

RSA[®]Conference2017

San Francisco | February 13-17 | Moscone Center



SESSION ID: SBX3-W4

Anatomy of Industrial Cyber Attacks



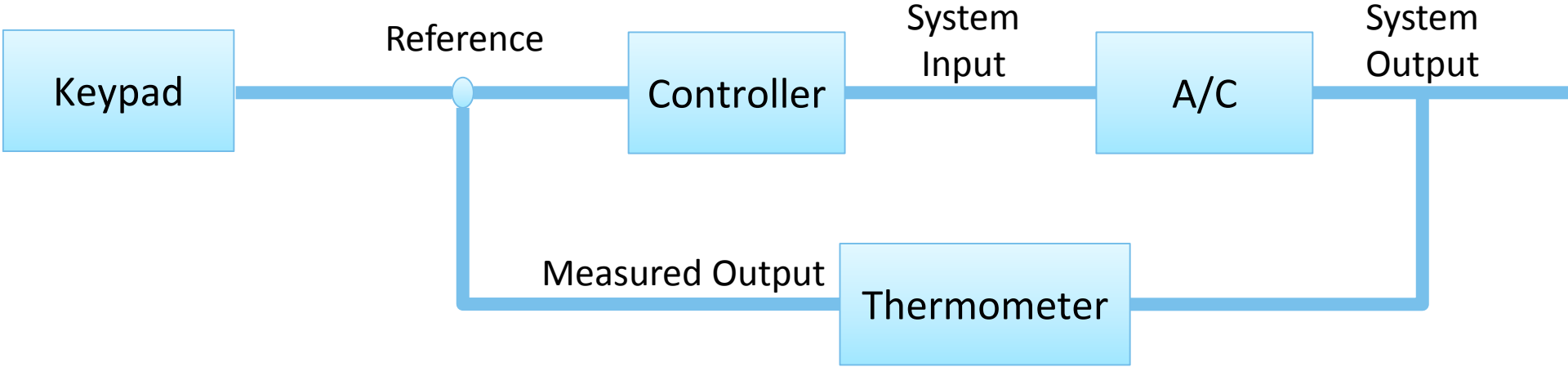
Mille Gandlesman
CTO
Indegy
@mgandelsman

Barak Perelman
CEO
Indegy
@BarakPerelman

Top Concerns as ICS Manager

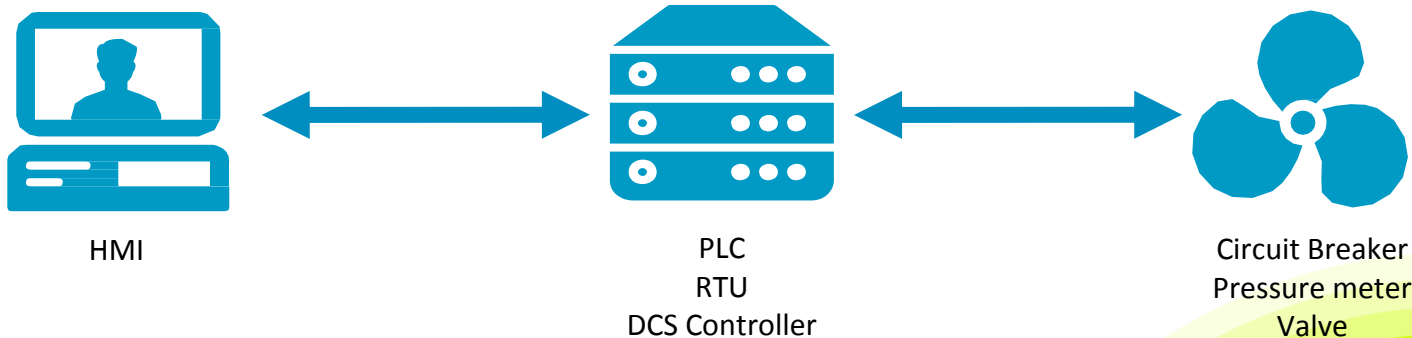
- How do I ensure my revenue generating process keeps running?
- How quickly will I discover a failure?
- How quickly can I pinpoint the source of the incident?
- How quickly can I recover?

How Would You Attack this System?

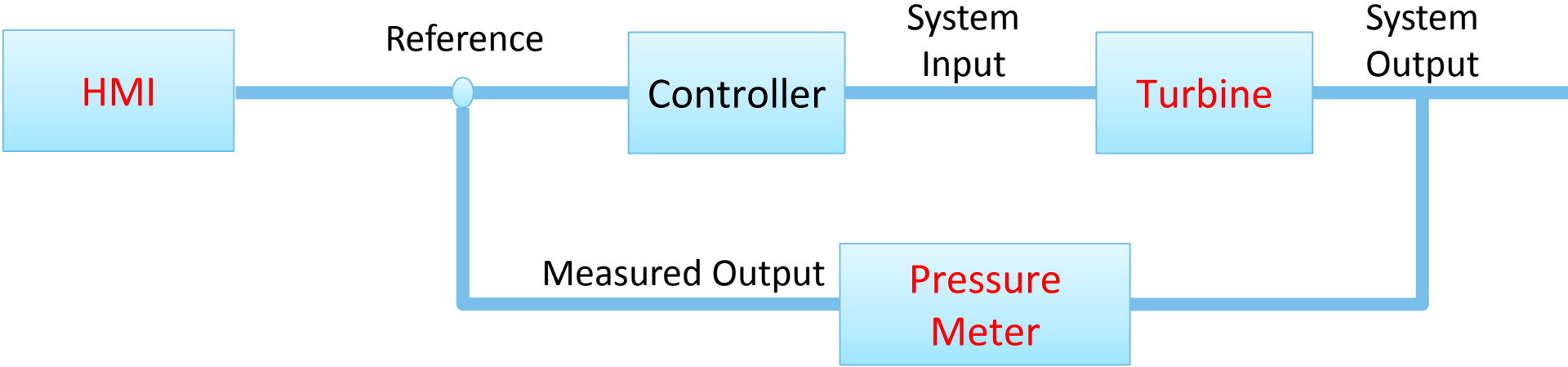


Vocabulary & Definitions

- SCADA / DCS –Supervisory, Control And Data Acquisition system (or a distributed one):
 - HMI, Engineering station – Windows machines for operators to interact with system
 - PLC/RTU/Controller – Dedicated 24/7 real time Industrial computers
 - Sensors/Actuators/IO – Industrial Equipment (Turbines, Pumps, Valves, etc.)

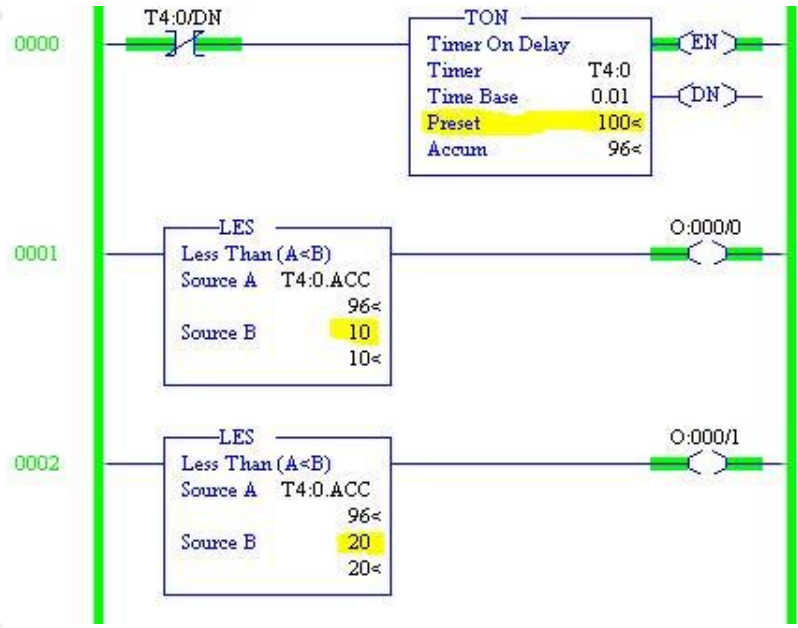


How Would You Attack this System?



Vocabulary & Definitions

- Process Parameters
- Logic
- Configuration
- Firmware



Security Gaps in an ICS Network

#RSAC

- Understanding what you have in your network
- No visibility into critical control-layer activity
- Blindspots of physical access to devices

#1: Understanding What You Have in Your Network

- System implemented a very long time ago
 - Changes made over years
 - Without documentation
- Or:
- It was recently inherited:
 - Nobody knows anything

#2: No Visibility into Critical Control Plane Activity

Regular Activity



HMI

(Data Plane)
Set RPM to **1000**



PLC / DCS

Set Actuator



Turbine

- Get new RPM from register
- If RPM > 2000
 Ignore new RPM
- Set new RPM

#2: No Visibility into Critical Control Plane Activity

Regular Activity



HMI

(Data Plane)
Set RPM to **1000**



PLC / DCS

Set Actuator



Turbine

- Get new RPM from register
- If RPM > 2000
 Ignore new RPM
- Set new RPM

Attack Scenario



HMI

(Control Plane)
Change Control Logic



PLC / DCS



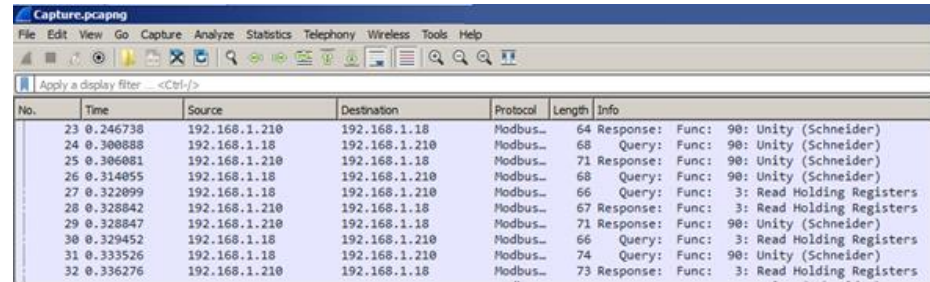
Turbine

- Get new RPM from register
- ~~If RPM > 2000~~
 ~~Ignore new RPM~~
- Set RPM to 5000



#2: No Visibility into Critical Control Plane Activity

- No Authentication Required:
 - Anyone with network access can change controller logic!
- Difficult to monitor:
 - The meaningful changes are the hardest to identify
- Note that there is no need to exploit vulnerabilities



The screenshot shows a network traffic capture in Wireshark. The display filter is set to 'Apply a display filter ... <Ctrl-/>'. The table below represents the data shown in the packet list pane.

No.	Time	Source	Destination	Protocol	Length	Info
23	0.246738	192.168.1.210	192.168.1.18	Modbus...	64	Response: Func: 90: Unity (Schneider)
24	0.300888	192.168.1.18	192.168.1.210	Modbus...	68	Query: Func: 90: Unity (Schneider)
25	0.306081	192.168.1.210	192.168.1.18	Modbus...	71	Response: Func: 90: Unity (Schneider)
26	0.314055	192.168.1.18	192.168.1.210	Modbus...	68	Query: Func: 90: Unity (Schneider)
27	0.322099	192.168.1.18	192.168.1.210	Modbus...	66	Query: Func: 3: Read Holding Registers
28	0.328842	192.168.1.210	192.168.1.18	Modbus...	67	Response: Func: 3: Read Holding Registers
29	0.328847	192.168.1.210	192.168.1.18	Modbus...	71	Response: Func: 90: Unity (Schneider)
30	0.329452	192.168.1.18	192.168.1.210	Modbus...	66	Query: Func: 3: Read Holding Registers
31	0.333526	192.168.1.18	192.168.1.210	Modbus...	74	Query: Func: 90: Unity (Schneider)
32	0.336276	192.168.1.210	192.168.1.18	Modbus...	73	Response: Func: 3: Read Holding Registers

#2: No Visibility into Critical Control Plane Activity

- Controller logic is the most critical part of an ICS network
Unfortunately it's also the weakest link there
- Sensor reading is not reliable for finding malicious activity
And also, might be too late
- Standard network monitoring is not enough
Control-layer aware deep packet inspection needed
Physical cyber attacks can occur

#3: Blindspots of Physical Access to Devices

- On-The-Fly-Changes:
 - What changed?
 - What was the previous configuration?
- System integrator access:
 - Who to blame on failure?

Apply What You Have Learned Today

- Next month you should:
 - Identify and create a backup of all your controllers
- Next quarter you should:
 - Keep track of control-layer actions in your ICS network
- Within six months you should:
 - Apply a security system that is aware to changes in controller logic, both those emerging from the network as well as locally