Breakage

Jason Larsen

Who am I?

- Currently work for IOActive
- Spent the last five years doing SCADA research
- I don't often get a chance to speak to security researchers

SCADA

- Supervisory Control and Data Acquisition

What do we know about SCADA?

- Controls physical systems
- Comes in two flavors
  - Supervisory Control
  - Momentary Control

SCADA vs. The Movies

- SCADA hacking has been a staple of Hollywood for a while
- Evil hackers use computers to kill people
- As a result, even non-computer people have some concept of SCADA hacking

Myth vs. Legend

- Lots of myths in SCADA
  - "Digital Pearl Harbor"
  - "Terrorist can take down the nation"
  - "I now have to fear my toaster"
- First let's have a reality check

Live Free or Die Hard

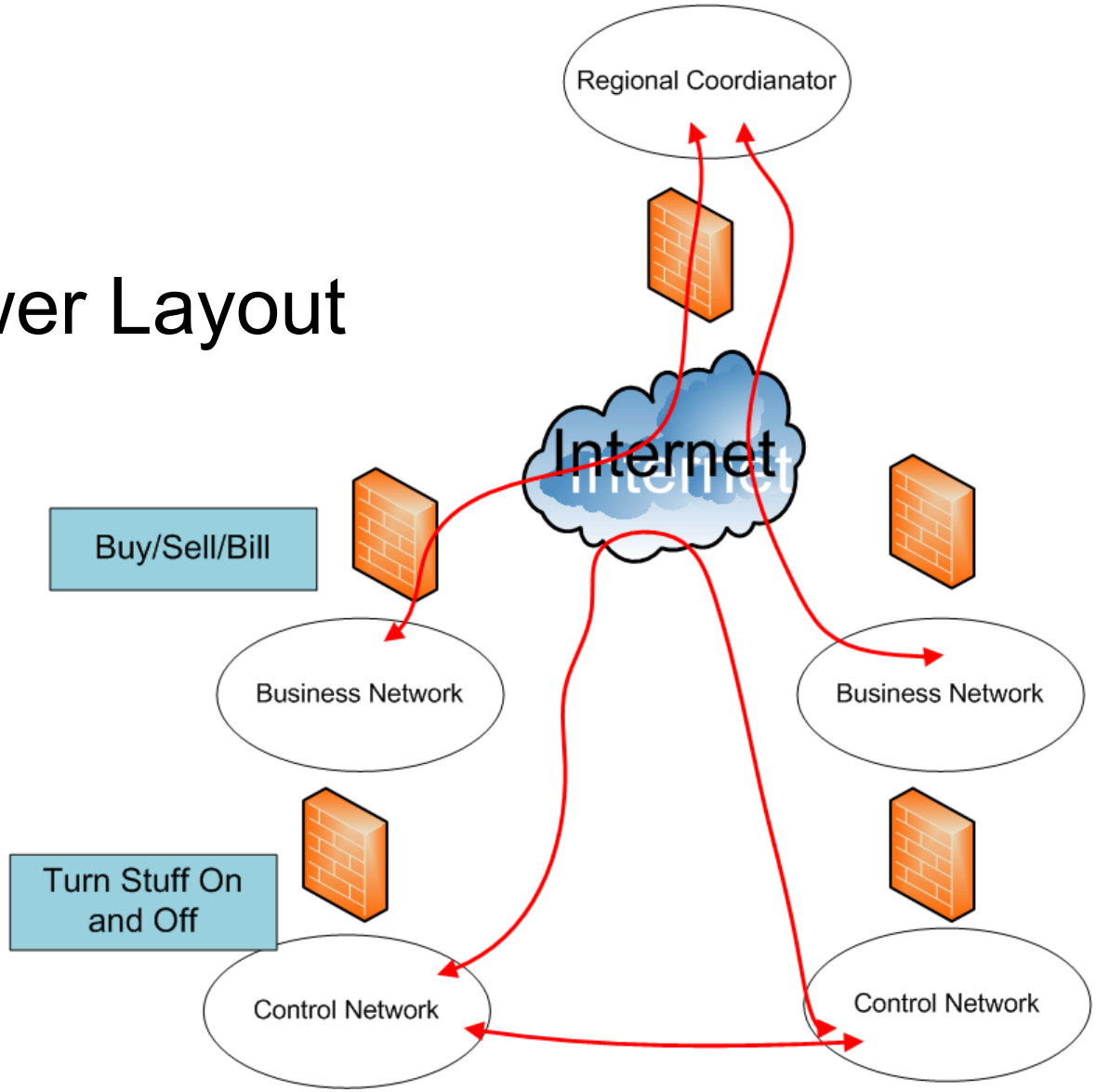
“Power Grid Isn’t Connected”

Electric Power Connectedness

- If you had to hook together the most critical computer systems in the nation, you'd use a bullet-proof protocol right?
- One that had been well thought out and was easy to secure?

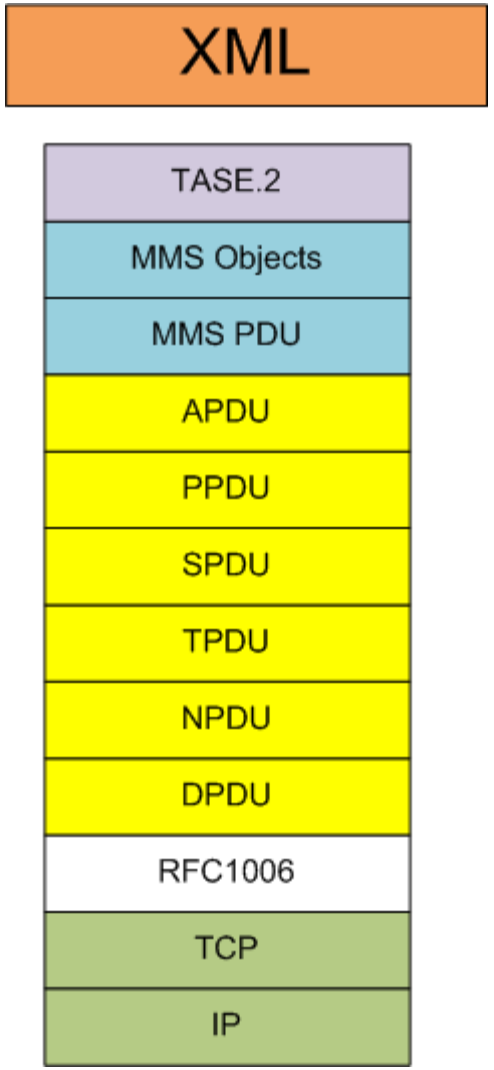
Electric Power Layout

(Finger Paint Version)



ICCP

- Complete TCP/IP Stack
- RFC Glue
- ISO Stack
- MMS Stack
- ASN.1
- Custom Protocol
- XML



“Only Super Hackers Can Get In”

Incidents

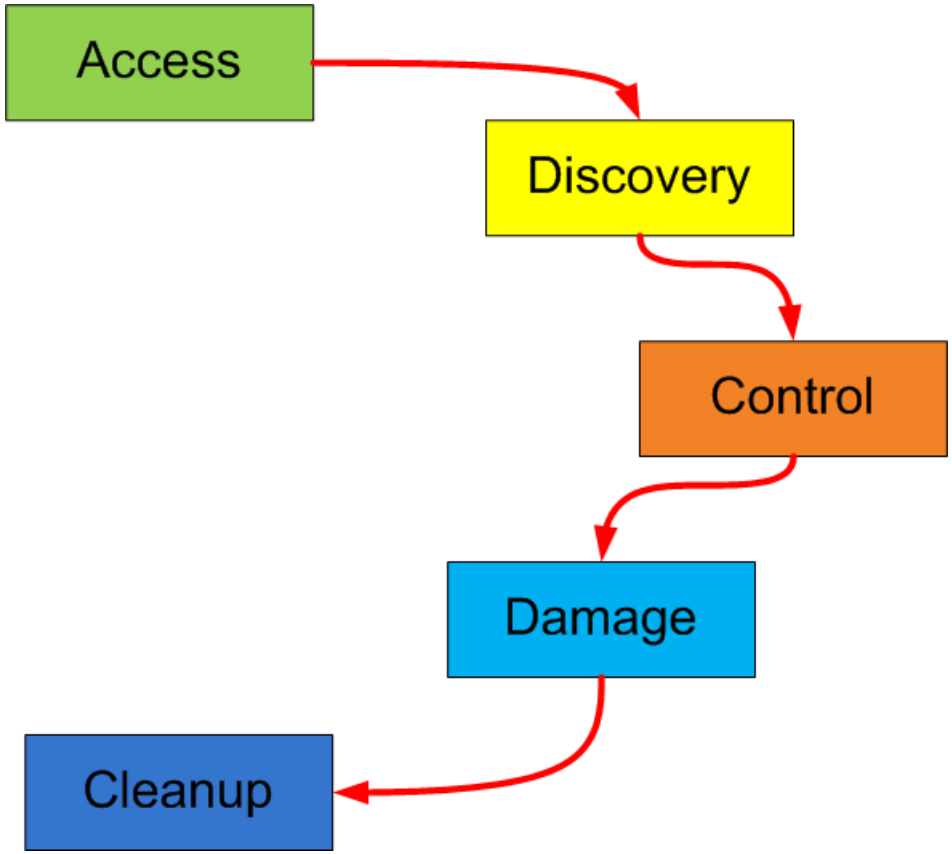
- JavaScript scans
- Extortion
- CIA statement

“Send all the Gas There”

Oil and Natural Gas Delivery

- Relief valves work really well
- Oil pipeline explosion in Russia
  - “ in June of 1982, a huge explosion occurred in the Siberian wilderness in the former Soviet Union. The yield was estimated at 3 kilotons It had been implanted in the host software by a foreign intelligence service.”

Stages of a SCADA Attack



Maximizing Damage

- Most public research has focused on access to the SCADA LAN and control of the process
- Very little information about how an attacker would maximize damage once he had achieved control

Big Equipment vs. Little Equipment

- Big equipment in a large process is generally easier to physically damage than tabletop equipment
- Only one public video of physical damage of big equipment

Aurora Project

Classes of Physical Damage

- Watching generators jump is fun, but are there other ways to physically damage equipment?

Example 1 - Water Hammers

QuickTime

Example 2 - Crunching Motors

Classes of Physical Damage

- Inertial Attacks
- Exclusion Attacks
- Resonance Attacks
- Wear Attacks
- Surge Attacks
- Latent Abilities

Inertial Attacks

- Heavy stuff doesn't like to speed up or slow down
- This is the easiest and most common way to make physical equipment fail
- The larger the process, the more likely it can be accelerated to failure

Exclusion Attacks

- Some stuff isn't supposed to happen at the same time
  - For example, the motor should never be operating if the oil pump isn't on

Resonance Attacks

- Resonance attacks happen mostly in electrical power and water distribution
- Small variation in current or flow are conserved as a standing wave in another part of the system
- Continuing the small variations increases the size of the standing wave
- These are the hardest to pull off remotely

Wear Attacks

- Components have a finite lifespan
- Manipulating the controls can often significantly reduce the lifespan of the component
  - For example, keeping a clutch 90% of the way engaged

Surge Attacks

- "Send all the gas there now"
- Continuous systems are designed to handle only a certain amount of product at a time
- Exceeding those limits can cause physical damage
  - For example, filling a mixer 100% full instead of the normal 20%

Latent Abilities

- Building every piece of a process out of custom components is expensive
- Wherever possible, off-the-shelf components are used
- Off-the-shelf components are often manufactured for more than one purpose
  - For example, a motor that can run in reverse but is never used that way

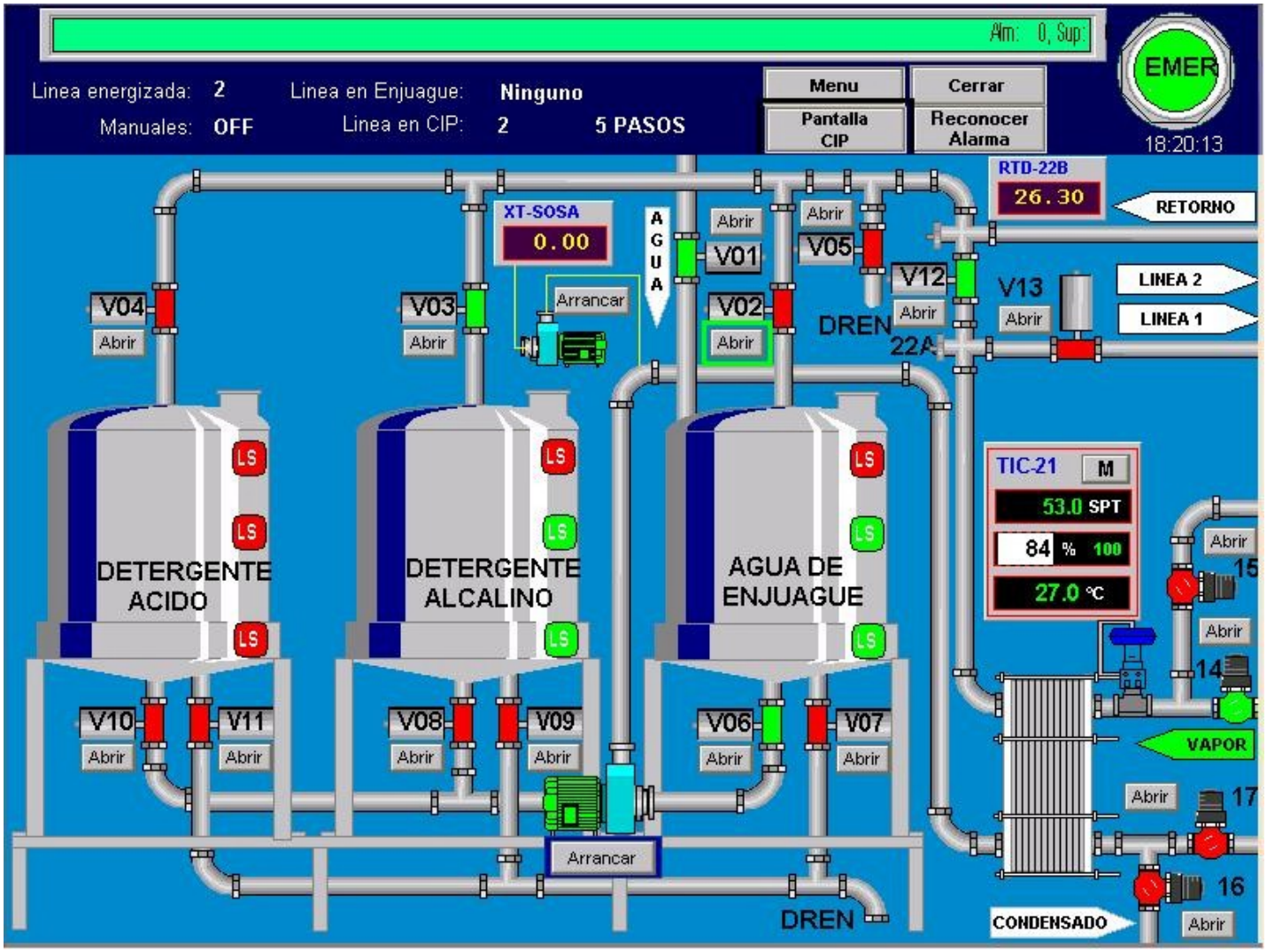
Discovery

- Great, but we probably don't have the engineer pointing out all the weaknesses

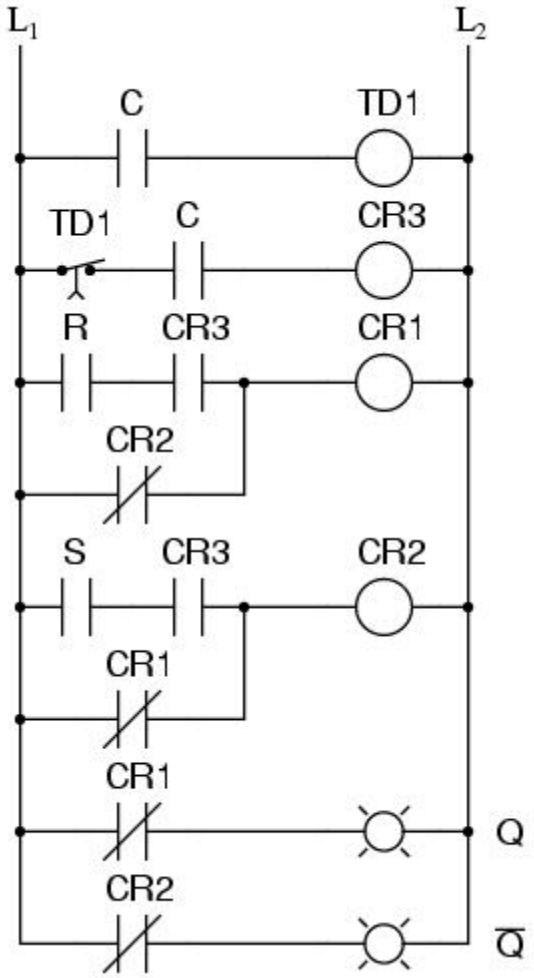
Information

- Equipment doesn't come with a manual on how to physically damage it
- You either have to find the weak points or guess
- Guessing can be surprisingly effective

What you probably already have



Analyzing Ladder Logic for Clues



E	S	R	Q	$\overline{Q}$
⌐	0	0	latch	latch
⌐	0	1	0	1
⌐	1	0	1	0
⌐	1	1	0	0
x	0	0	latch	latch
x	0	1	latch	latch
x	1	0	latch	latch
x	1	1	latch	latch

Ladder Logic

- In modern systems, most of the process safety depends on the logic in the controllers
- Analyzing tells you what the engineer that designed the process was worried about

Start at the Master Stop

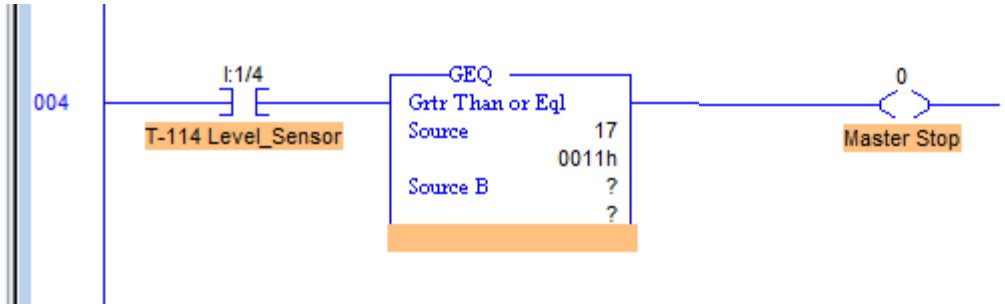
- All roads that lead to the master stop are interesting
- It can be labeled any number of things—luckily labels are human readable

Ladder Logic

- This is a candidate for an exclusion attack
- The engineer wanted to make sure that a motor wasn't running at the same time a valve was closed

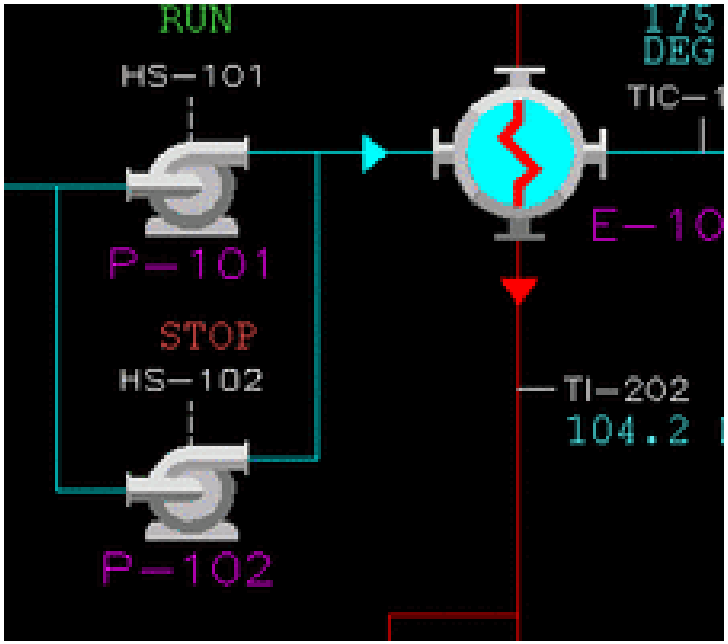
Ladder Logic

- If the level is above 17, shut everything down
- Since this is in the ladder logic, we can override the shutdown



Operator's Console

- Here's a good candidate for a surge attack
- Did the engineer plan for both pumps to kick on at full power simultaneously?

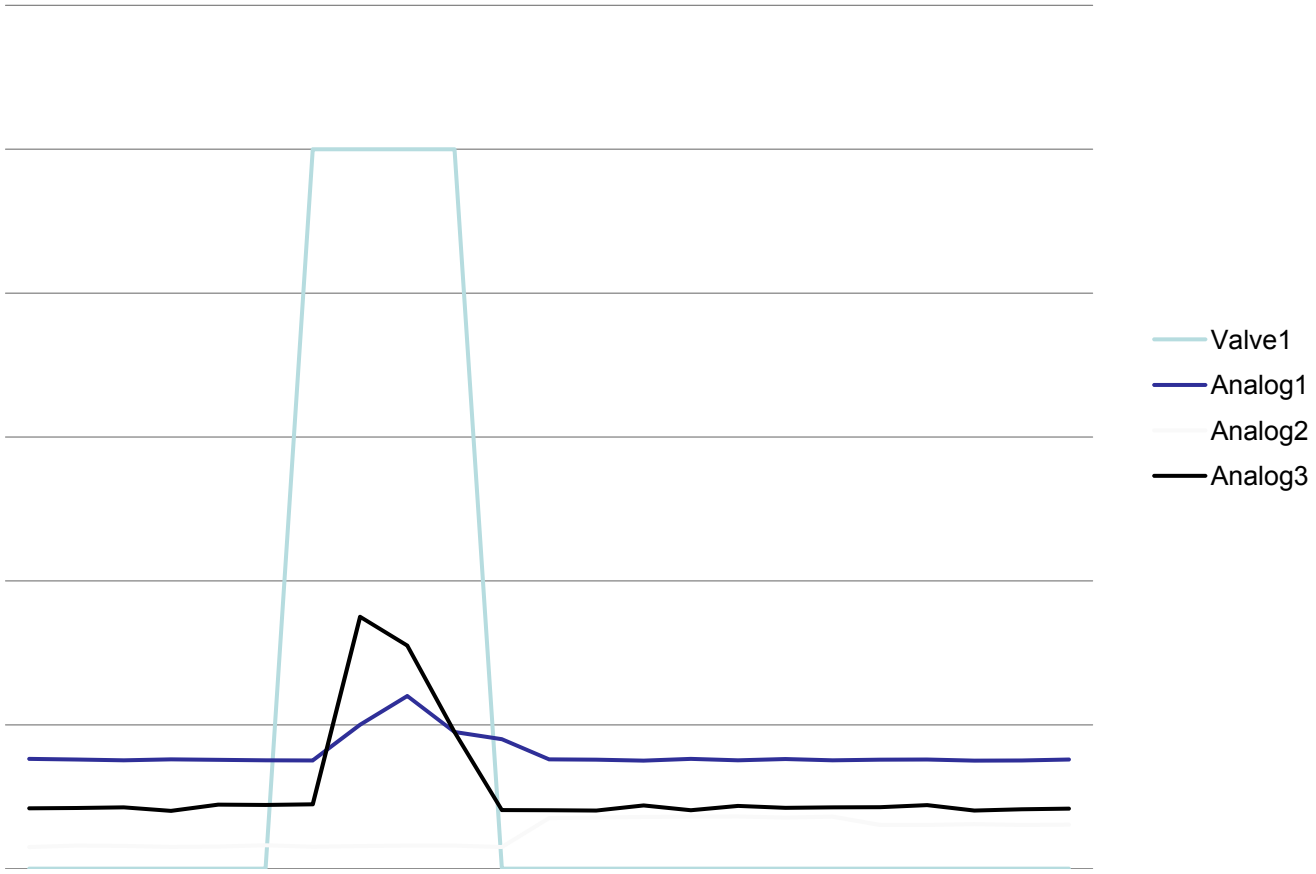


Inertial and Resonance Attacks

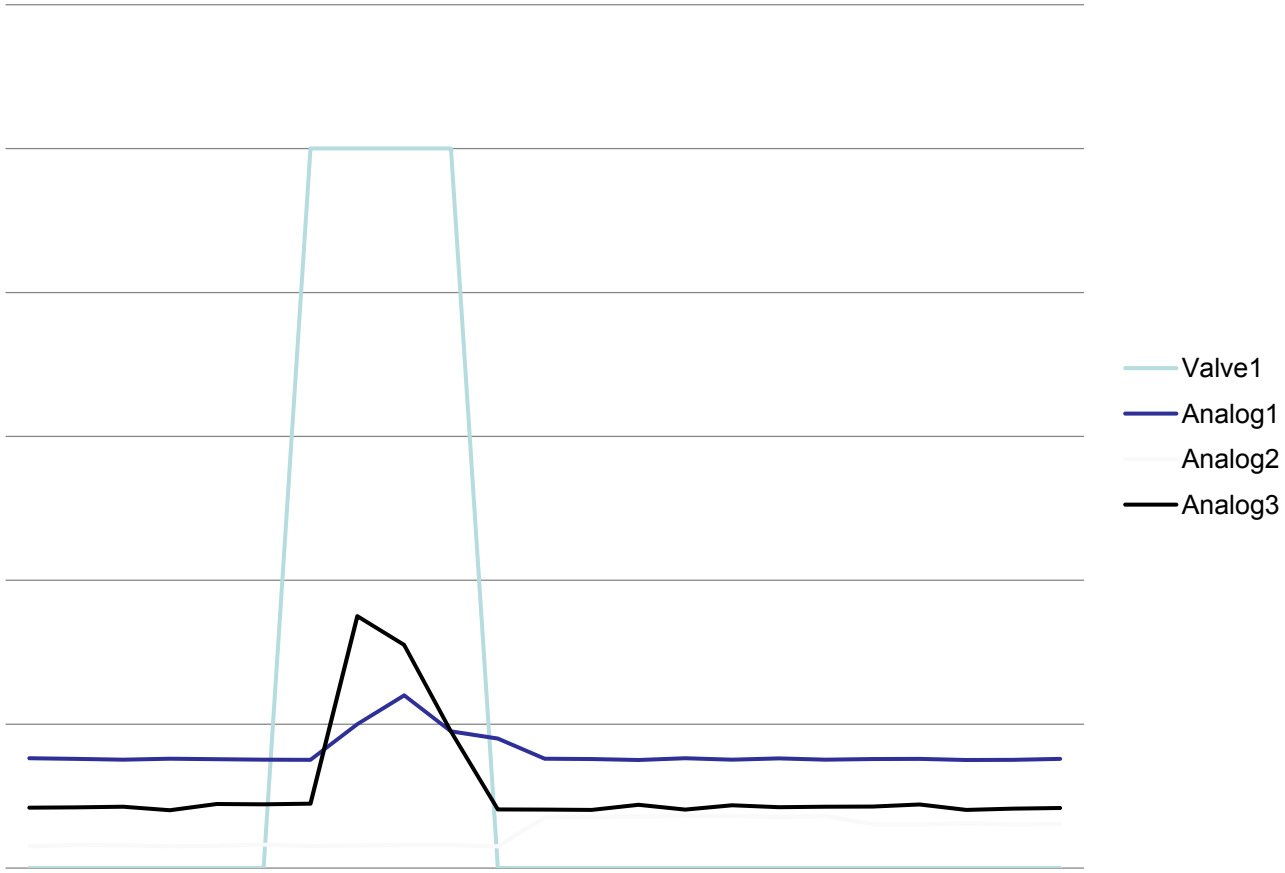
- Test a control point
- Look for indications
- Maximize the indications

The test hit

- Pick a point to manipulate and manipulate it



Looking For Indications



Maximizing the Indications

- Other inputs you control may change the height of the peaks
- If two inputs produce peaks in the same values, they can be synchronized to produce waveform addition
- Fast-moving values more often lead to breakage
- Don’t get stuck on a single peak—often breakage occurs where you least expect it

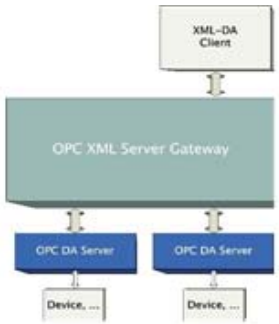
Physical Damage

- Engineers try to take into account all the things that can go wrong in a process
- This is no different than searching for buffer overflows in code
- You're looking for something the engineer missed

Where do we have to be?

- How deep into the system you need to hack depends on two factors
  - How fast you need to manipulate the point
  - What layers of the system perform sanity checks

Where do we have to be?



The Defenders

- If physical damage isn't instantaneous, the personnel running the process may try to stop the attacker
- As far as I know, no experimental data exists on the response time of the defenders

The Defenders

- Attackers can easily change the state of the defender's display
- Defenders are often in noise-controlled offices, per OSHA
- Diversion???

Why Study Physical Damage?

- The current assumption is that the attacker will be stopped at the firewall
  - That really hasn't happened
- Current thread models only consider the process under malicious control doing what it was meant to do

Why Study Physical Damage?

- The worst-case scenario is physical damage to the process
- Hopefully, by understanding the worst case we can come up with a list of physical safeguards that need to be in place

Questions?

- Jason Larsen
- IOActive