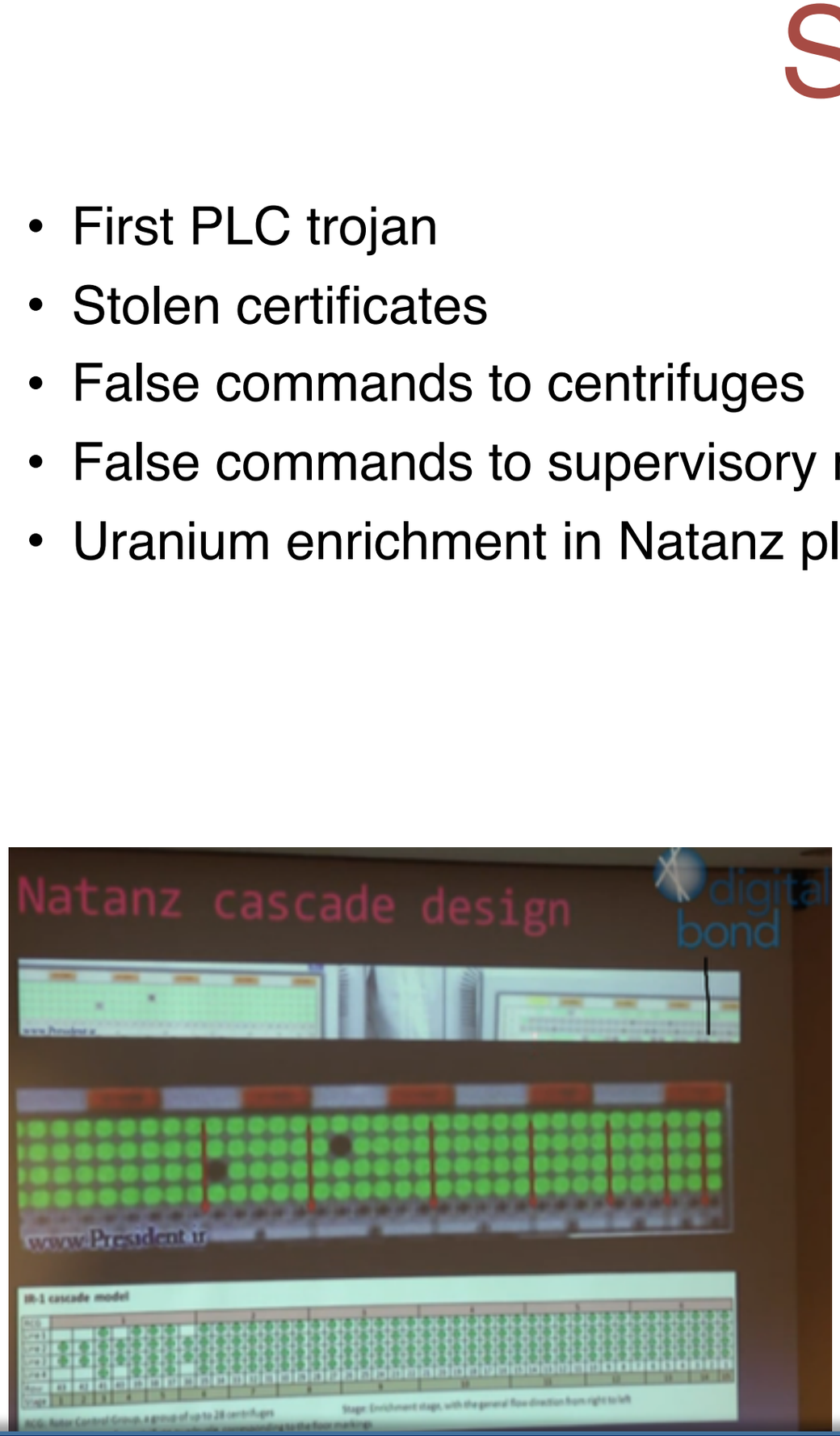
First Stuxnet victims were five Iran

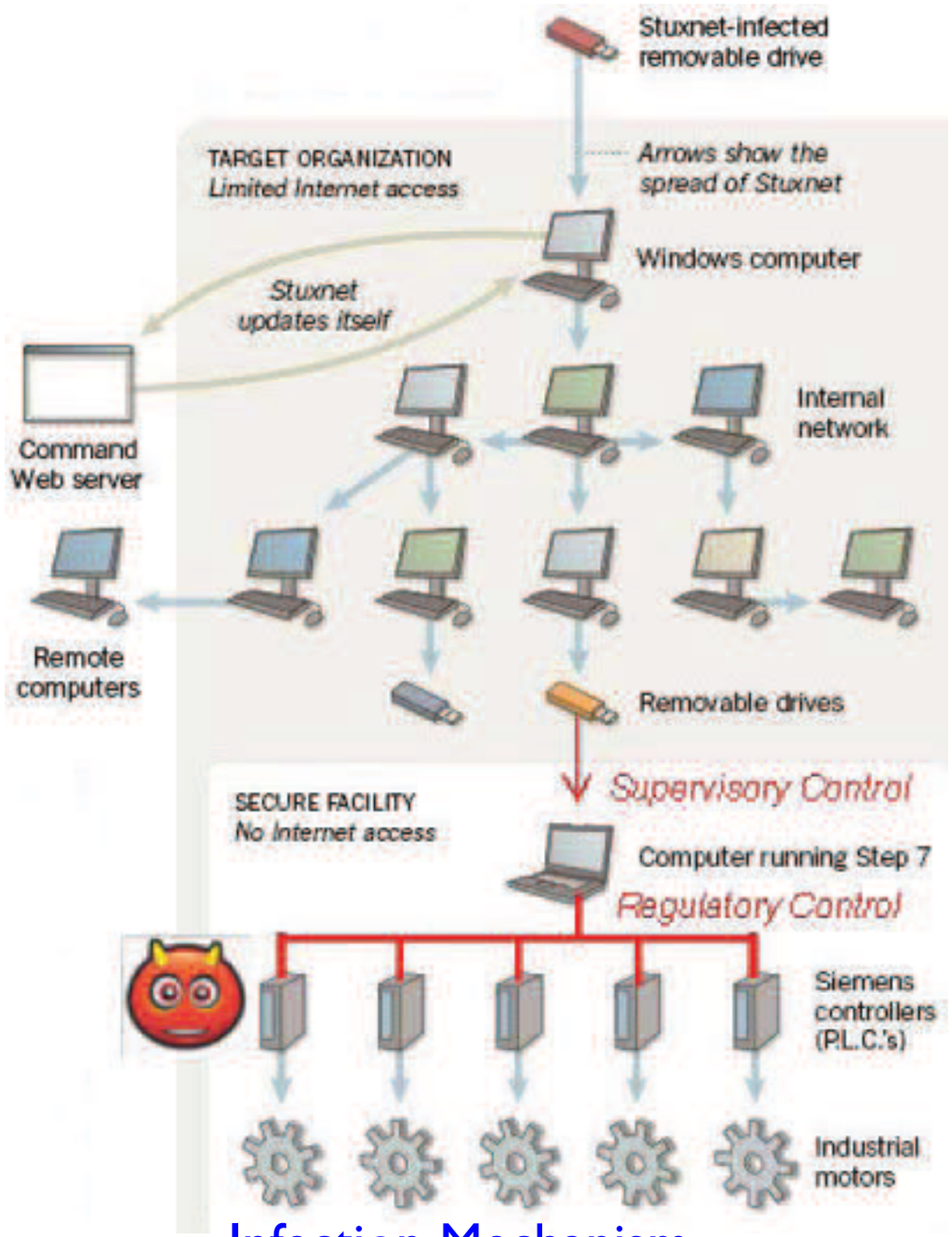
A German steel factory suffered massive damage after hackers managed to access production networks, allowing them to tamper with the controls of a blast furnace, the government said in its annual IT security report.

Due to these failures, one of the plant's blast furnaces could not be shut down in a controlled manner, which resulted in "massive damage to plant," the BSI said, describing the technical skills of the attacker as "very advanced."

Stuxnet

- First PLC trojan
- Stolen certificates
- False commands to centrifuges
- False commands to supervisory network
- Uranium enrichment in Natanz plant in Iran



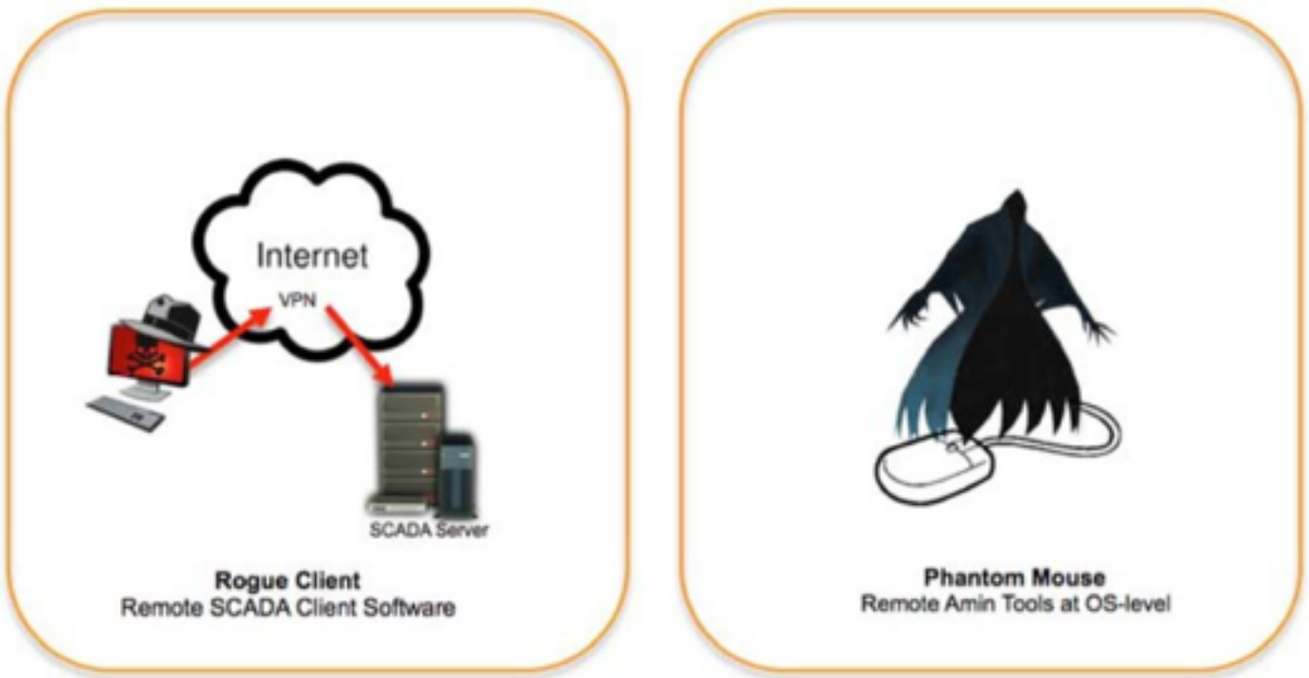


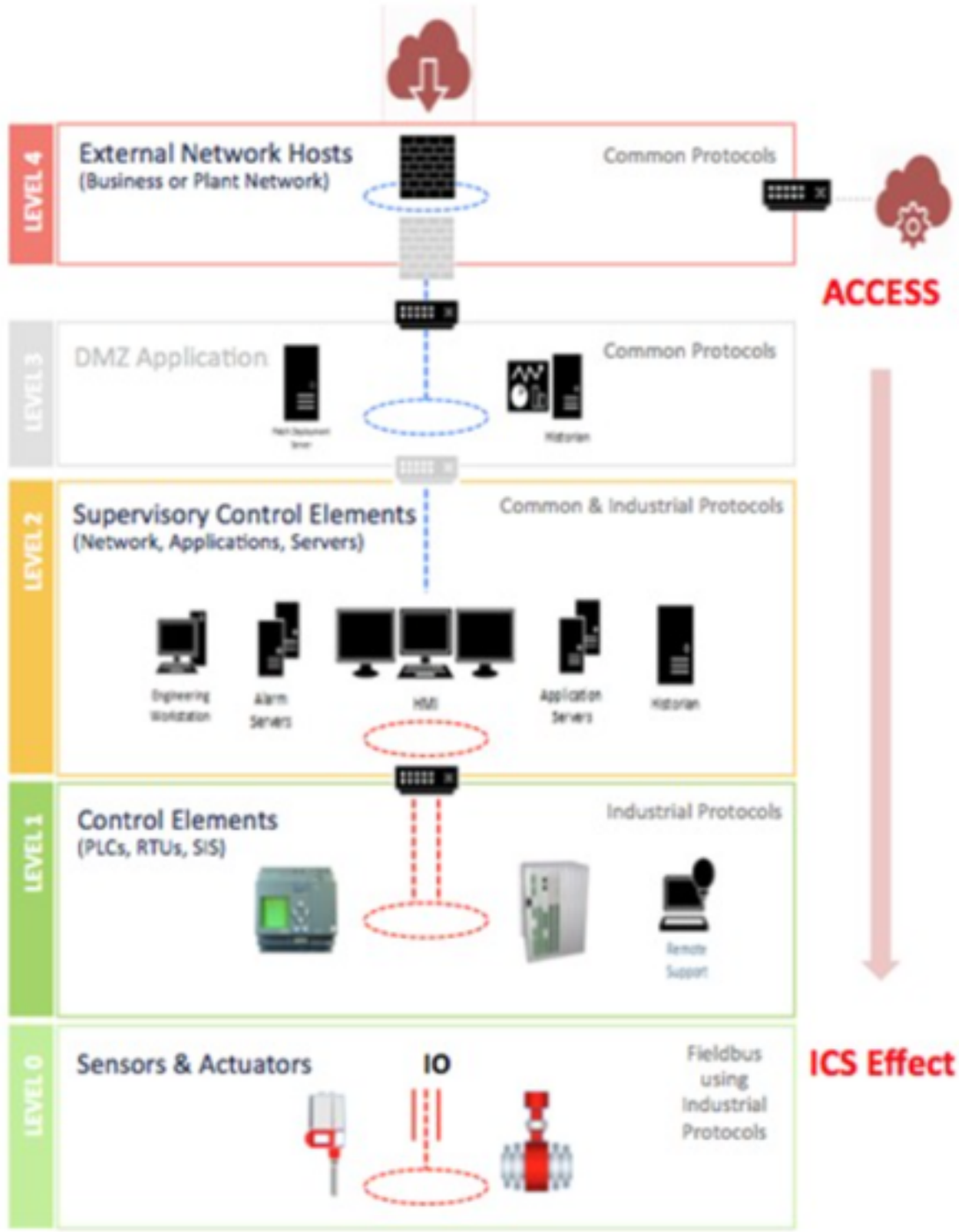
Infection Mechanism

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

SCADA Hijacking Techniques





The attackers develop two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

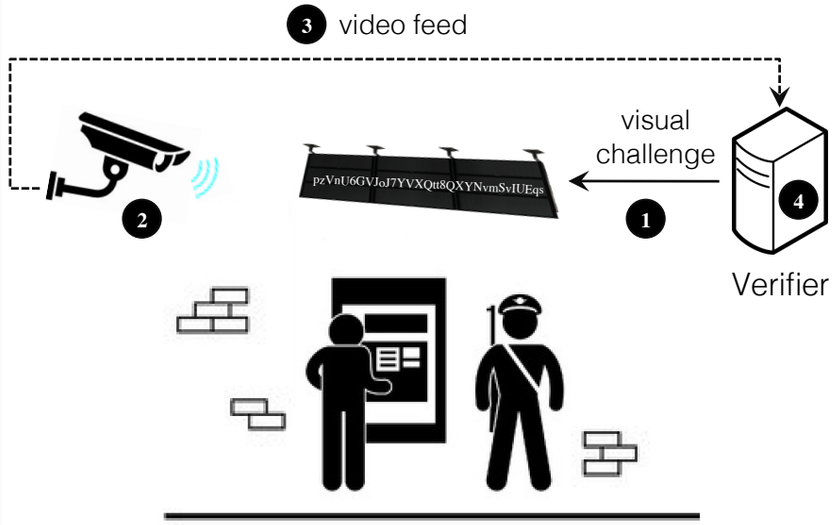
Intrusion Detection for IoT

My Research:
Intrusion Detection Systems (IDS) in IoT by monitoring the "physics" of cyber-physical systems

Sponsors:

NIST MITRE NSF intel

Example 1: Visual Challenges verify that video feed hasn't been modified

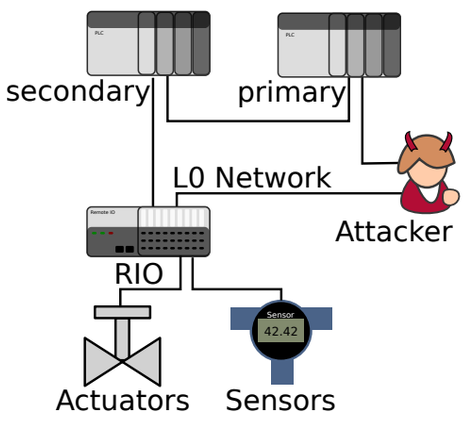


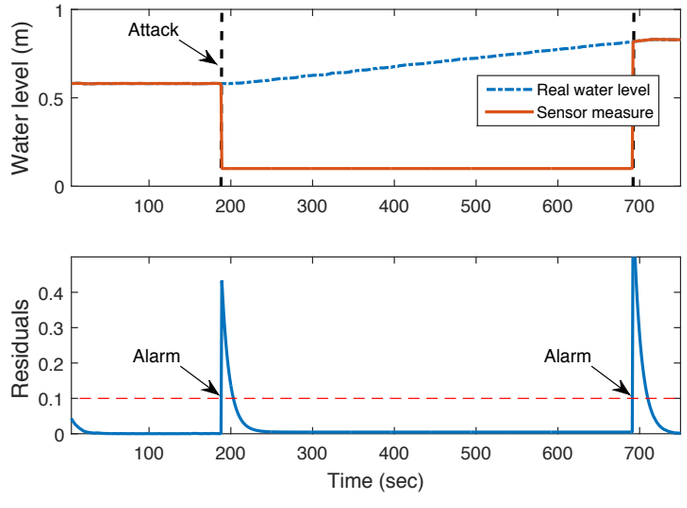
If image captured by camera does not show our challenge we detect an attack

Second Place: ACM student research competition GHC 2015

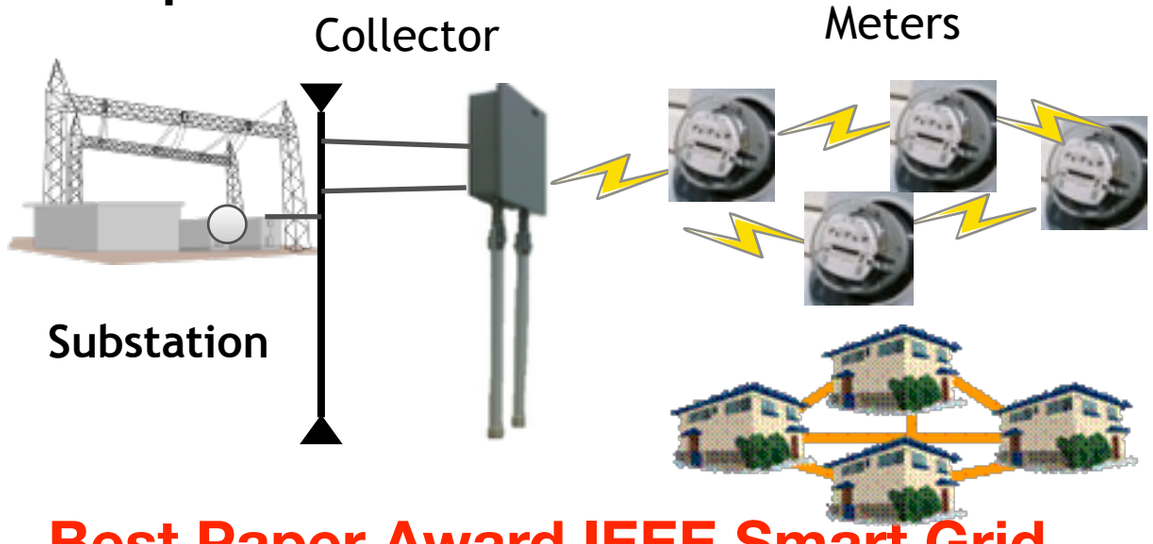
Example 2: IDS for SCADA systems

Deployment in two water treatment facilities



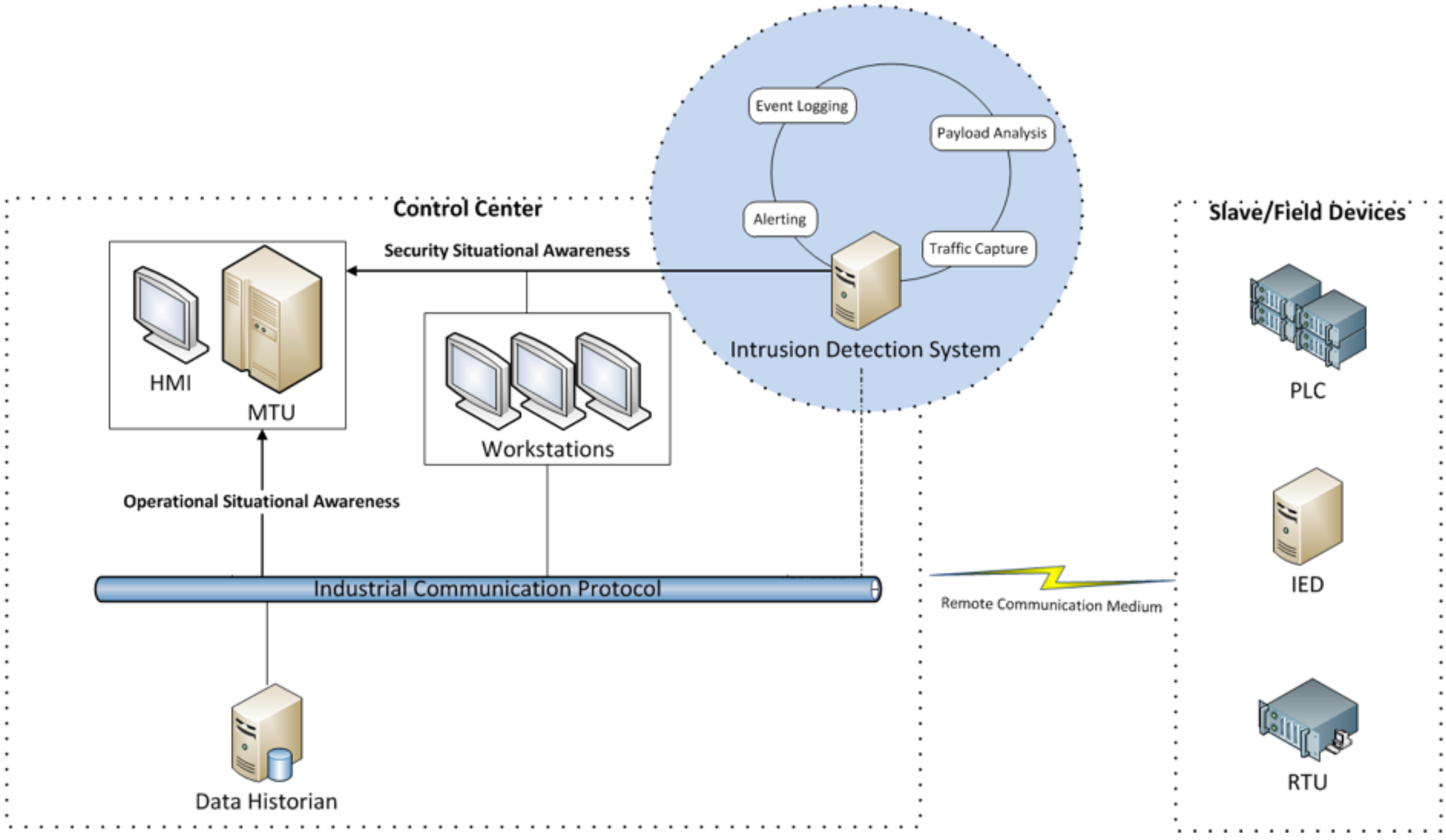


Example 3: IDS for AMI



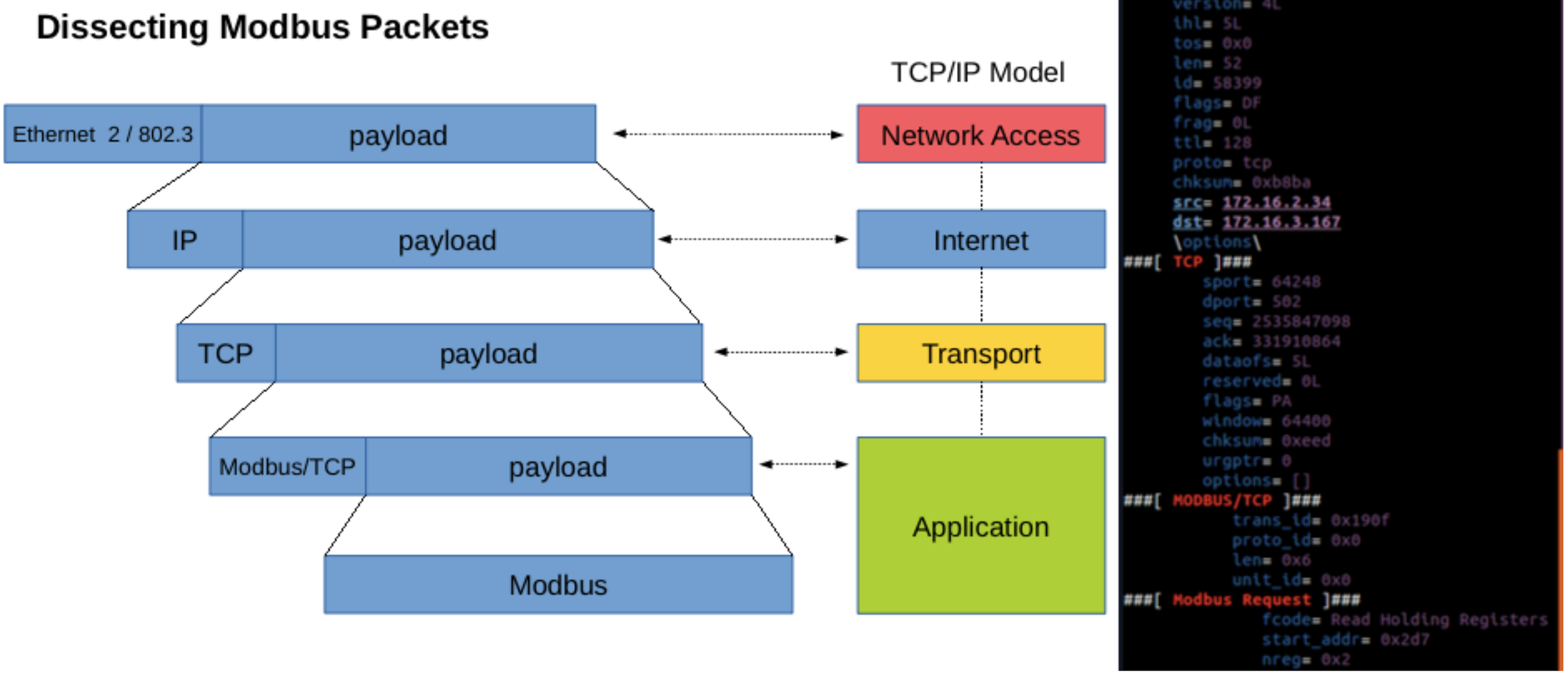
Best Paper Award IEEE Smart Grid Communications Conference 2014

Network Intrusion Detection



Deep-Packet Inspection for Industrial Control Protocols

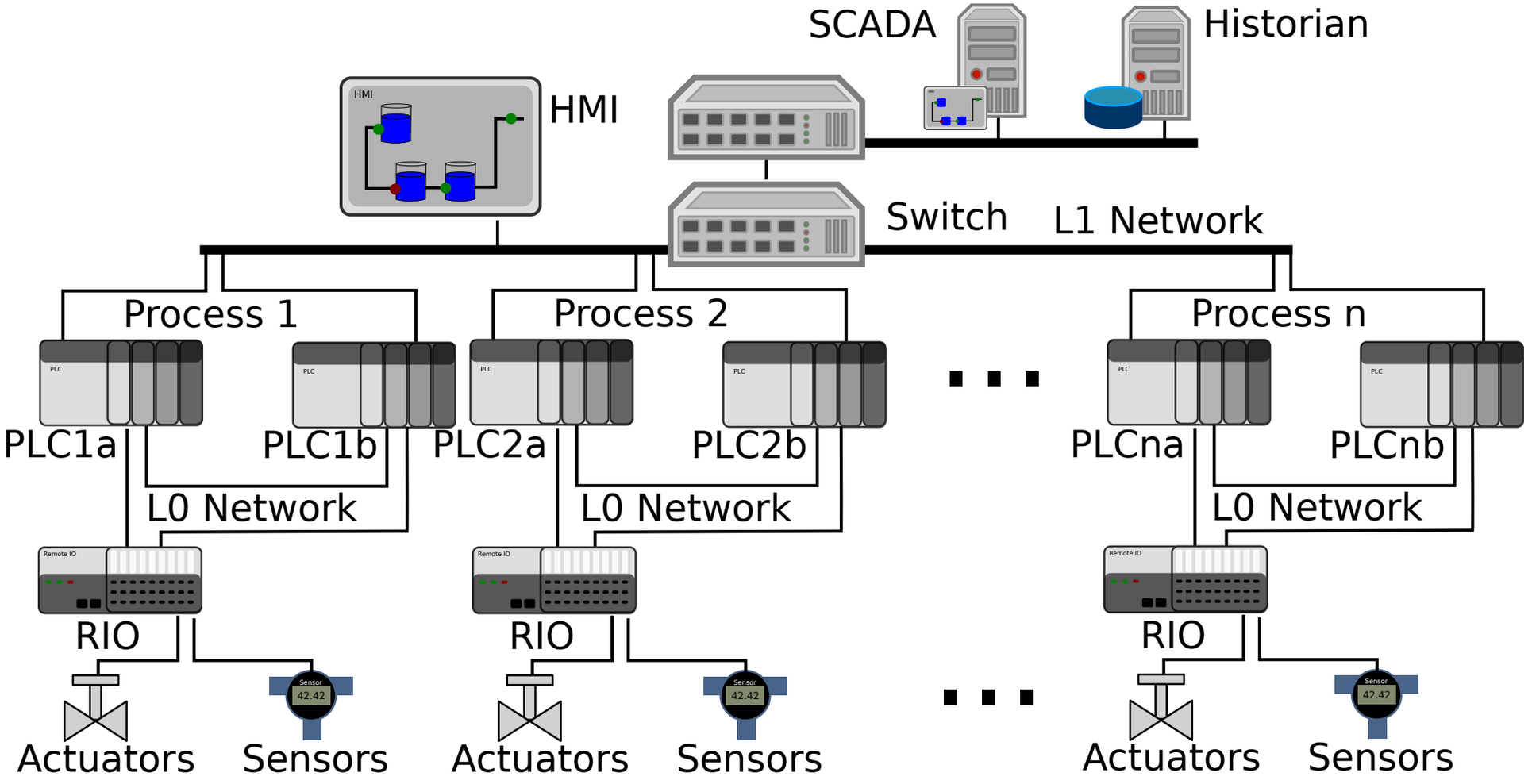
Scapy parser for Modbus




```
###[ Ethernet ]###
  dst= 00:0d:8d:00:91:0f
  src= 84:2b:2b:65:96:47
  type= 0x800
###[ IP ]###
     version= 4L
     ihl= 5L
     tos= 0x0
     len= 52
     id= 58399
     flags= DF
     frag= 0L
     ttl= 128
     proto= tcp
     chksum= 0xb8ba
     src= 172.16.2.34
     dst= 172.16.3.167
     \options\
###[ TCP ]###
        sport= 64248
        dport= 502
        seq= 2535847098
        ack= 331910864
        dataofs= 5L
        reserved= 0L
        flags= PA
        window= 64400
        chksum= 0xeed
        urgptr= 0
        options= []
###[ MODBUS/TCP ]###
           trans_id= 0x190f
           proto_id= 0x0
           len= 0x6
           unit_id= 0x0
###[ Modbus Request ]###
              fcode= Read Holding Registers
              start_addr= 0x2d7
              nreg= 0x2
```

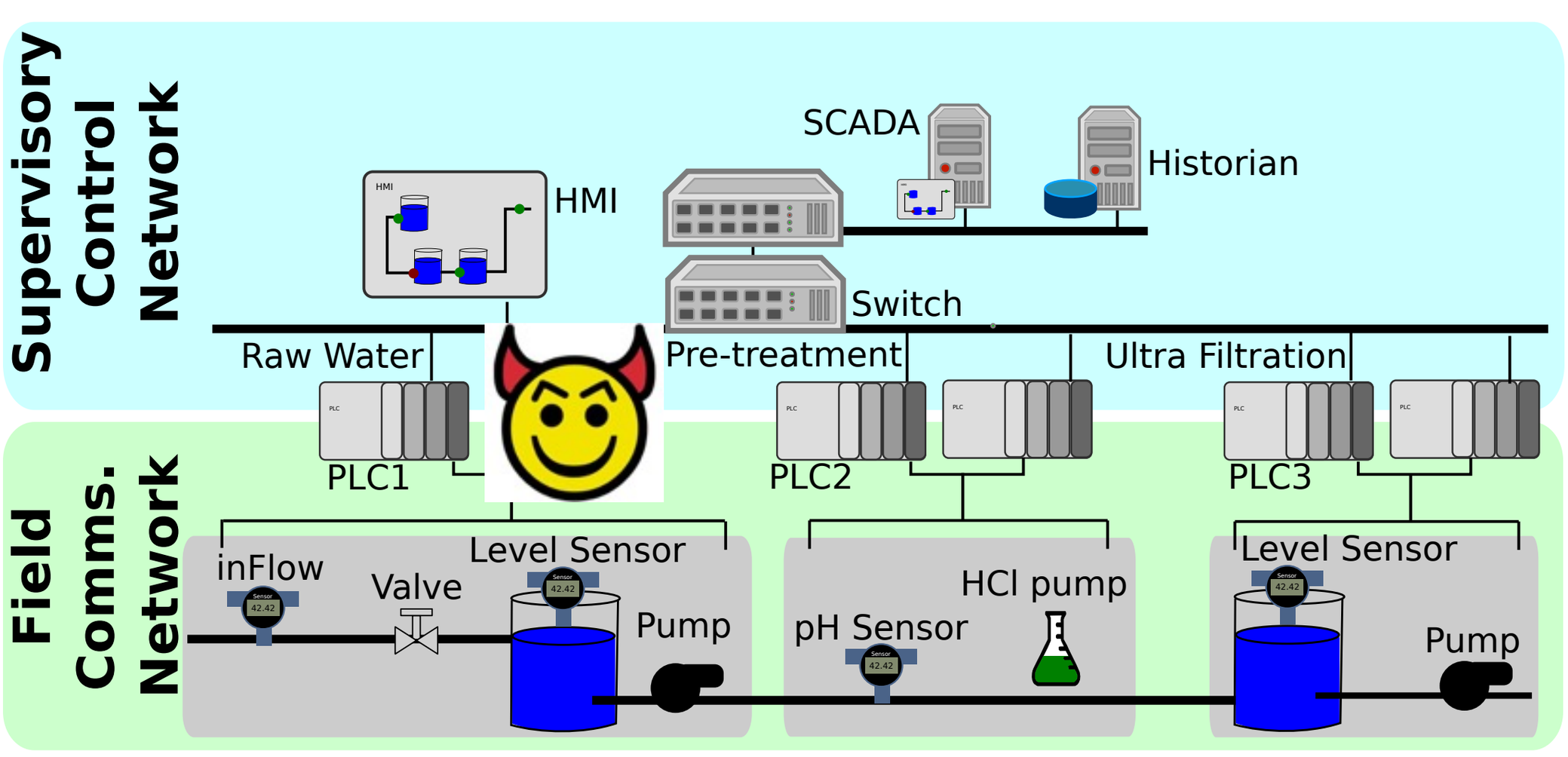
Large Variety of Industrial Control Protocols- Few Parsers, Semantic Info, Closed

- Modbus/TCP
- EtherNet/IP
- Profinet
- DNP3
- EtherCAT
- S7
- BACnet
- WirelessHART
- ISA 100

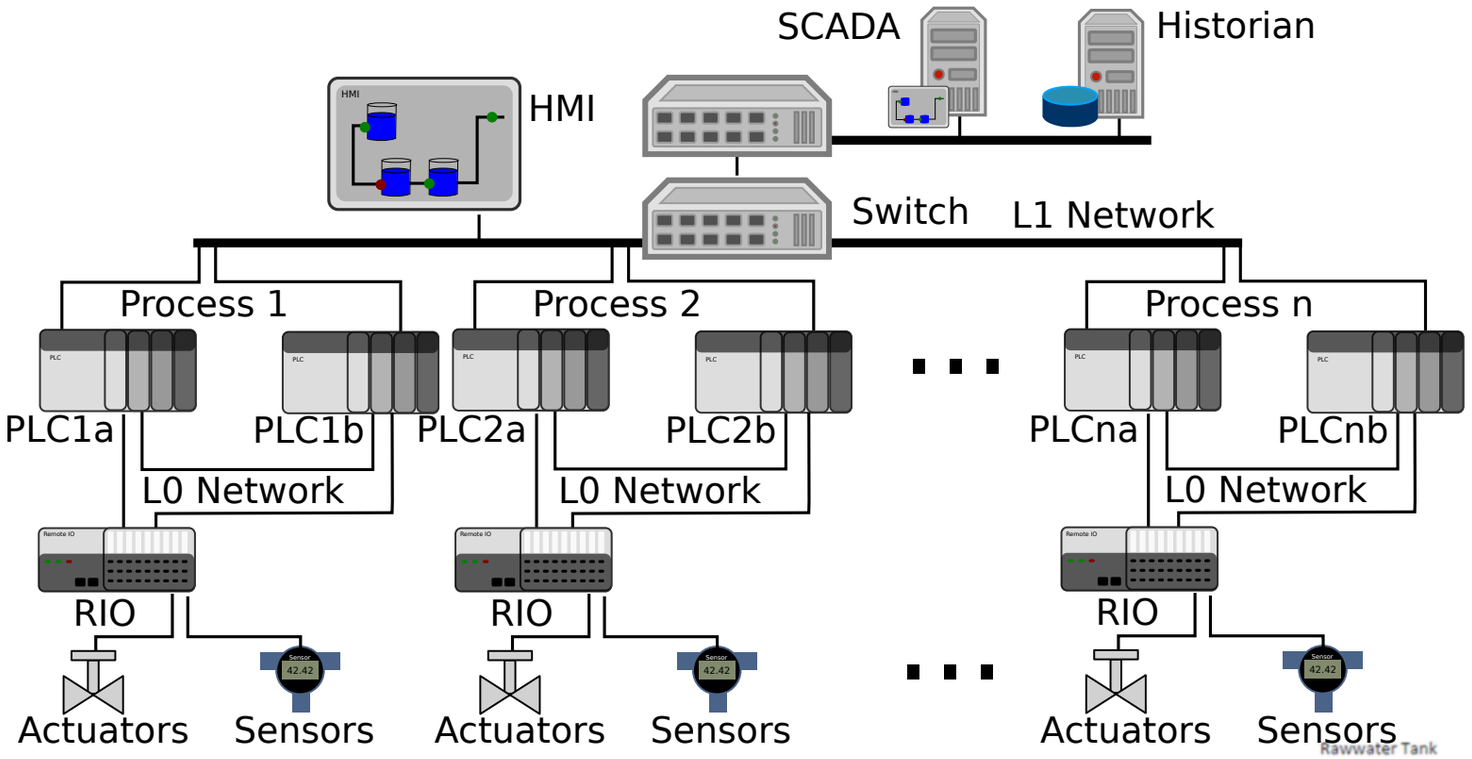


We Need to Monitor Field Networks

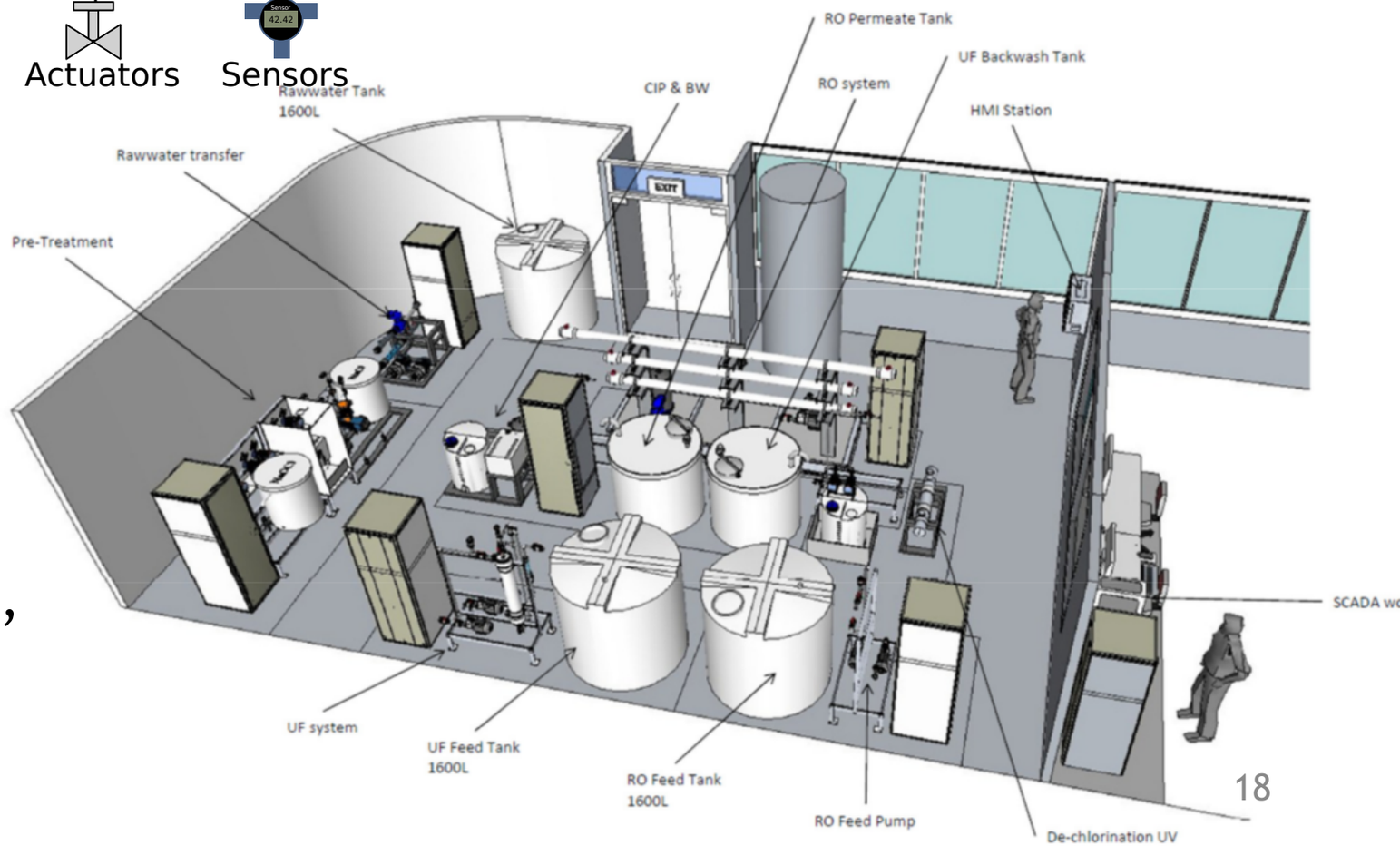
It is easier to deploy monitors in the Supervisory Network:
-highly structured info (easier to understand)
-mirror ports
BUT
Compromised PLC can send malicious data to the field and report that everything is normal to supervisory network



Developing Monitors at the Field Level (SWaT Testbed in SUTD)



D. Urbina, J. Giraldo, N. Tippenhauer, and A. Cardenas. *Attacking Fieldbus Communications in ICS: Applications to the SWaT Testbed.* Proceedings of Singapore Cyber Security Conference (SG-CRC), 2016.



We Need to Monitor the Physics of The System

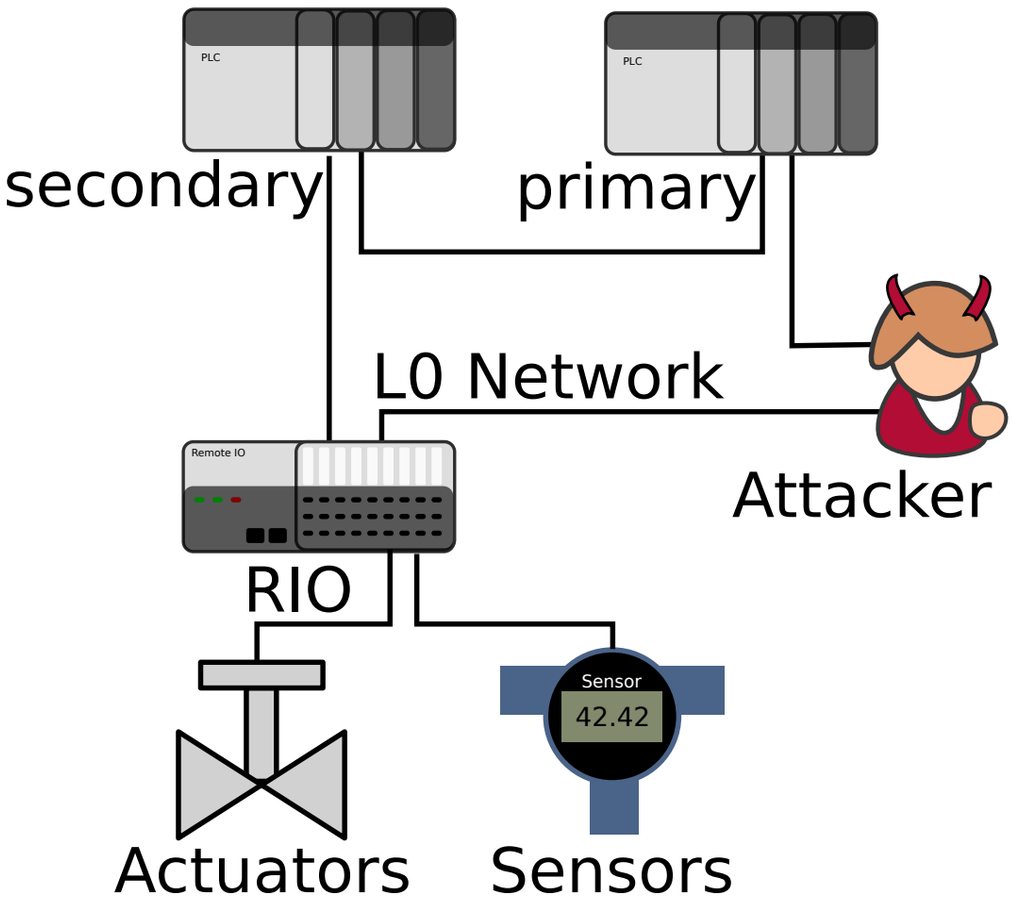
- Protocol specification/patterns correct but false info
- Physical systems follow immutable laws of nature
  - Fluid dynamics (water systems) or Electrodynamics (power grid) used to create time-series models
- These models can be used to check
  - If control commands were executed correctly
  - Sensor values are consistent with expected behavior

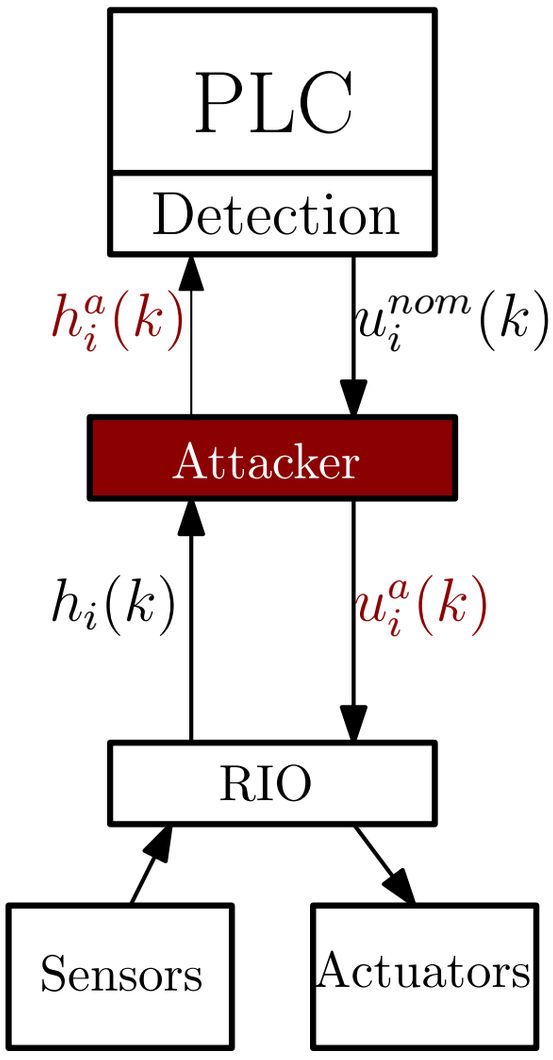
LDS Model for Raw Water Tank

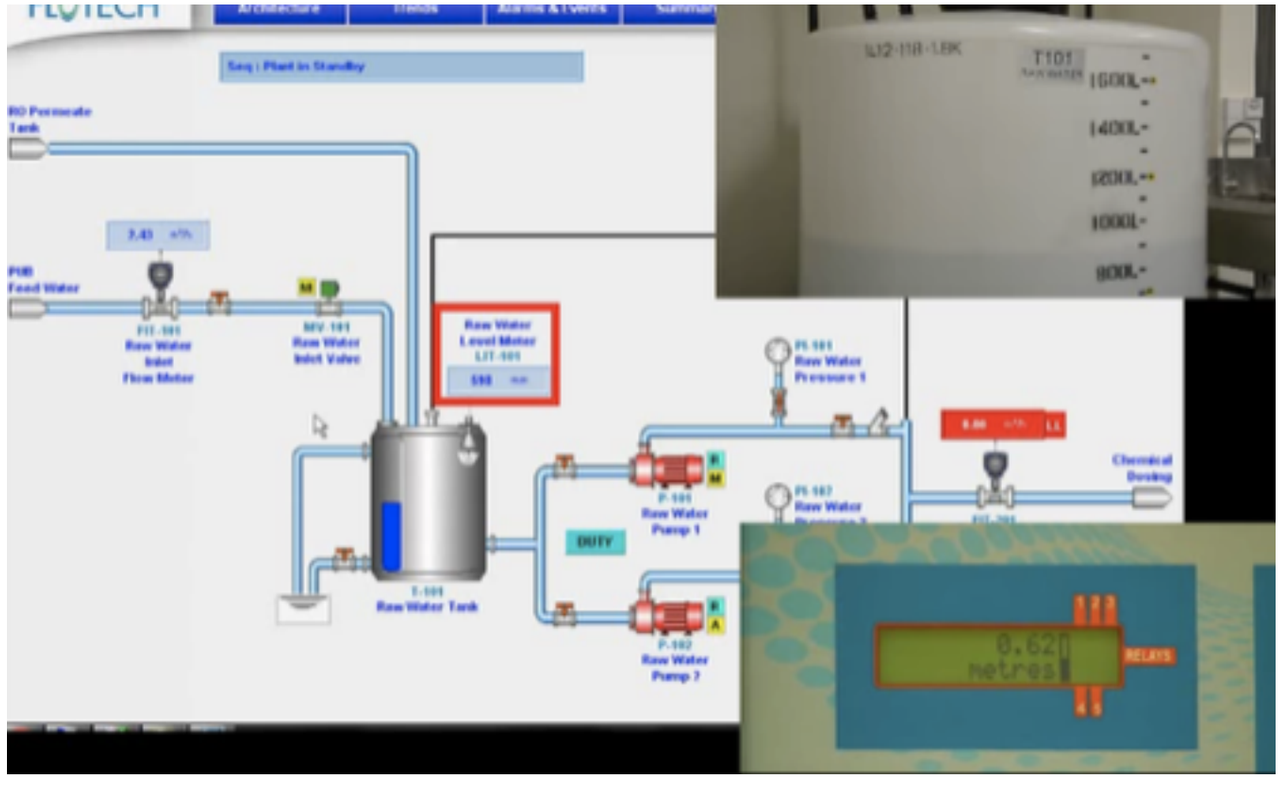
$$\frac{dV_i}{dt} = A_i \frac{dh_i}{dt} = Q_{i,in} - Q_{i,out}$$

$$h_{k+1} = h_k + \frac{Q_{i,k} - Q_{o,k}}{A}$$

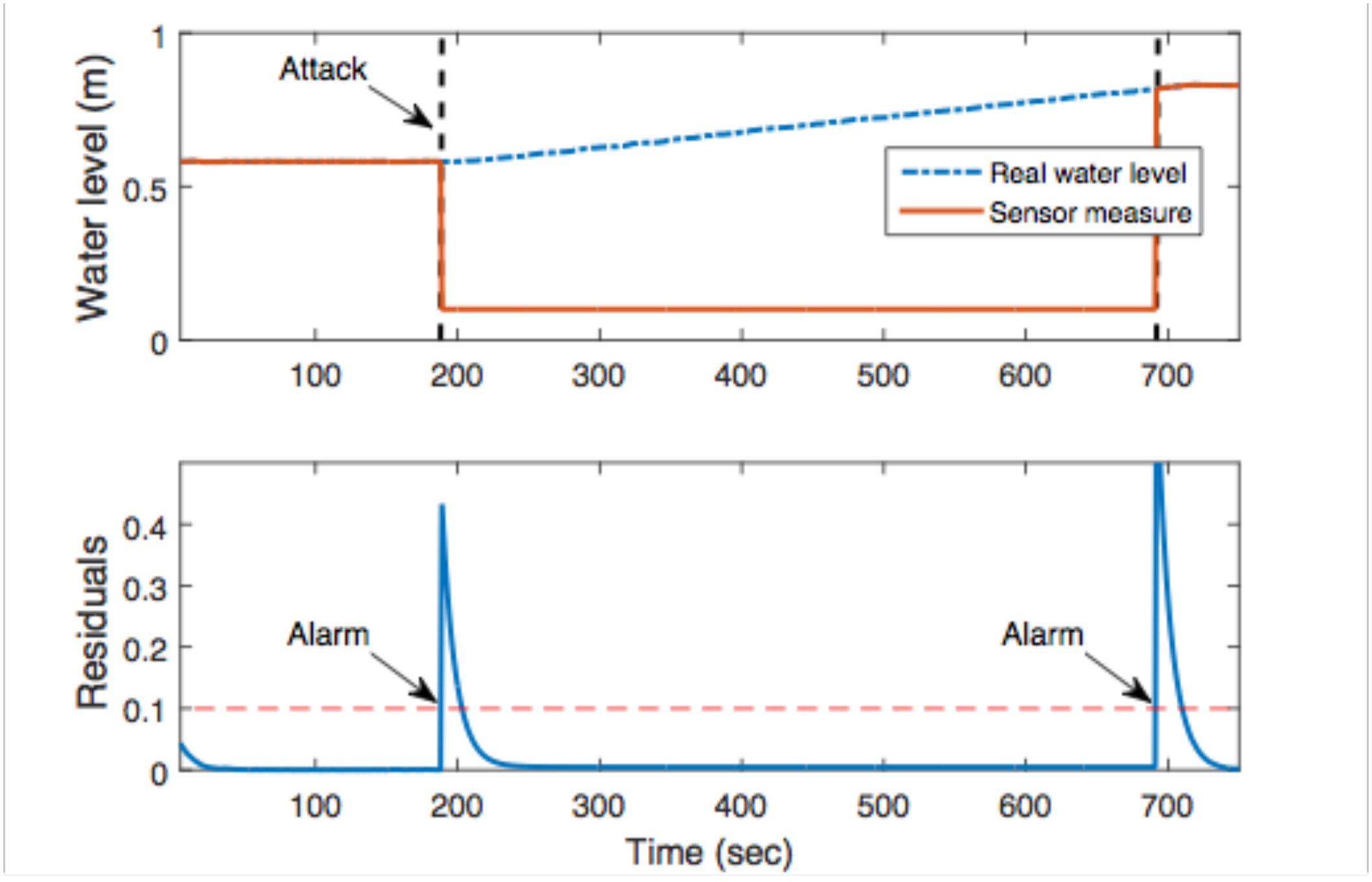
Implementing the Attack and the Defense







Problem: We Can Always Create Attacks That Are Detected



Undetected Attacks to Water Testbed