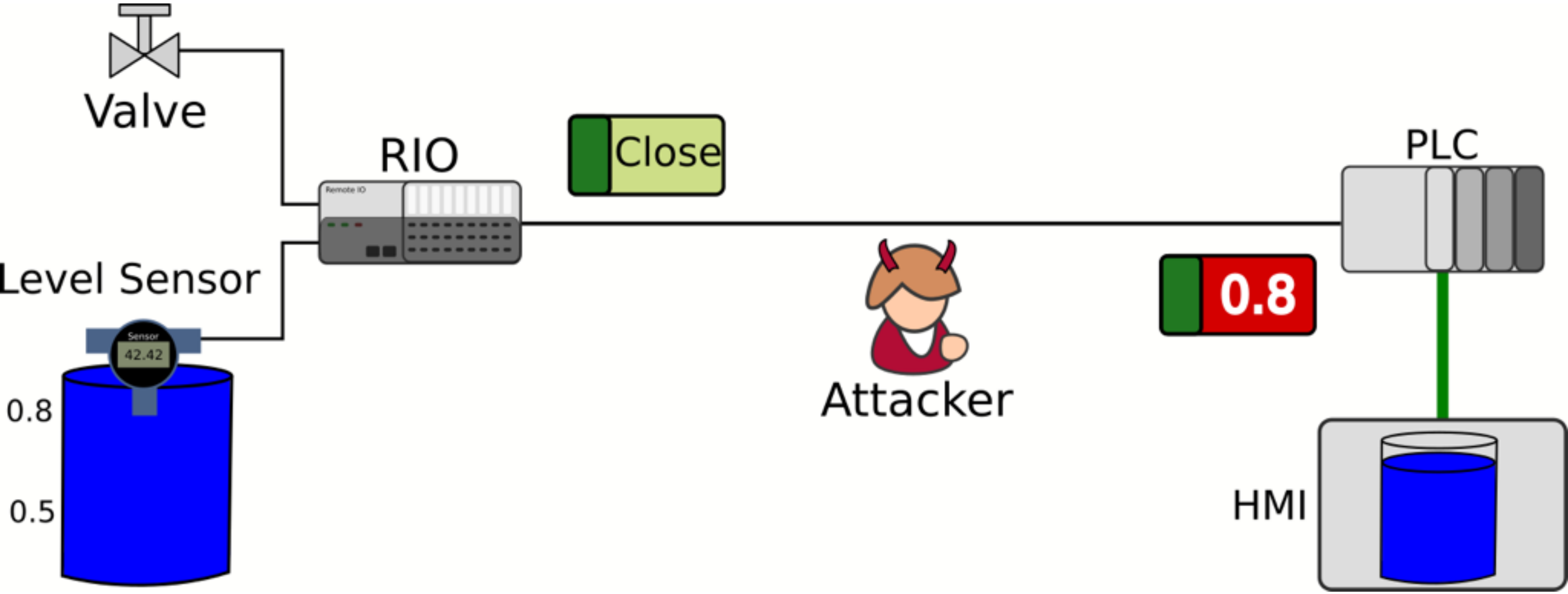
# Securing Control Systems

Alvaro Cardenas
Universidad of Texas at Dallas
2017

# 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
- 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!

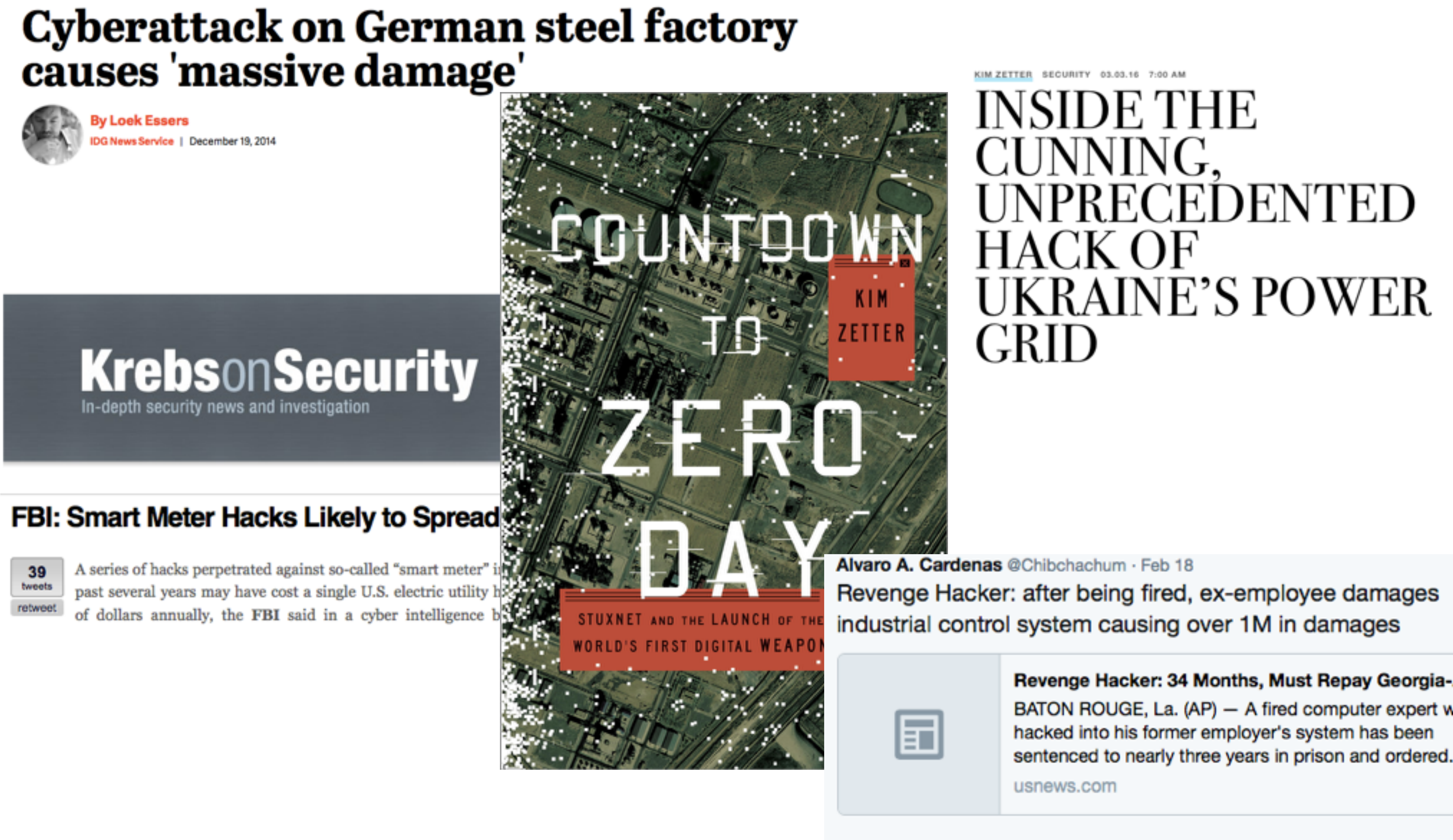
# Attack: Overflowing Tank



Attacker Objective:
Cause overflow

Control Logic:
If level < 0.5, close valve
If level > 0.8, open valve

# Attacks to CPS Systems on the Rise



## Cyberattack on German steel factory causes 'massive damage'

By Loek Essers
IDG News Service | December 19, 2014

**KrebsonSecurity**
In-depth security news and investigation

## FBI: Smart Meter Hacks Likely to Spread

A series of hacks perpetrated against so-called “smart meter” i
past several years may have cost a single U.S. electric utility h
of dollars annually, the FBI said in a cyber intelligence b

COUNTDOWN TO ZERO DAY

KIM ZETTER

STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON

KIM ZETTER SECURITY 03.03.16 7:00 AM

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

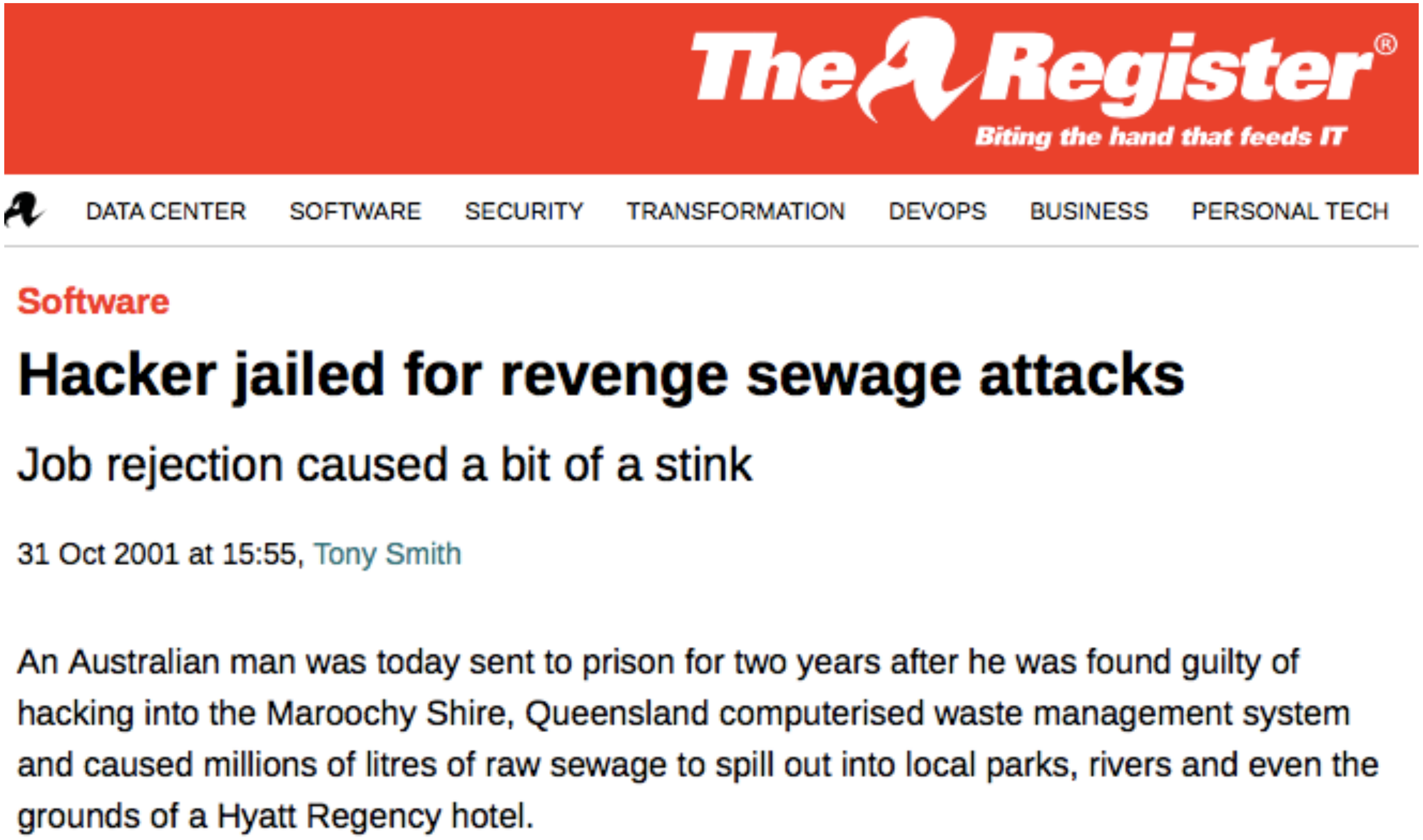
**Alvaro A. Cardenas** @Chibchachum · Feb 18

Revenge Hacker: after being fired, ex-employee damages industrial control system causing over 1M in damages

**Revenge Hacker: 34 Months, Must Repay Georgia-**
BATON ROUGE, La. (AP) — A fired computer expert w
hacked into his former employer's system has been
sentenced to nearly three years in prison and ordered.
usnews.com

# Back in 2007

2000 Maroochy Shire waste water control system



Software

## Hacker jailed for revenge sewage attacks

Job rejection caused a bit of a stink

31 Oct 2001 at 15:55, Tony Smith

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

# Back in 2007

Security of Control Systems?

Nothing new!
Use normal IT security tools!

Not my job!
It’s the IT security guy’s job!

Security

Control

If attacker has partial control of
system, it can drive it to unsafe states.

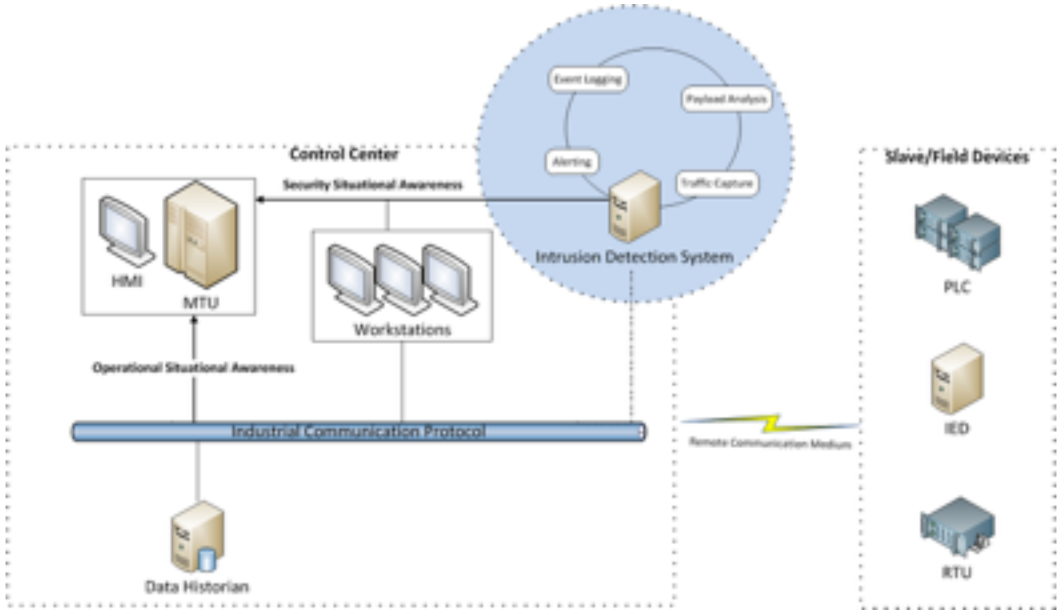
Not my job!
It’s the control engineers job!

Nothing new!
Safety and fault tolerance will
save the day!

**Attacks != Failures**

# Cy-Phy Lab Research Areas

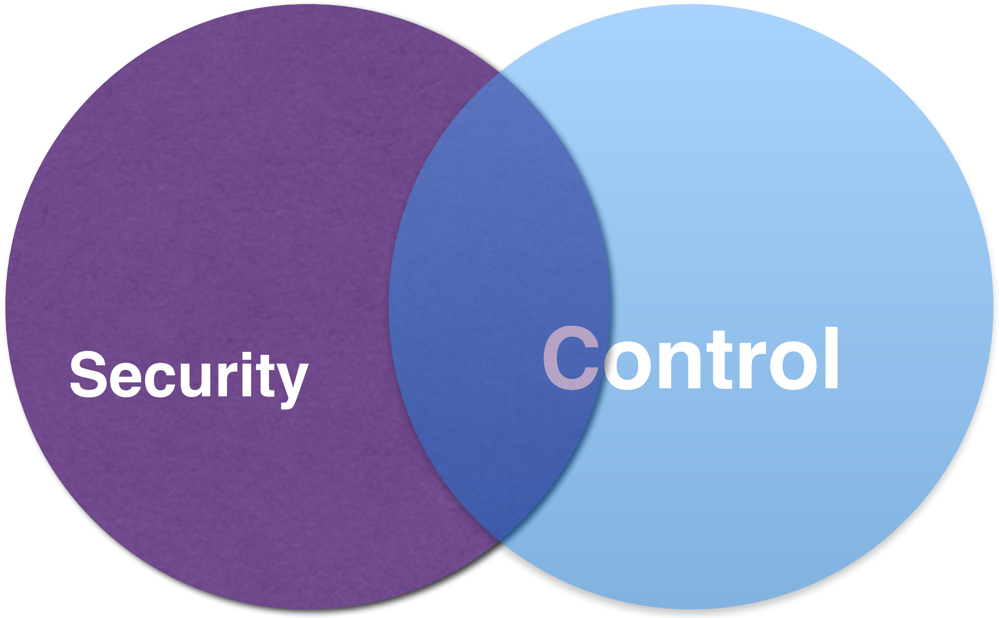
**ICS Network Security Monitoring**
AsiaCCS 2011, RAID 2012, ACSAC 2015, CCS 2016, ACC 2017


Event Logging
Payload Analysis
Control Center
Alerting
Traffic Capture
Slave/Field Devices
Security Situational Awareness
HMI
MTU
Workstations
Intrusion Detection System
PLC
Operational Situational Awareness
Industrial Communication Protocol
Remote Communication Medium
IED
RTU
Data Historian

**Attack-Resilient CPS**
HSCC 2009, GameSec 2013, IEEE ToSG 2016

**Attacks / Risk Assessment / Economics (Breaking into the System != Breaking the System)**
CIP 2009, ACSAC 2014, IEEE ToSG 2014, SG-CRC 2016

**Privacy**
Allerton 2012, CDC 2014, HoTSoS 2017, ACC 2017

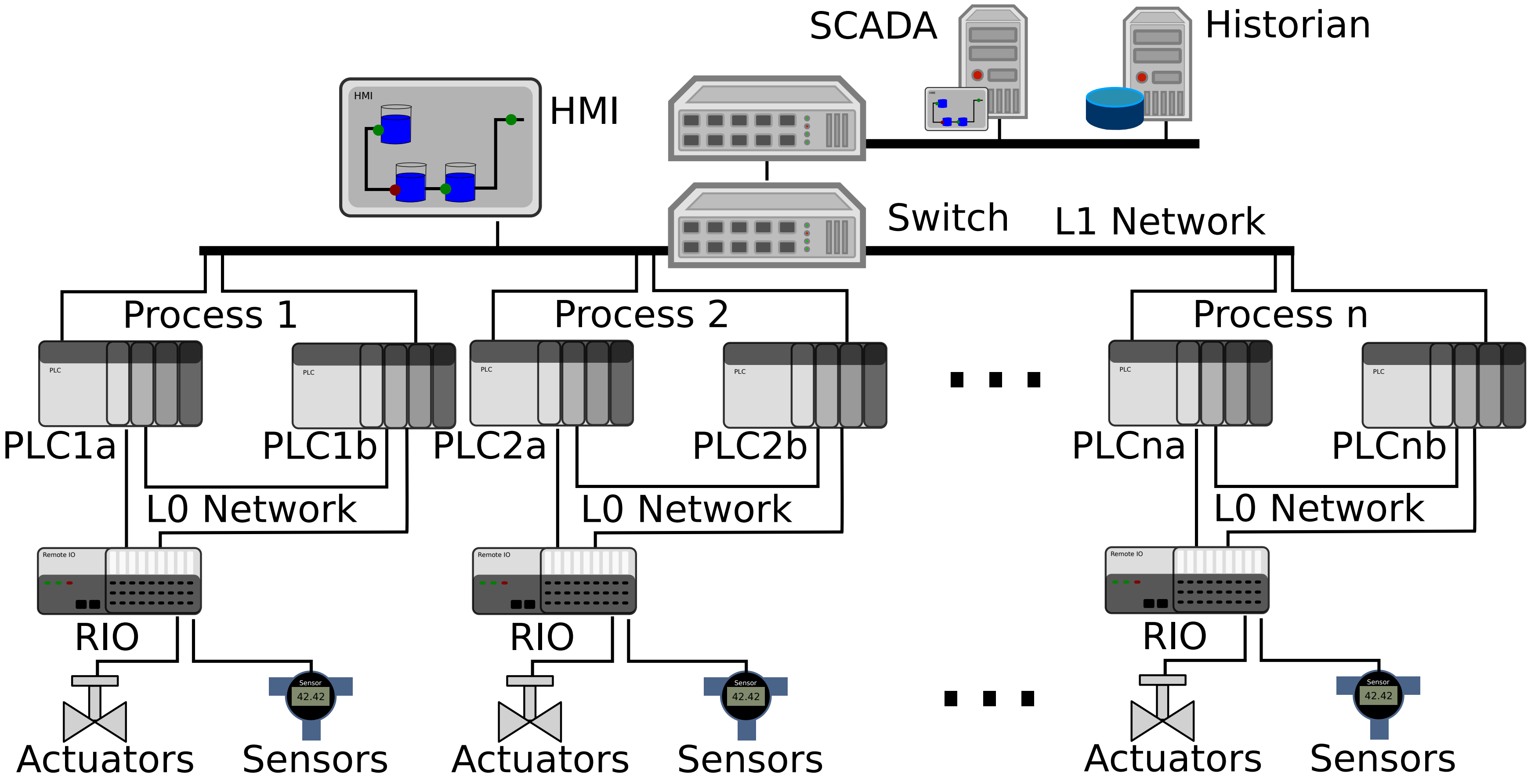


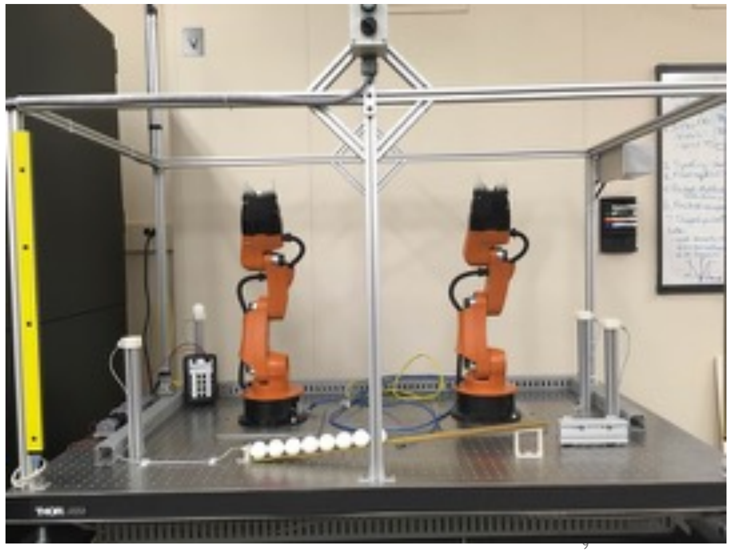
# Challenges in Monitoring Industrial Control Networks

- Many protocols
- Few parsers
- Extracting semantic info
- Closed systems

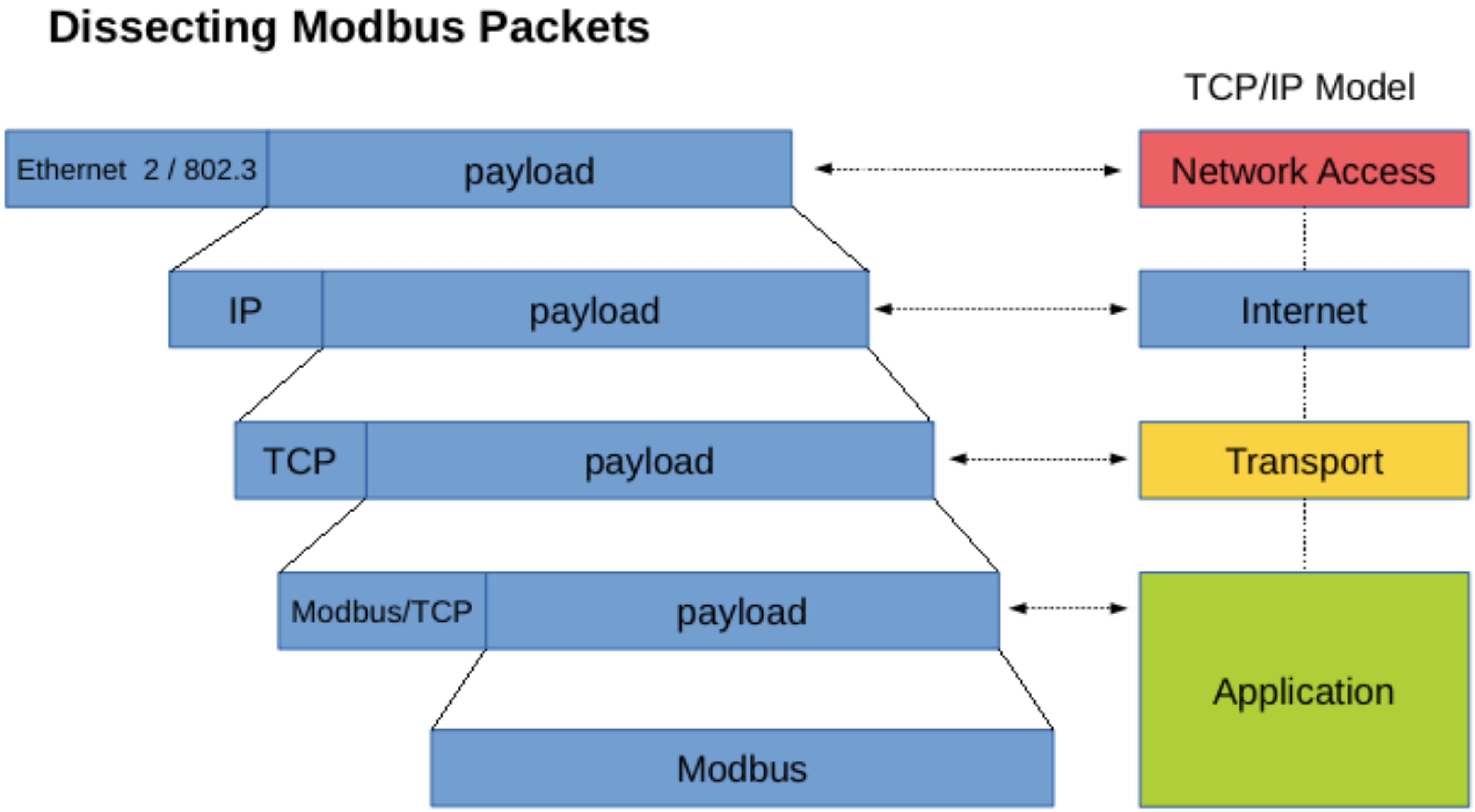
Cy-Phy Lab includes:

- Modbus/TCP
- EtherNet/IP
- Profinet
- ICCP
- ANSI C12.22
- DeviceNet
- DNP3
- EtherCAT
- S7

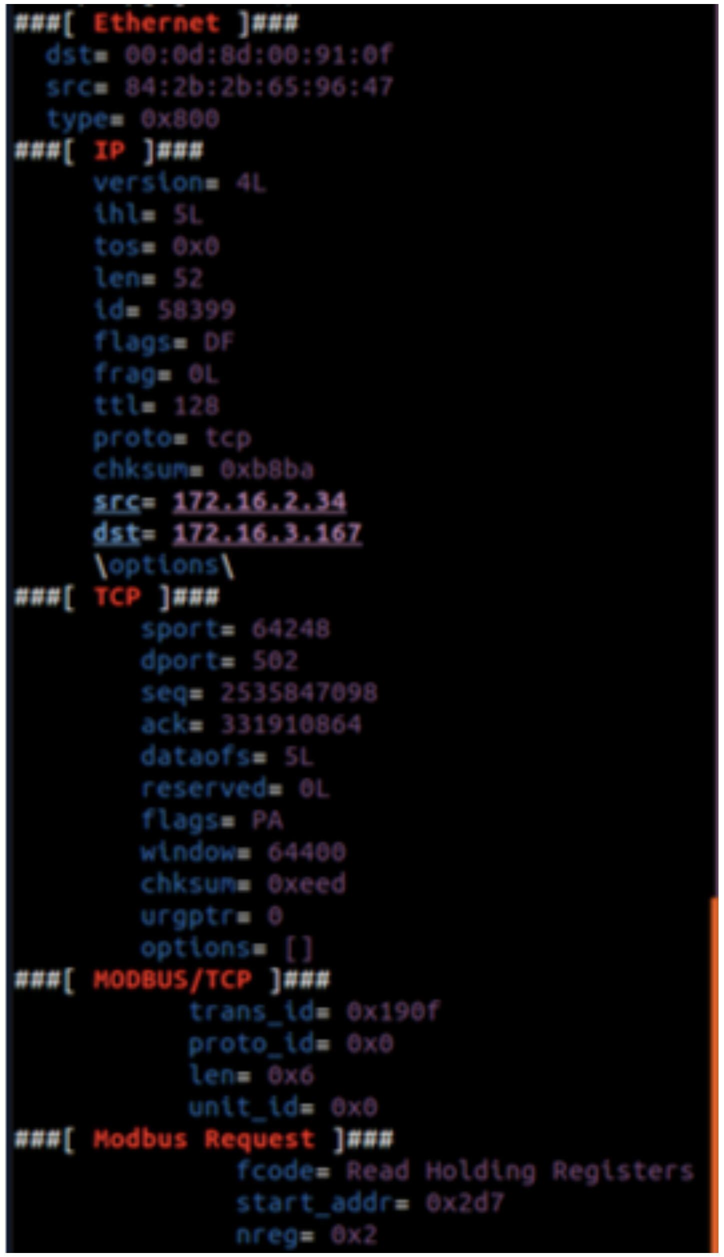




# Deep-Packet Inspection for Industrial Control Protocols



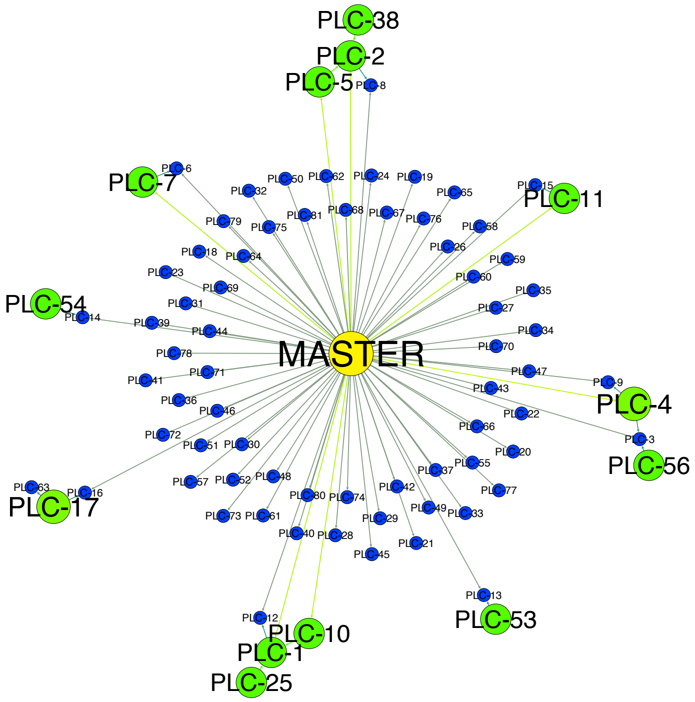
Scapy parser for Modbus



```
###[ 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
```

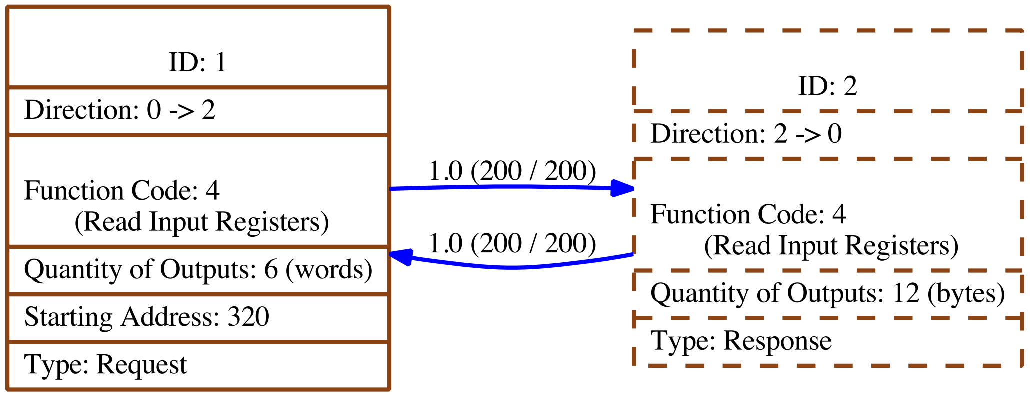
# Network Monitoring at Different Application Layers

| Headers | Commands<br>Discrete Values | Process Values |
|---|---|---|



**IEEE SmartGridComm 2014**

Best Paper Award



ID: 1

Direction: 0 -> 2

Function Code: 4
(Read Input Registers)

Quantity of Outputs: 6 (words)

Starting Address: 320

Type: Request

ID: 2

Direction: 2 -> 0

Function Code: 4
(Read Input Registers)

Quantity of Outputs: 12 (bytes)

Type: Response

**IEEE CPS-Sec 2016**

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

$$S_0 = 0. \quad (S_k + |r_k| - \delta)^+ \overset{?}{>} \tau$$

**ACM CCS 2016**
**ACC 2017**