Éireann Leverett
@blackswanburst

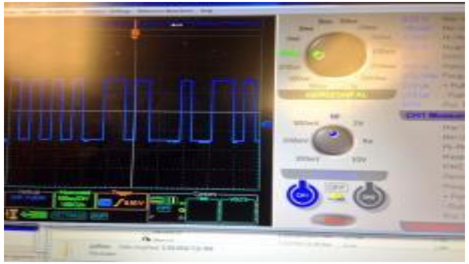
Can a hacker damage a power plant, and is it likely?

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Senior Risk Researcher @ Centre for Risk Studies
Founder @ Concinnity Risks

I’ve been around the block.



Can a hacker damage a power plant?

“The future is old, it isn’t anything new.”

- Ridley Scott

“Hegel was right when he said that we learn from history that man can never learn anything from history.”

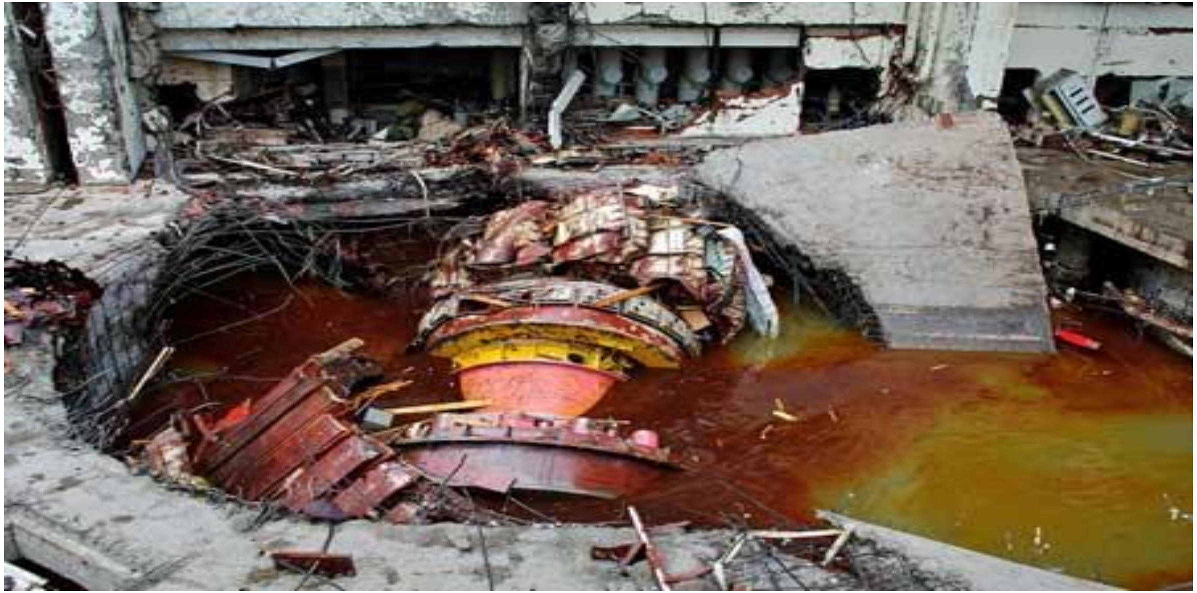
- **George Bernard Shaw**

Let’s be methodical, to make this easy.

- If you’re not hackers, splitting this into multiple questions is easier, conceptually:
  - Can power plants be damaged by accident?
  - What about safety systems?
  - Can an engineer damage a power plant through malicious acts on the engineering computers?
  - Can safety systems be bypassed?
  - Can a hacker or malicious code get access to the engineer’s computer?
  - In summary, our systems are designed to protect against…

Can power plants be damaged?

- **Sayano-Shushenskaya hydroelectric**
  - 17 August 2009
  - Water Hammer tears turbine out of the floor
  - 9/10 Turbines destroyed control room flooded
  - 75 killed



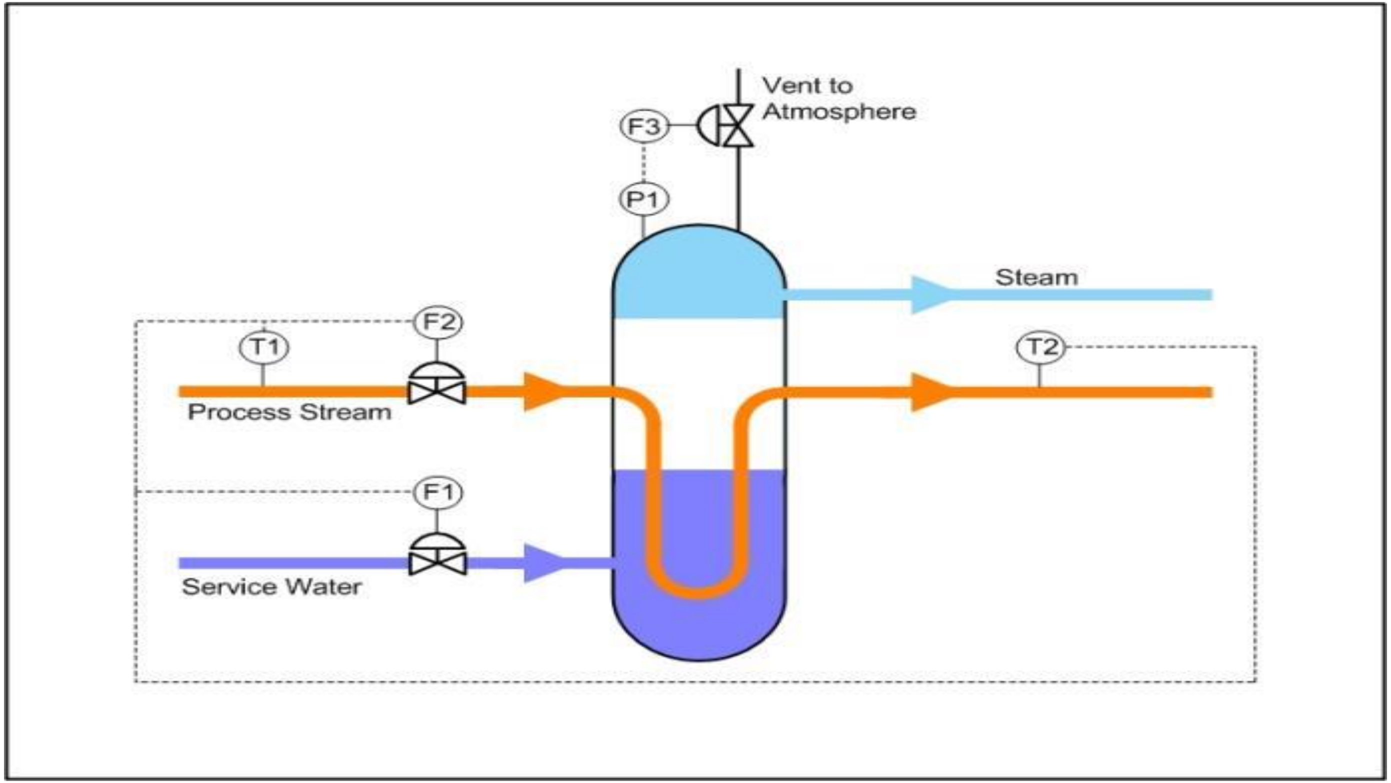
What about safety systems?

IF T2 > 200 ˚C,
THEN F1 = 30 gal/min

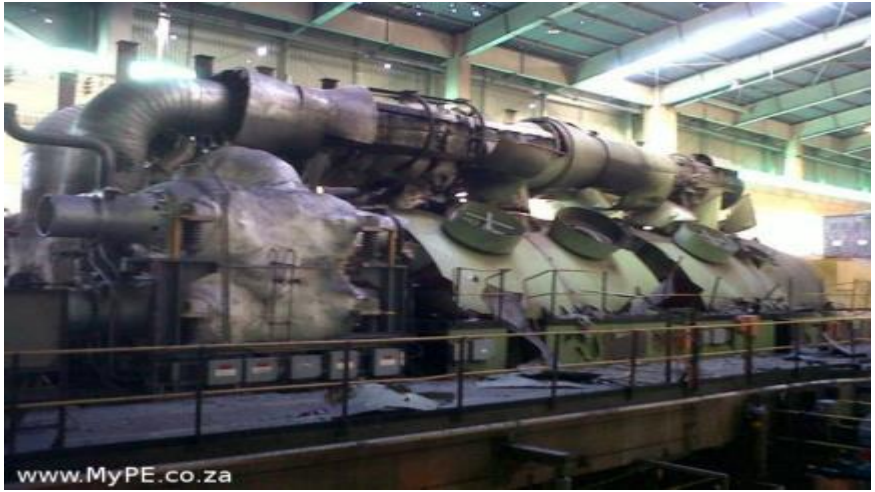
IF T2 < 100 ˚C,
THEN F1 = 10 gal/min

IF P1 > 150 psi,
THEN open F3

IF T1 > 350 ˚C,
THEN F2 = 2 gal/min



Can a clumsy engineer cause damage via a computer?



We have precious few cases of engineers maliciously damaging systems in peacetime. However, we can still use safety reports from accidents to sense how bad it could be. The pictures above depict the impact of when a generator “overspeeds”.

It exceeds it’s safe operating RPM. Every generator has a limit of this type.

Can a malicious engineer cause damage via a computer?

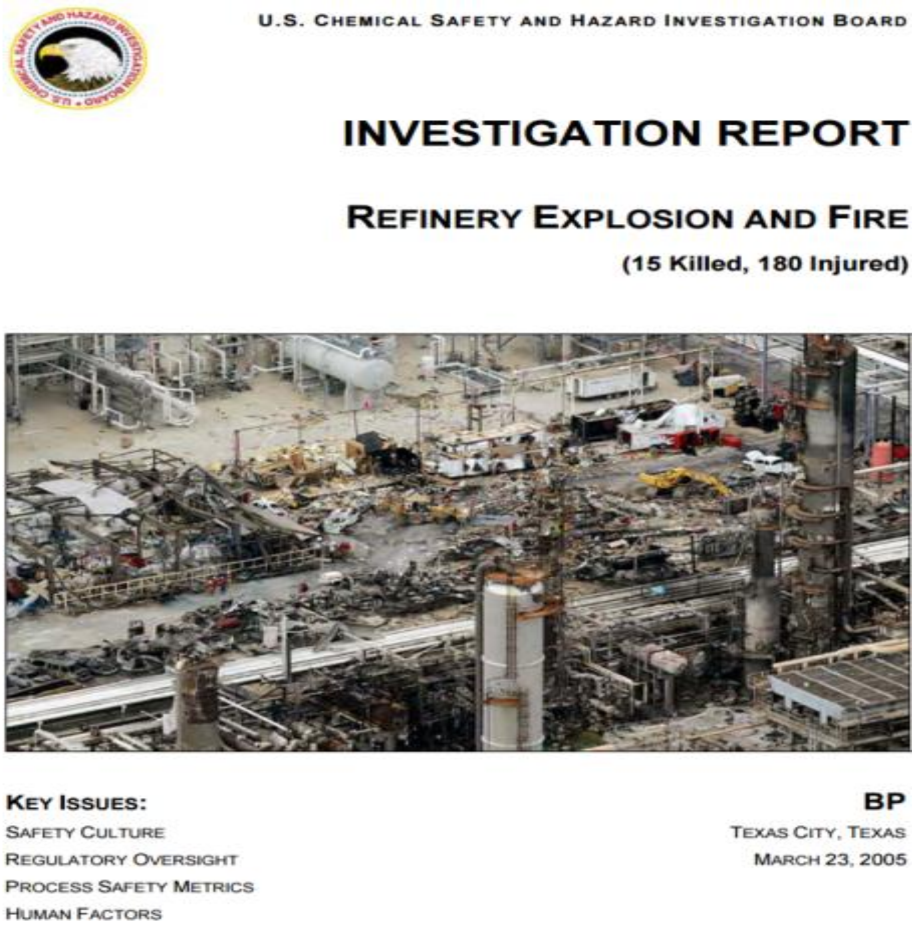
We'll examine one case of a malicious engineer later.

However, you can google "human factors" "safety incident" to see that reaction time and decision making are key factors.

In particular, the Texas City BP incident. Multiple sensors failed to report correct values, and an accident occurred.

Engineers using faulty data failed to prevent a major disaster.

What if you could manipulate that data…



U.S. Chemical Safety and Hazard Investigation Board

INVESTIGATION REPORT

Refinery Explosion and Fire

(15 Killed, 180 Injured)

Key Issues:
Safety Culture
Regulatory Oversight
Process Safety Metrics
Human Factors

BP
Texas City, Texas
March 23, 2005

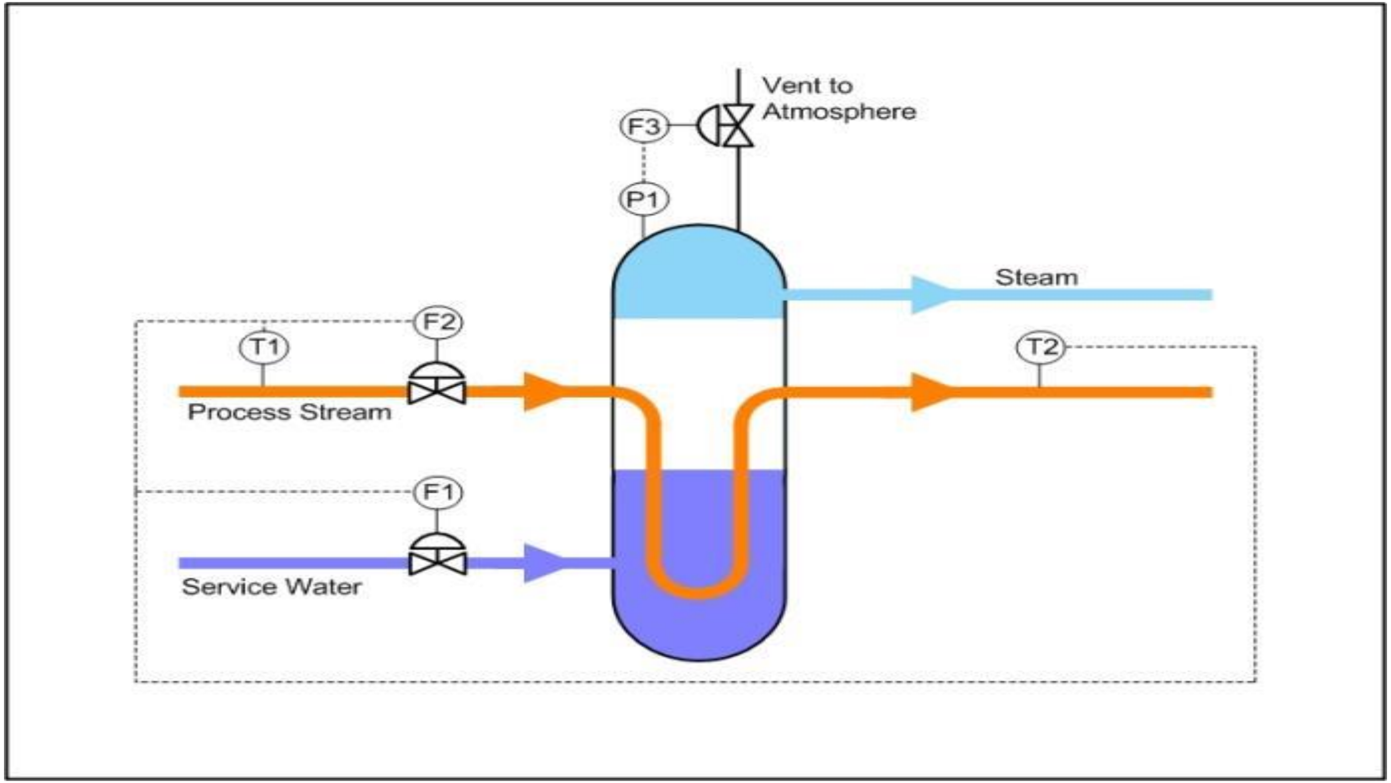
Is it possible to bypass safety systems?

IF T2 > 200 ˚C,
THEN F1 = 30 gal/min

IF T2 < 100 ˚C,
THEN F1 = 10 gal/min

IF P1 > 150 psi,
THEN open F3

IF T1 > 350 ˚C,
THEN F2 = 2 gal/min



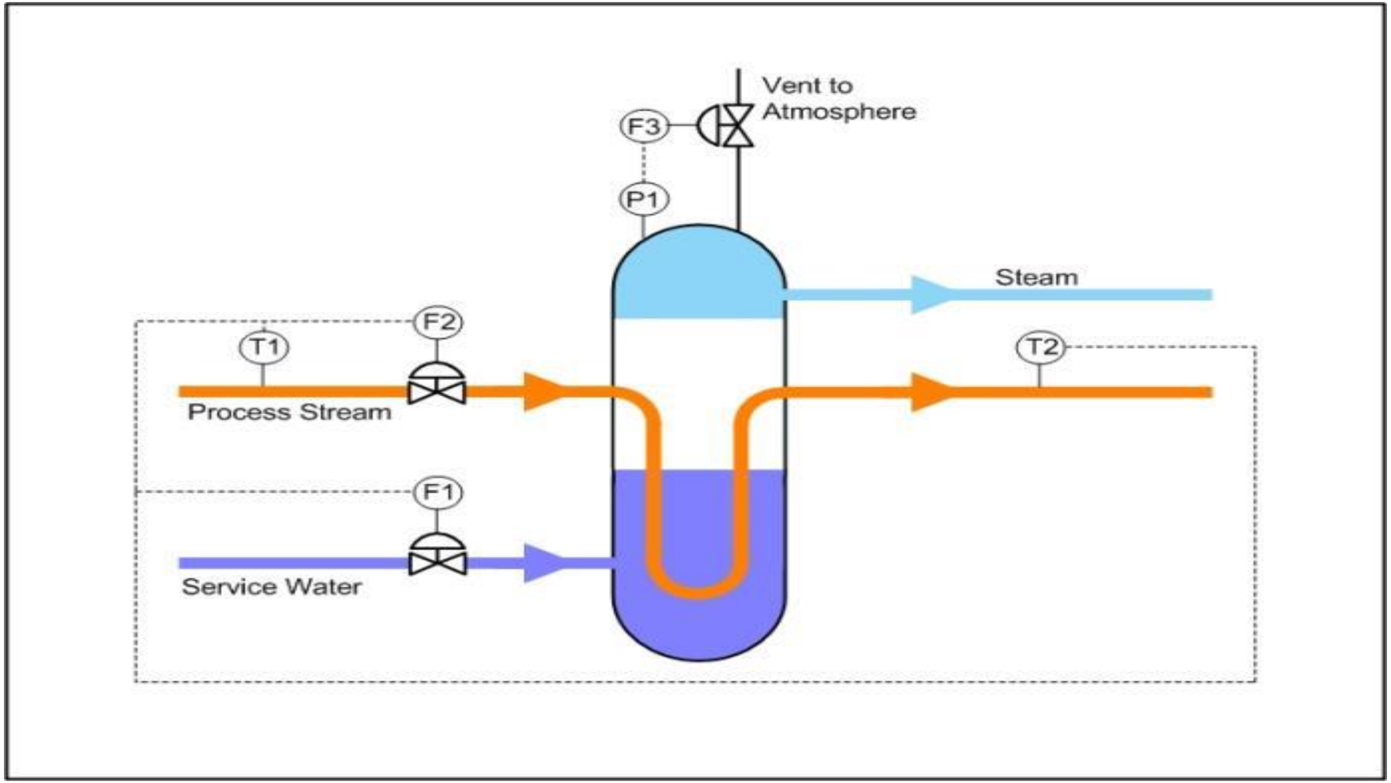
Change the logic

IF T2 > 200 ˚C,
THEN F1 = 30 gal/min

IF T2 < 100 ˚C,
THEN F1 = 10 gal/min

IF P1 > 150 psi,
THEN open F3

IF T1 = 350 ˚C,
THEN F2 = 2 gal/min



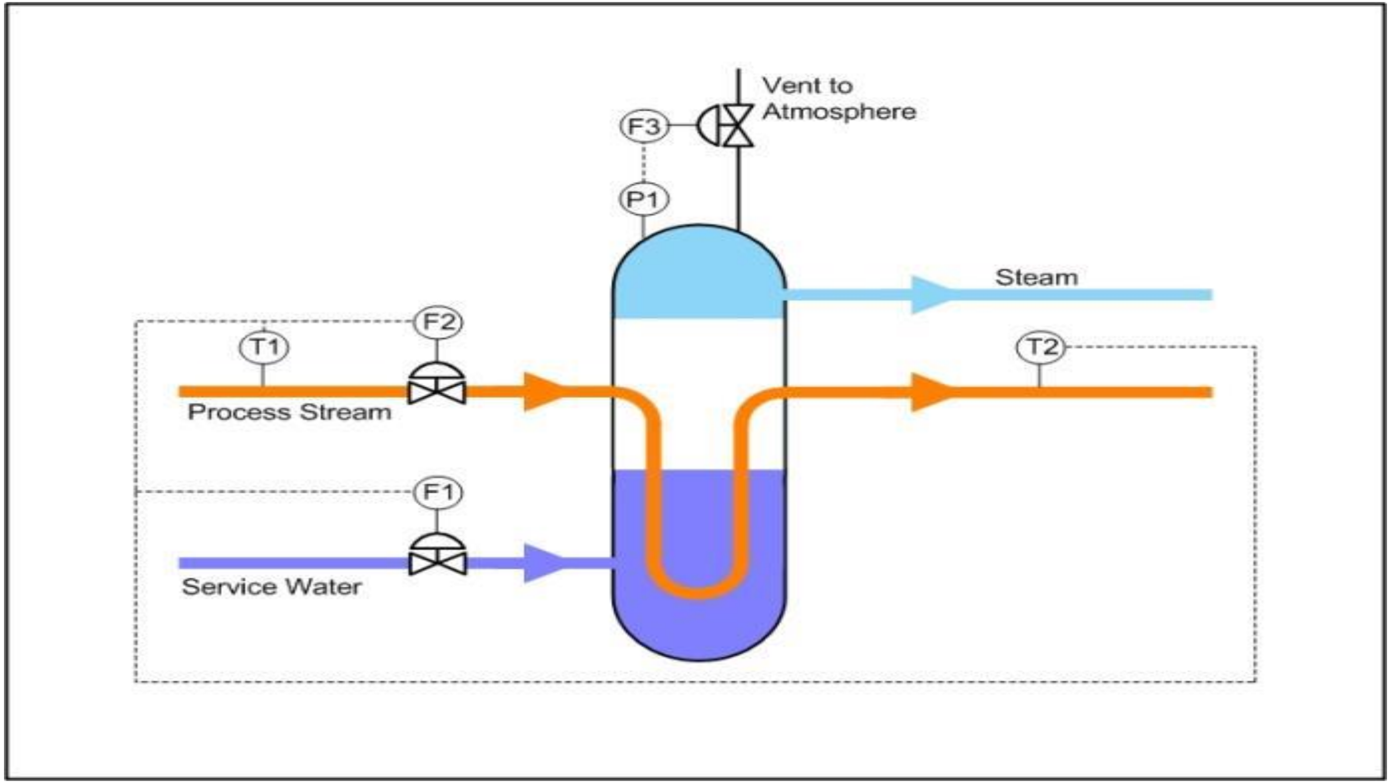
Change the limit

IF T2 > 200 ˚C,
THEN F1 = 30 gal/min

IF T2 < 1000 ˚C,
THEN F1 = 10 gal/min

IF P1 > 150 psi,
THEN open F3

IF T1 > 350 ˚C,
THEN F2 = 2 gal/min



UNIVERSITY OF CAMBRIDGE
Judge Business School

Centre for
Risk Studies

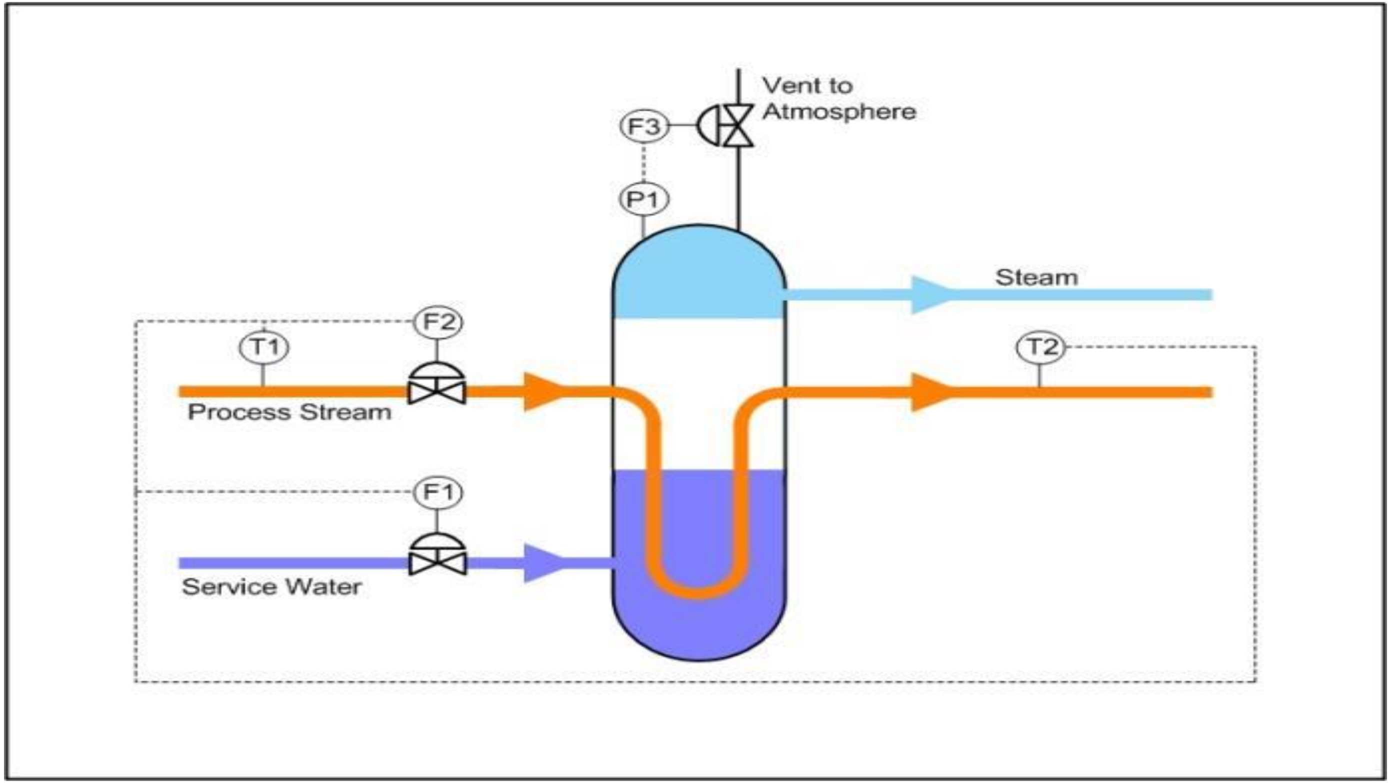
Change the sensor value

IF T2 > 200 ˚C,
THEN F1 = 30 gal/min

IF T2 < 100 ˚C,
THEN F1 = 10 gal/min

IF 50 > 150 psi,
THEN open F3

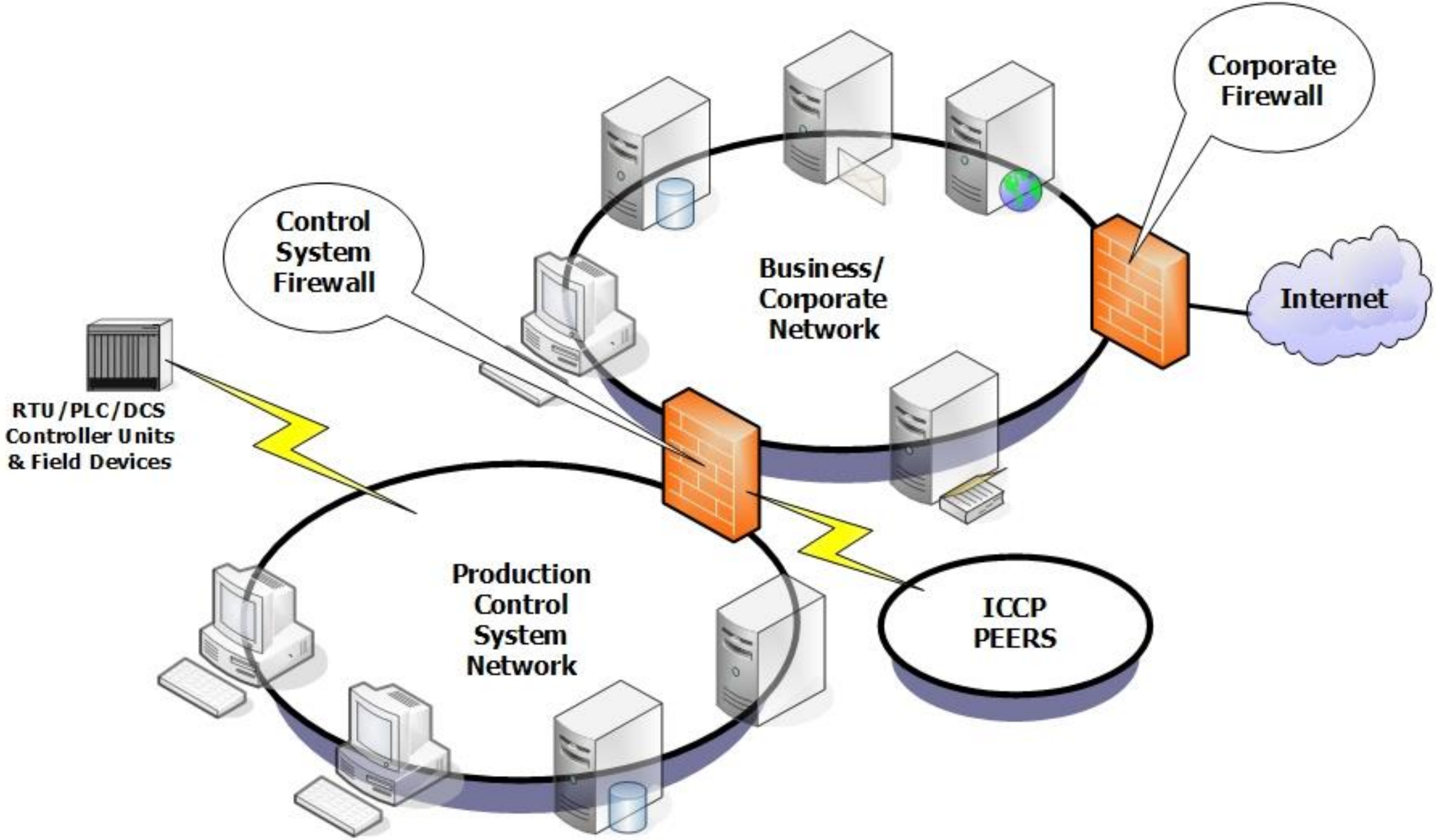
IF T1 > 350 ˚C,
THEN F2 = 2 gal/min



Modern pressure sensors…

- Firmware
- Calibration
- Scalars
- Connectivity

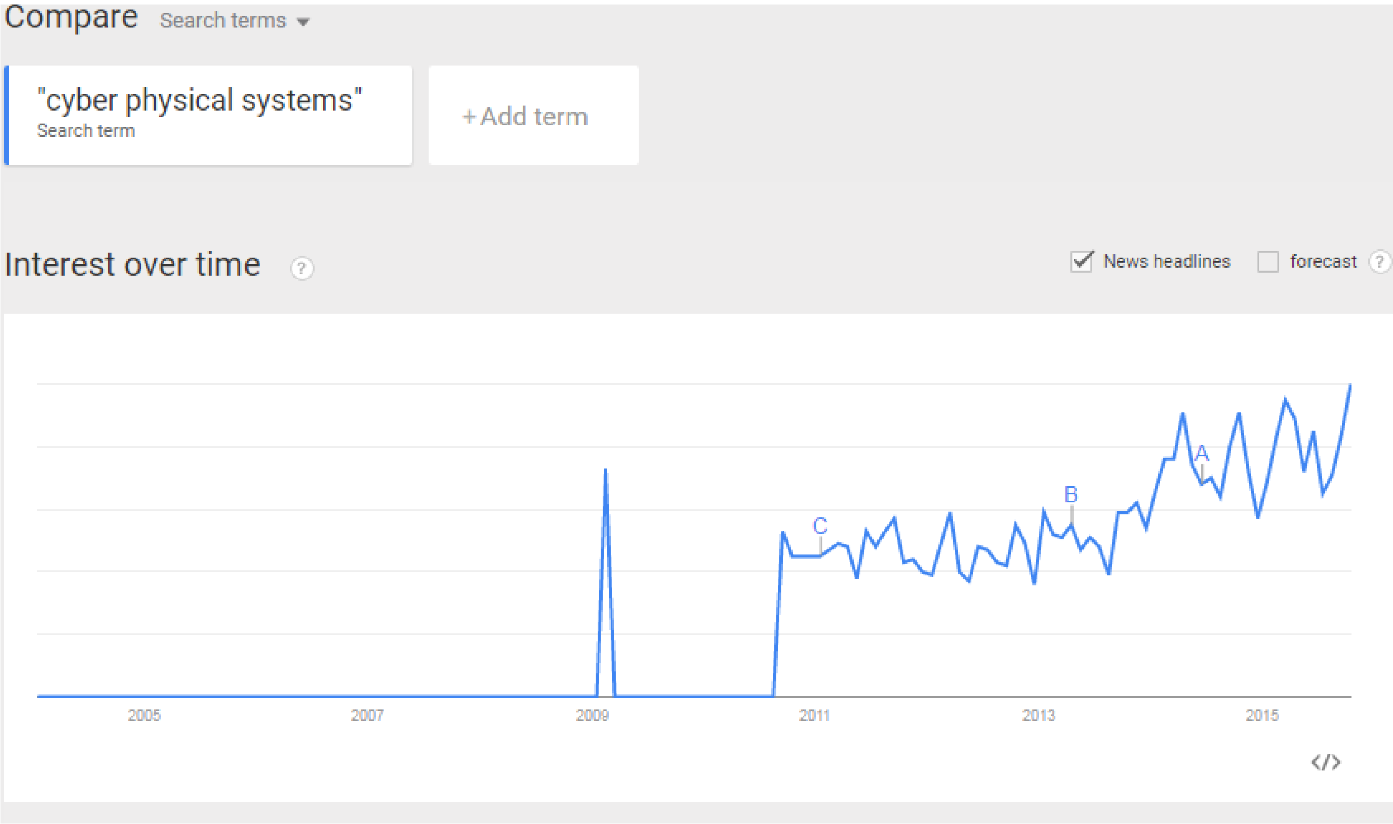
Is it possible to get access?


Corporate Firewall
Control System Firewall
Business/ Corporate Network
Internet
RTU/PLC/DCS Controller Units & Field Devices
Production Control System Network
ICCP PEERS

What does academia say? Is it theoretically possible?

- Fire and Explosions in Substations (Allan, Fellow, IEEE, 2002)
- Using Hybrid Attack Graphs to Model CyberPhysical Attacks in the Smart Grid (Hawrylak et al, IEEE, 2012)
  - “The example case presented in this paper consists of a transformer (Transformer_A) in a substation that is attacked causing it to overheat.”
  - “This will result in load being shifted to alternate paths and could lead to a cascading failure or blackout.”
- A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid (Liu et al, IEEE, 2014)
- The Potential For Malicious Control In A Competitive Power Systems Environment (DeMarco et al, IEEE, 1996)
- Modelling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information (Srivastava, 2013)
  - “Finally, devices within an ESP may be compromised intentionally by an individual with authorized physical access.”

Mentions of cyber physical systems over time



Compare Search terms ▾

"cyber physical systems"
Search term

+ Add term

Interest over time ?

☑ News headlines □ forecast ?

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Maroochyshire, Feb-April 2002

Threat Type: Insider Attack

Motivation: Revenge

Goal: Sabotage

Methodology: Man in the middle over radio

- **Attack details**
  - Equipment stolen from previous employer
  - Exacted revenge on previous employer and Maroochyshire council for rejecting his application.
  - Sabotaged radio communications on at least **46 occasions**
  - Resulted in **800k gallons of sewage** spilled in parks, rivers, etc.

- **Lessons learned**
  - It's not easy to catch an insider
  - Insider attacks are less frequent but higher impact
  - Incident Response and Forensics are key capabilities

Daimler-Chrysler, August 2005

Threat Type: Zotob Worm
Motivation: Spyware Installation ($)
Goal: Infection
Methodology: MS05-039 Plug-n-Play

- **Attack details**
  - Zotob worm knocked **13 plants offline.**
  - ca. 50,000 workers stranded
  - Vehicle production stalled for ca. 1 hour at some plants
  - $14 million in downtime cost
  - Impact on 3rd party support connections

- **Lessons learned**
  - Network segmentation/segregation is important
  - Viruses **can** impact ICS infrastructure (ISA99 Zones and Conduits addresses this concern)
  - You’re part of an eco-system, everybody bears responsibility

Brown’s Ferry Nuclear Plant, August 2006

Threat Type: Slammer Worm (+3 Years)
Motivation: N/A
Goal: Non-ICS targets
Methodology: Buffer Overflow

- **Attack details**
  - **Slammer worm** side-effects made operators initiate manual ‘scram’ procedure because of loss of recirculation flow resulting in a **‘high power, low flow’ condition**
  - Loss of recirculation is a serious condition under which operation is not permitted.
  - $600k cost in downtime alone

- **Lessons learned**
  - Non-ICS malware can impact ICS infrastructure.
  - Airgapping delays infection but patching still required

Harrisburg PA Water Plant, October 2006

Threat Type: Targeted Threat Agent
Motivation: Mischief
Goal: Set up a cheap server to run online games
Methodology: Compromised laptop

- **Attack details**
- Foreign actors compromised employee laptop.
- Used as pivot point into the company network
- Looking for **systems to 'repurpose' for file sharing, spam**, …

- **Lessons learned**
- Press is faster/as fast as law enforcement
- Threat agents don't discriminate ICS from non-ICS
- International incidents happened long before Stuxnet
- An international collaborative framework is needed

Tehema Colusa Canal Authority, August 2007

Threat Type: Insider Attack
Motivation: Disgruntled Employee
Goal: Criminal Damage
Methodology: Trojan

- **Attack details**
  - Disgruntled employee installed unauthorized (malicious?) software on SCADA systems controlling irrigation.
  - **Charged in 2007, charges dropped in 2011.**

- **Lessons learned**
  - Forensics is slower than incident response
  - Focus on IR first, Forensics later
  - Revisiting past incidents brings new insights
  - The line between attack and accident is thin and blurry

Lodz, January 2008

Threat Type: Targeted Threat Actor
Motivation: Mayhem
Goal: Sabotage
Methodology: Altered Universal Remote

- **Attack details**
  - **Teenager customized a remote control** device that allowed him to control tram junctions in the city of Lodz.
  - **Four trams derailed**, others needed to make emergency stops leaving passengers hurt.

- **Lessons learned**
  - Distributed field devices have their own vulnerabilities.
  - Protocols over an open medium increase vulnerability.
  - Urban environments dramatically change ‘impact’.
  - Detecting the attacker may not be trivial (high cost).

E.On, Kingsnorth, November 2008

Threat Type: Targeted Threat Actor
Motivation: Environmental Protest
Goal: Sabotage
Methodology: Physical Penetration

- **Attack details**

- Lone protester scaled the fence of E.ON Facility.
- Emergency Shutdown of a 500MW generator
- Site team responded **“quickly and professionally to control situation”.**

- **Lessons learned**

- Physical Security matters!
- Incident **Response** is a key asset.
- Intruder was never caught.

Pacific Energy, May 2008

Threat Type: **Disgruntled Employee**
Motivation: **Revenge**
Goal: **Sabotage**
Methodology: **Disabling Alarms Systems**

- **Attack details**
  - Disgruntled **former IT Contractor** accessed systems remotely.
  - Impaired leak detection systems.
  - Resulted in **thousands of dollars** of damages
  - No environmental impact as a result of attack

- **Lessons learned**
  - Basics (e.g. Access Control) are important.
  - 3rd parties introduce additional risk, control it.
  - Log retention for post-incident analysis is mandatory.

Dragonfly/Energetic Bear, 2011-?

Threat Type: Directed Attack Campaign
Motivation: Reconnaissance
Goal: Access/Data Exfiltration
Methodology: Phishing & Lateral Movement

- **Attack details**
  - Compromised ICS Software Vendors websites and/or software
  - **Users downloading software also got a Trojan**
  - MB Connect Line GmbH
  - eWon VPN vendor

- **Lessons learned**
  - Block access from external
  - IR team/NSM might have caught them
  - Insider trust is a risk

German Steel Mill, Before Aug 1 2015

Threat Type: Directed Attack
Motivation: Sabotage/Ransom
Goal: Access/Physical damage
Methodology: Phishing & Lateral Movement

- **Attack details**
  - Phishing emails compromised the business network
  - Emails appeared to be **from trusted source**
  - “Failures accumulated in individual control components or entire systems,”
  - “unable to shut down a blast furnace in a regulated manner” which resulted in **“massive damage to the system.”**
  - Motivation unclear

- **Lessons learned**
  - Block access from external
  - IR team/NSM might have caught them
  - Insider trust is a risk

In general how secure is the electrical industry?

- NERC CIP fines were introduced in 2005
  - Up to 1M per day for non-compliance
  - Declaring it necessary to have “an electronic security perimeter” for critical assets.
  - Basically, for 10 years we had to tell people to use firewalls
  - While modern attackers bypass firewalls with phishing
  - The fact we had to FINE people should tell you how “secure” this industry is.

Ok, fine, it’s a “soft” industry, with lots of attacks, but hacking a generator?

Conclusions

- Yes in theory.
- Yes in practice.
- We have no idea what the likelihood is.
- The historical data is very sparse.

- The history of ICS incidents must belong to society.
- http://www.risidata.com/Database

- Today's systems are resistant to murphy, not malice.
- I & my team have compromised many utilities from outside the firewall into the control room, and gained full control.
- No I will not tell you which ones or how.
- I will say the fastest was 3 days with a team of 2.

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School