Singapore University of Technology and Design

# Cyber Physical Systems: Security and Safety


**Aditya P Mathur**

Adopted from: **Aditya P Mathur**
International Workshop on Information Security (IWIS-2012)

December 15, 2012

# Questions of interest

What is a CPS?

What are the security issues in CPS and how do they differ from those in traditional information systems?

To what extent can a CPS be secured against cyber crime?

Are there some fundamental design principles that ought to be used when designing or upgrading a CPS?

What are the curricular ramifications of CPS security?

# Coverage

CPS examples and concerns, components, abstraction, incidents

Traditional versus CPS security

Industrial control systems

Two real-life incidents: Toys and Iran

Control systems: basics

Case studies: Medical devices and Irrigation Systems

CPS: design principles, research and educational needs

# Cyber Physical Systems: Examples

# Shipping

rafgarfewfsadf

Several countries and cities in the world have some of the world's busiest ports and large transshipment hubs.

For example, PSA Singapore Terminals are connected by 200 shipping lines to 600 ports in 123 countries, with daily sailings to every major port of call in the world.

# Healthcare

Singapore offers Asia's best healthcare system, and its standard of medical practice ranks among the best in the world.

The *Joint Commission International (JCI)* has accredited 11 hospitals and three medical centers in Singapore.

# Infocomm

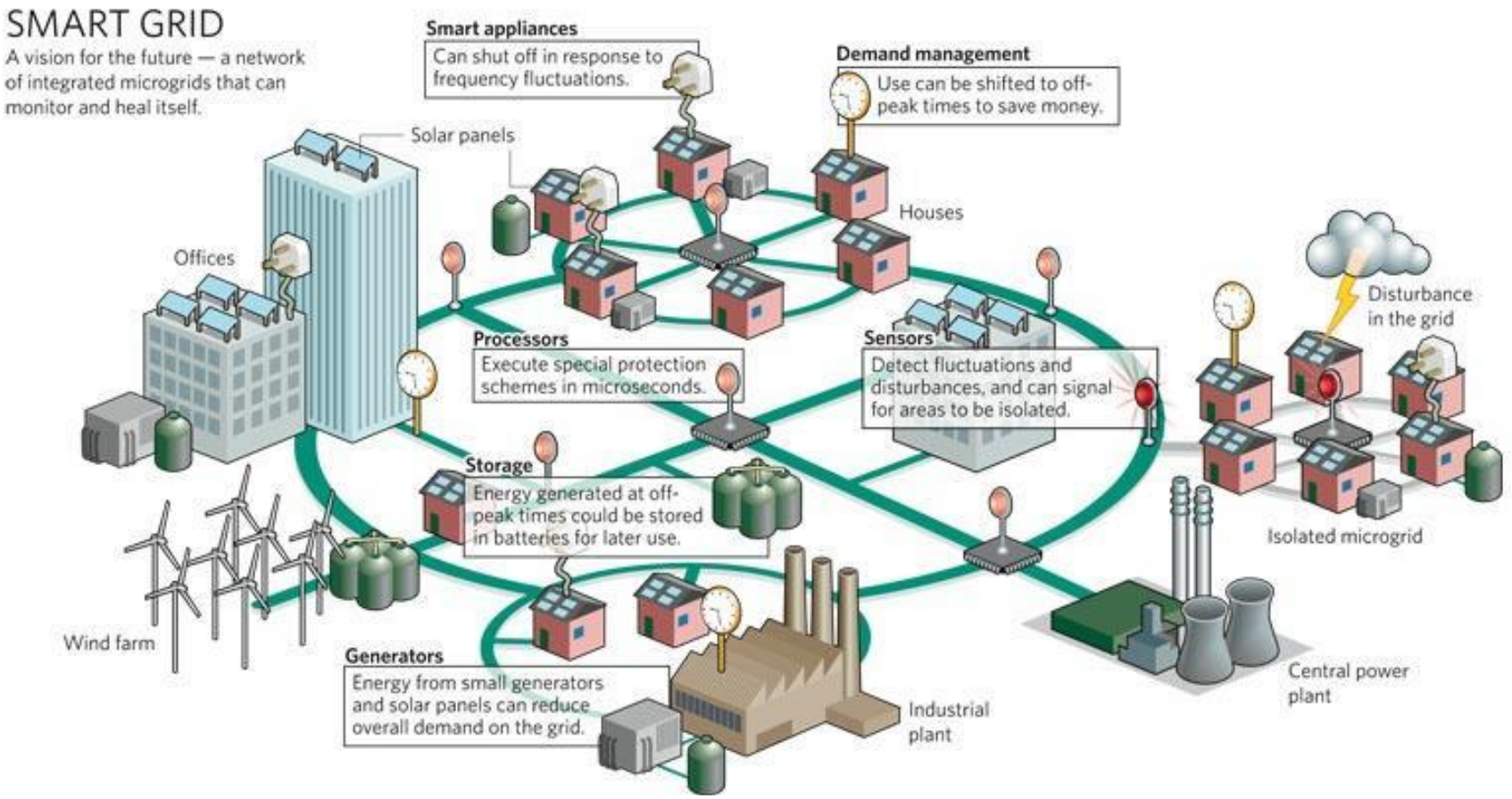
Singapore today ranks as the second most network-ready country in the world and the first in Asia, according to the World Economic Forum's Global Information Technology Report 2010/2011.

# Energy

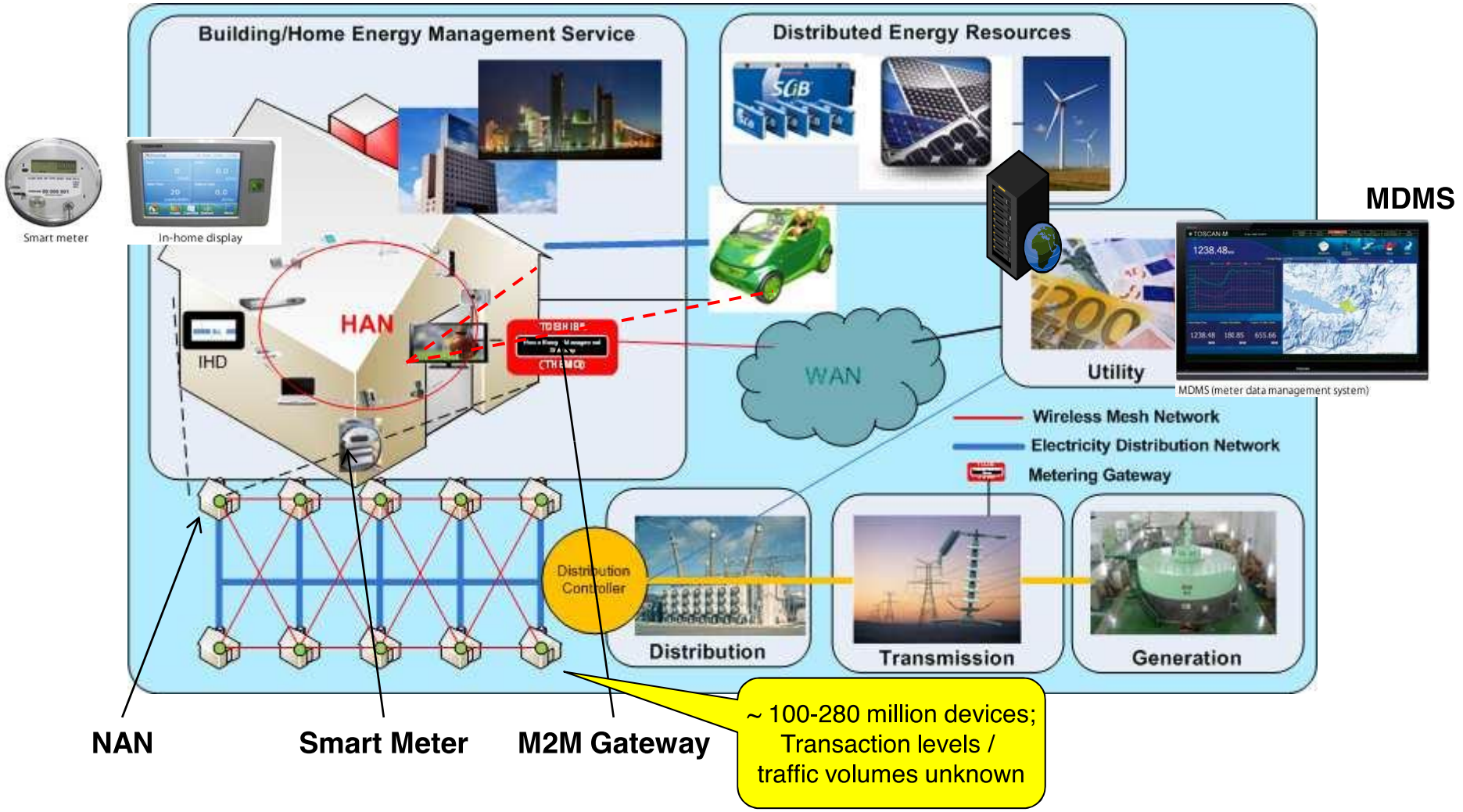
“Today, Singapore is the undisputed oil hub in Asia and is one of the world’s top three export refining centers....”

# Smart Grid - Overview

- Smart Grid : Overlay electrical grid with sensors (phasor monitoring units - PMUs) and control systems (SCADA) to enable:
  - reliable and secure network monitoring, load balancing, energy efficiency via smart meters, and integration of new energy sources



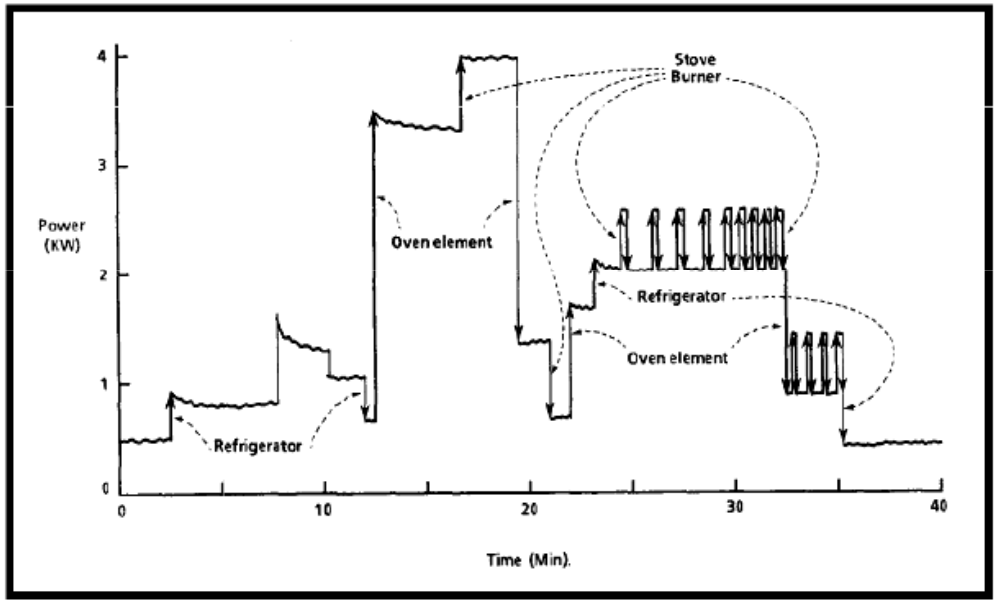
# Smart Grid – Smart Metering




Use of smart metering data for **energy management**, **load balancing**, **billing**, **DR**, **DSM**, **micro-grid management**, **new products and services**, etc.

# Smart Metering Privacy Issue (1)

- **Data usage threats against <u>Customer privacy</u>**
  - Easy to deduce patterns of home activity from high frequency metering data.
    - Which devices you own and use
    - When you use them
    - When you're at home
    - Lifestyle routines
  - Personalised services/offers, e.g. ads depending on exposed private data...




S. Drenker and A. Kader, "Nonintrusive monitoring of electric loads," in IEEE Computer Applications in Power, vol. 12, no. 4, pp. 47-51, 2002.

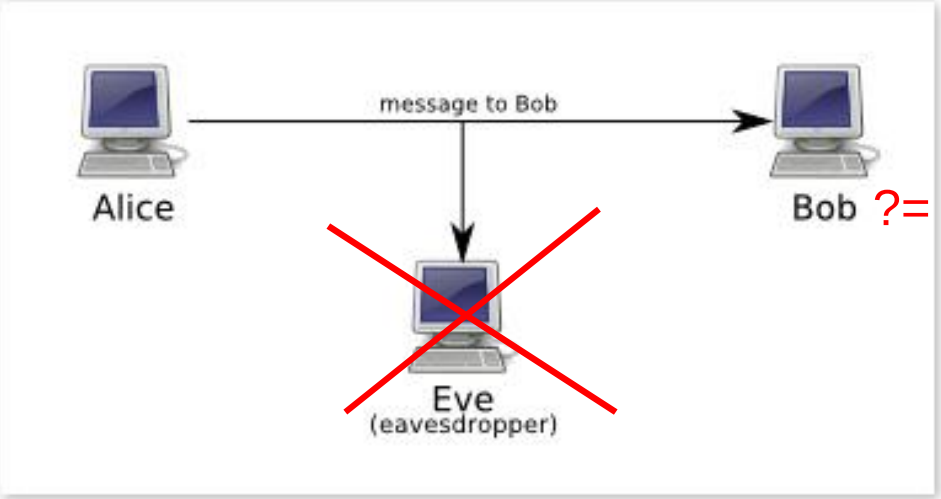
# Smart Metering Privacy Issue (2)

- **With such data exposed**
  - Who can we trust with it?
  - Malicious attacks
  - No privacy even in your own home?

- **Who should be allowed to control this, and under what kind of legal framework?**
  - Who owns / controls the data?
  - For what purpose? For how long?
  - Consent:
    - Opt-in or opt-out?

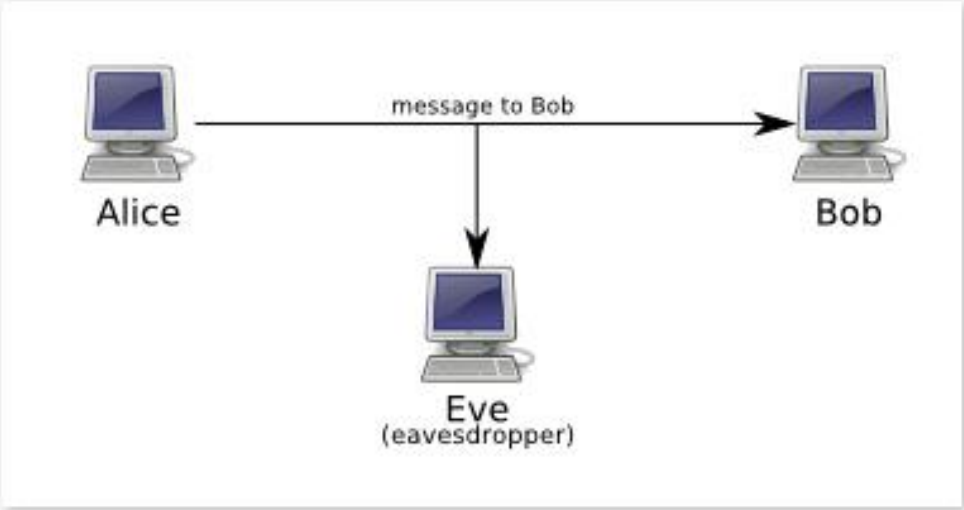
# Privacy is not Secrecy

- Privacy: the ability to prevent unwanted transfer of information (via inference or correlation) when legitimate transfers happen.
- But privacy is not secrecy!
- Privacy problem: disclosing data provides informational utility while also enabling potential loss of privacy
  - Every user is potentially an adversary
  - Encryption is not a solution!



# Privacy versus Secrecy

- Privacy: the ability to prevent unwanted transfer of information (via inference or correlation) when legitimate transfers happen.
- But privacy is not secrecy!
- Secrecy Problem: Protocols and primitives clearly distinguish a malicious adversary vs. intended user and secret vs. non-secret data.
  - Encryption may be a solution.



# Possible Solutions

- Robust Smart Metering Design with privacy constraints
- Utility-Privacy Tradeoff Design
- Privacy Invasion Detection/Prevention
- Data masking
- Data Anonymisation

# Other Potential Concerns:

# CPS Vulnerability

Are your energy, healthcare, water, shipping, transportation systems vulnerable to network attacks?

What, if any, are the vulnerabilities in such systems?

When exploited, how might such vulnerabilities affect people?

# CPS Control systems

Are the control systems in your large and critical CPSs systems robust enough to withstand deception attacks?

Are these control systems programmed to withstand denial of service attacks?

# Surviving from Physical attacks

- What happens if we lose part, or even most of the computing systems?
- Will redundancy alone solve the problem?
- How to measure and quantify of resilience of current systems?
- How to ensure high availability of CPS?

# Defending Against Device Capture Attack

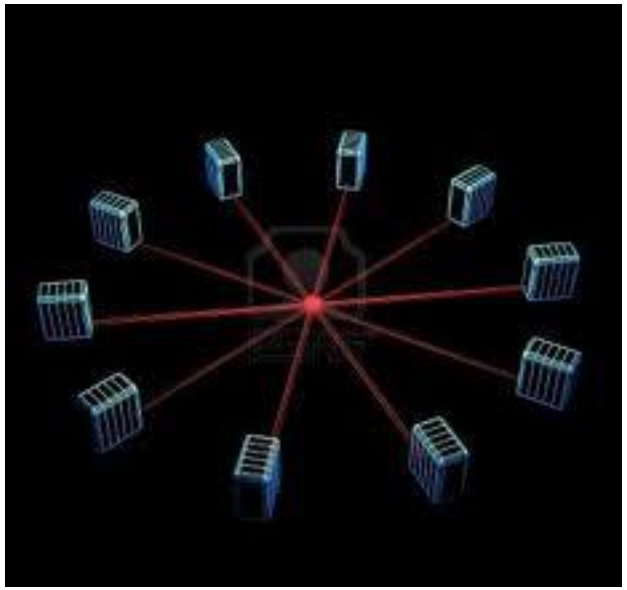
- Physical devices in CPS systems may be captured, compromised and released back by adversaries.
- How to identify and ameliorate the system damage with trusted hardware but potentially untrusted/modified software?

# Real-Time Security in CPS

- CPS often requires real-time responses to physical processes
- Little Study on how attacks affect the real-time properties of CPS
- How to guarantee real-time requirements under attack?

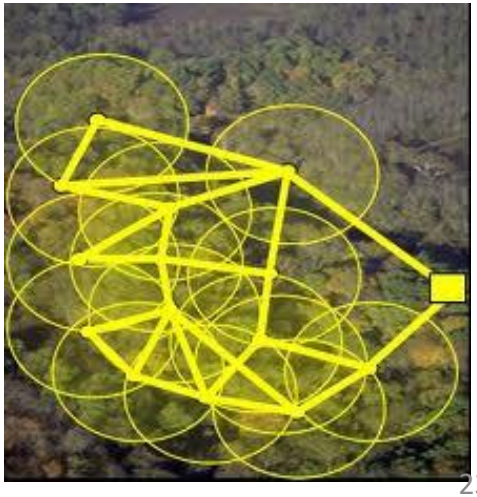
# Concurrency in CPS

- CPS is concurrent in nature, running both cyber and physical processes
- Little research on handling large-scale concurrent systems



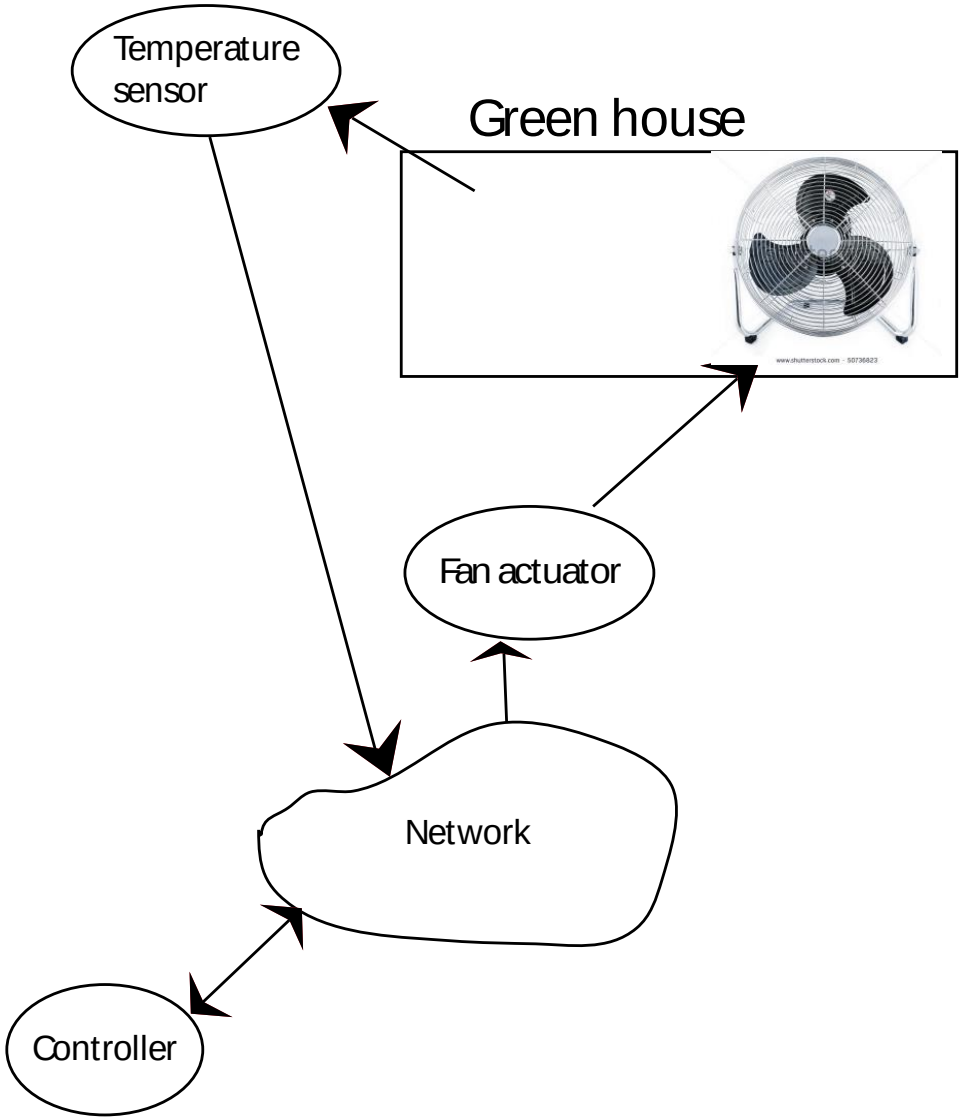
# Collaboration and Isolation

- CPS needs to effectively isolate attackers while maintaining collaborations among different, distributed system components
- How to avoid cascading failures while minimizing system performance degradation?

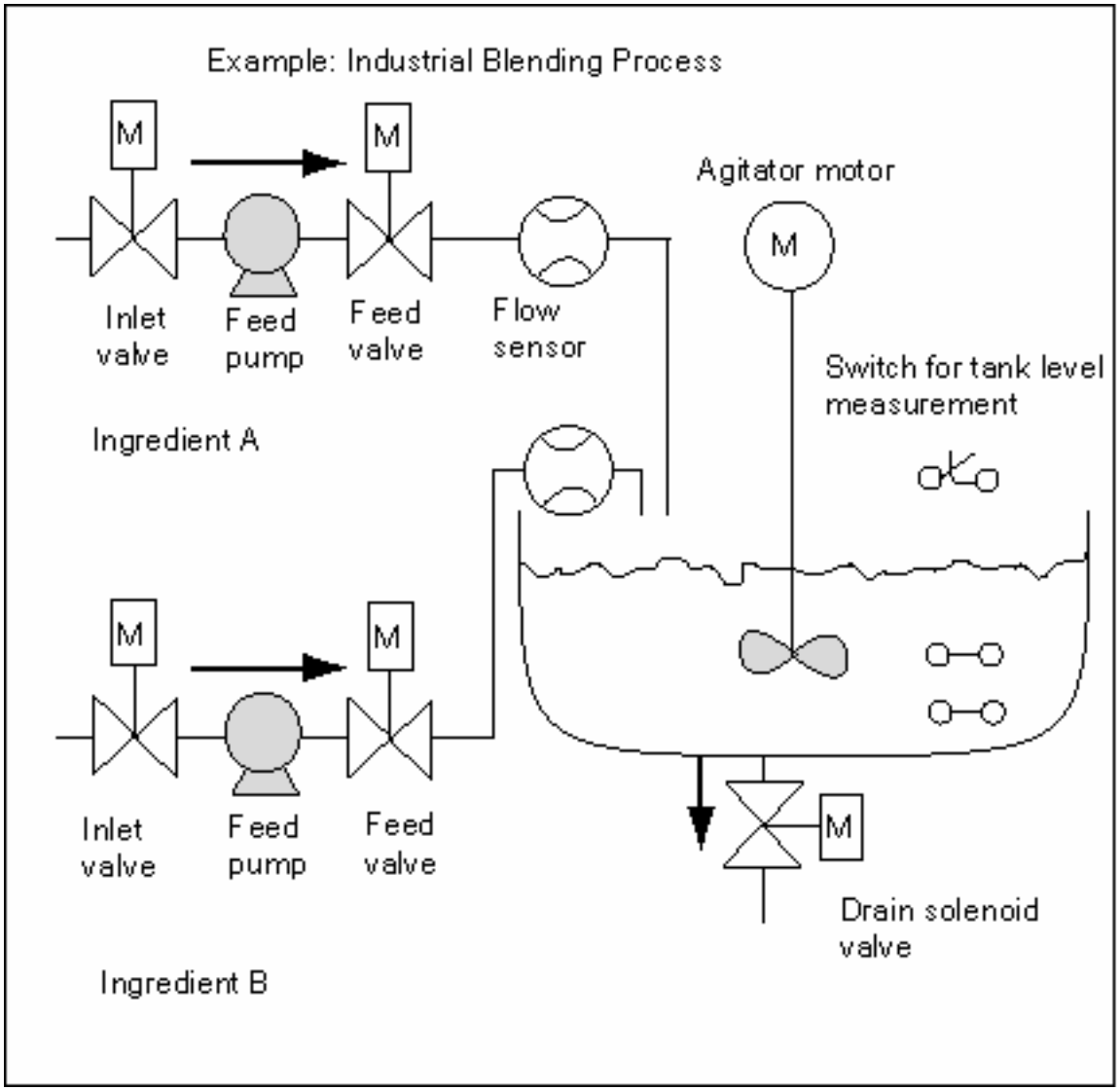


# Cyber Physical System: Components

# CPS: Greenhouse



# CPS: Blending process



# CPS Other examples

Pacemaker

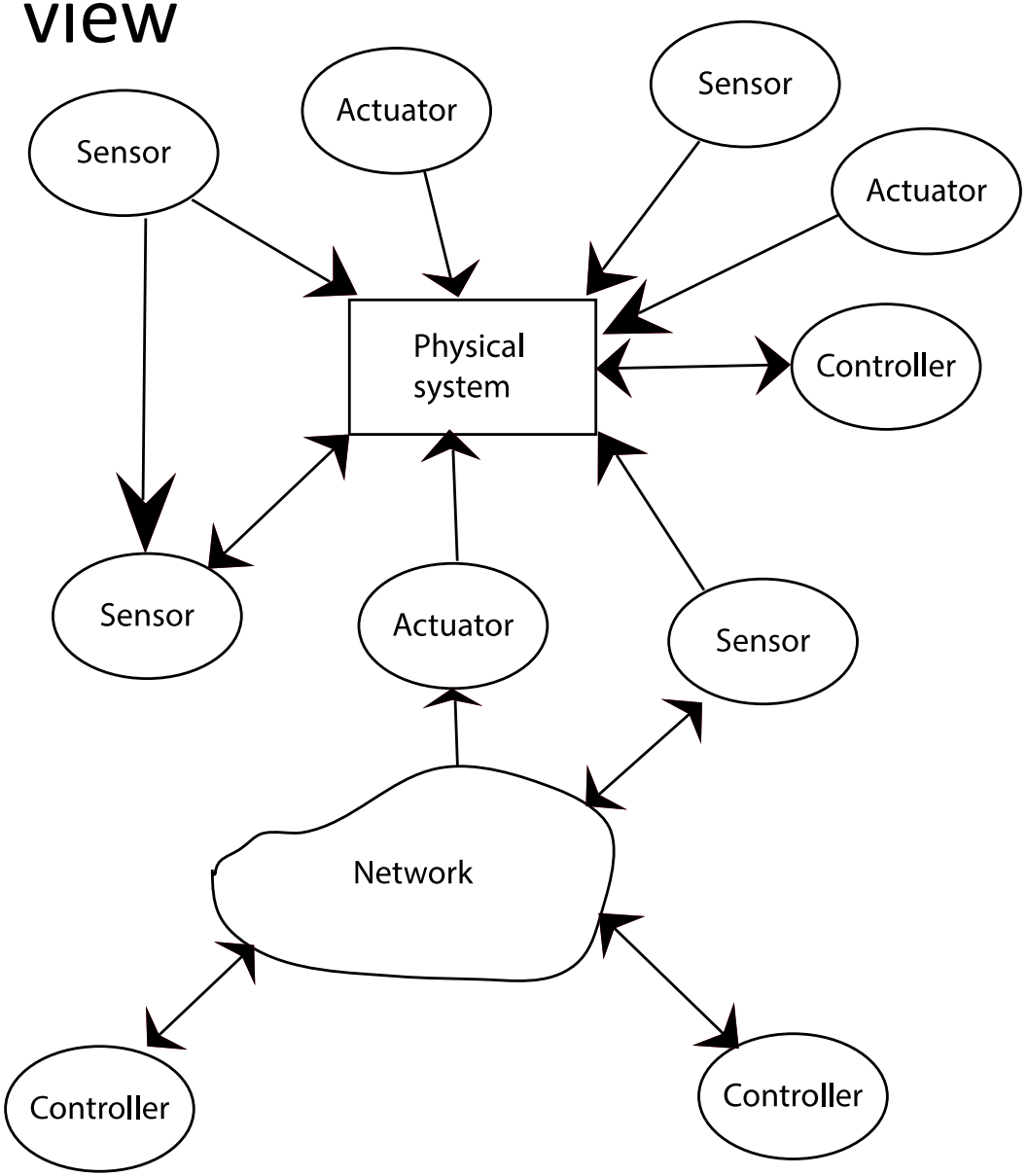
ICD (Implantable Cardiovascular Defibrillator)

Insulin pump

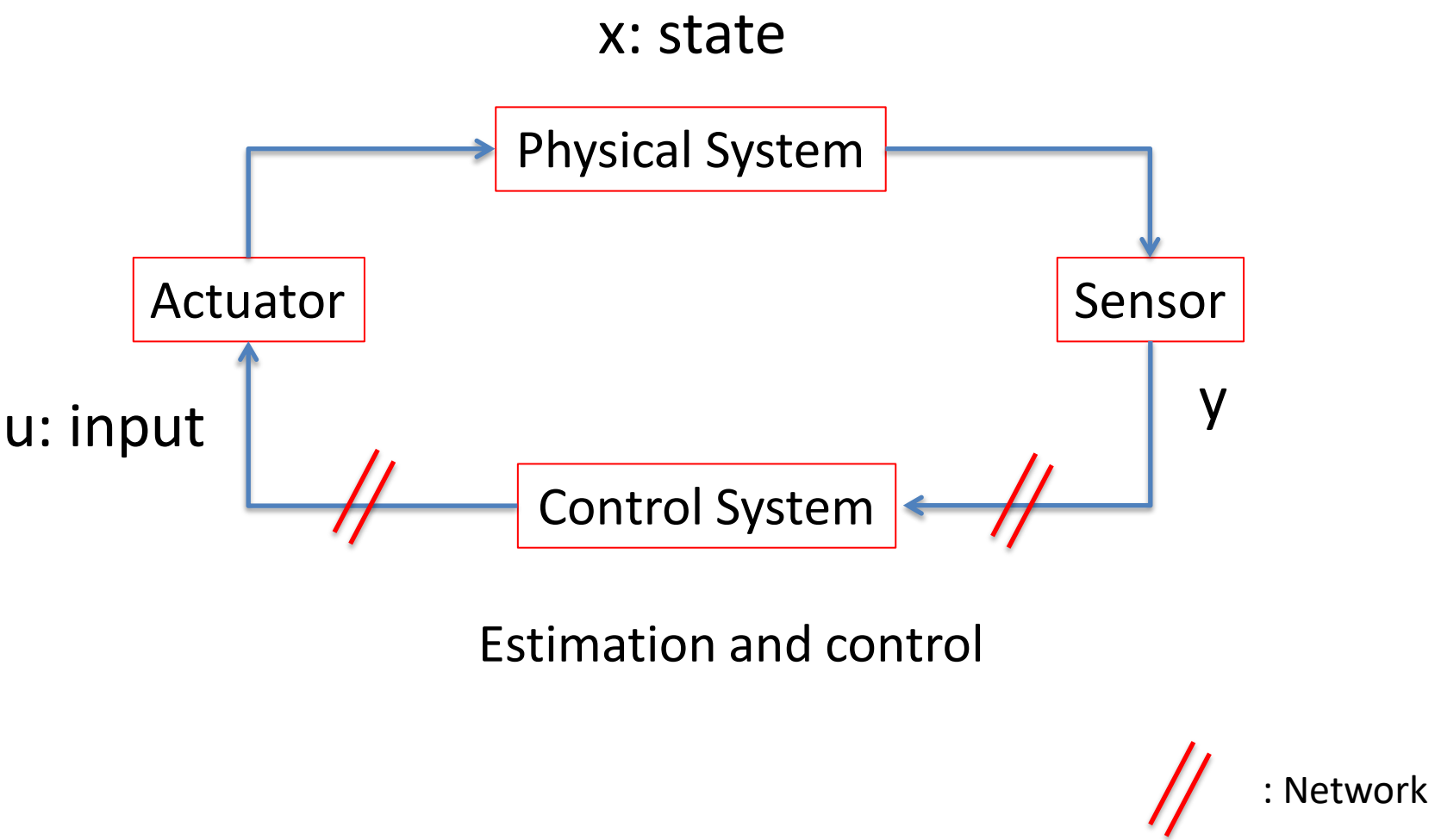
Neuro-stimulators

# Cyber Physical Systems: Abstraction

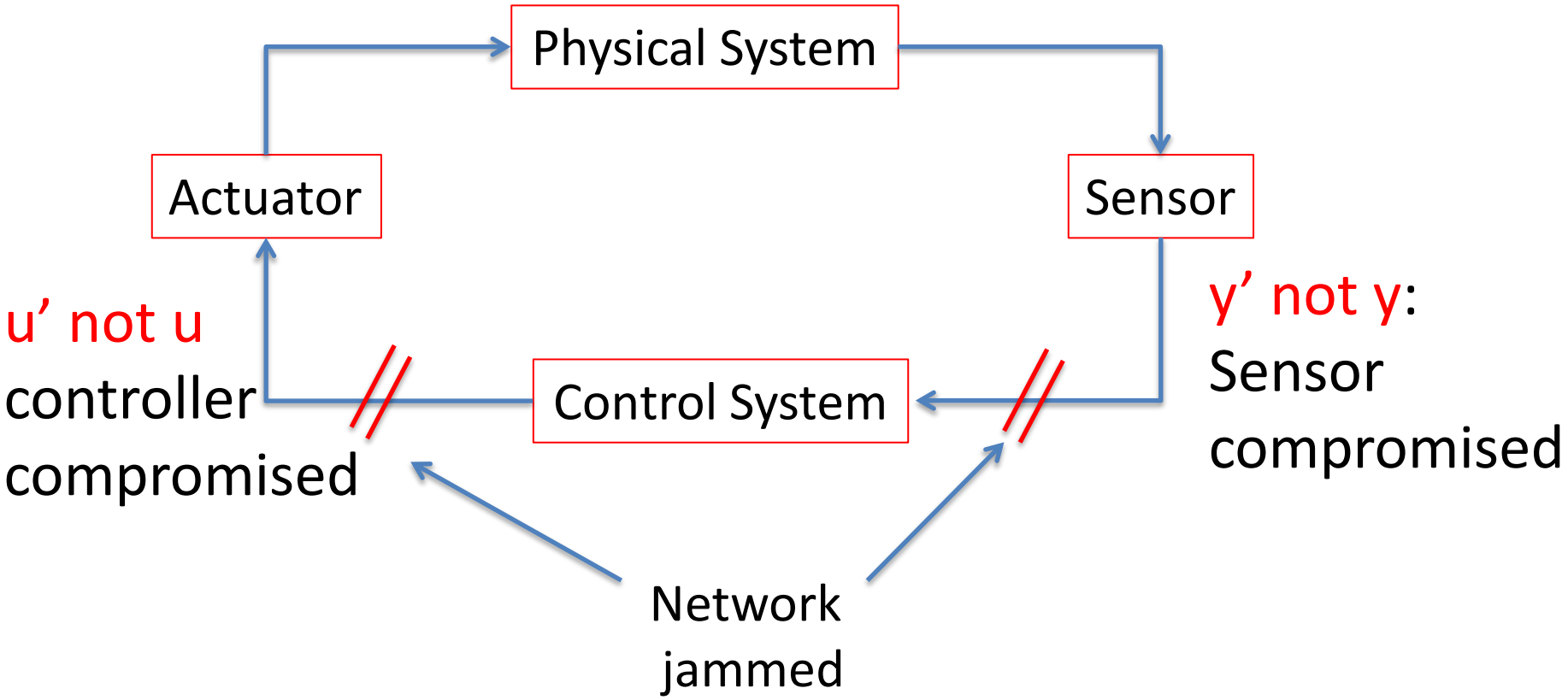
# CPS: Component view



# CPS: Systems View



# CPS Network-based Attacks



# Existing Techniques

Authentication

Digital signatures

Access control

Intrusion detection

# Enhancement of existing approaches

How deception and DoS attacks affect application layer performance (e.g., estimation and control)?

Intrusion detection and deception attacks in control systems?

What if a human is not in the loop for intrusion detection?

# CPS incident statistics

# CPS incident databases

BCIT Industry security incident database→TOFINO

http://www.tofinosecurity.com/

Wurldtech: http://www.wurldtech.com/

Cyber incidents involving control systems,  Robert Turk,

October 2005, Idaho National Laboratory, INL/EXT-05-00671

http://www.tofinosecurity.com/blog/2012-scada-security-predictions-how-did-eric-byres-do

# Sample CPS incidents

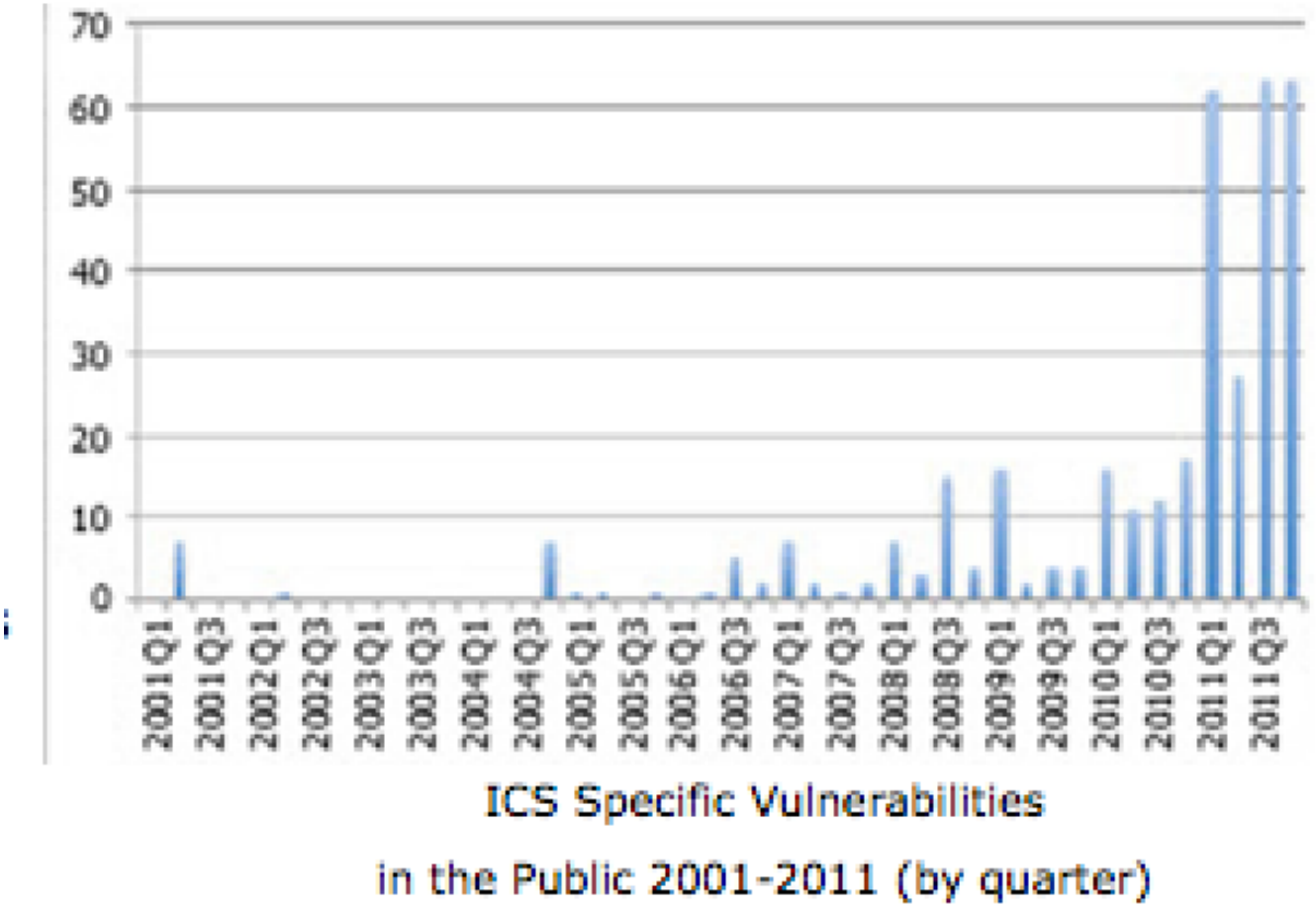
Over 500 SCADA vulnerabilities found in 2011

2010: Stuxnet [http://www.tofinosecurity.com/stuxnet-central]

2010: Night Dragon, Duqu, Nitro

Nov 2012: kAndyKAn3 worm attacks North Pole Toys

# CPS incident report statistics




ICS Specific Vulnerabilities

in the Public 2001-2011 (by quarter)

Empirical Analysis of publicly disclosed ICS vulnerabilities since 2001" by Sean McBride

# CPS incident (more) statistics

42% of all incidences were conducted by means of mobile malware

61% of the perpetrators originated from external sources

43% of perpetrators were malware authors

# Traditional versus CPS security

# Traditional

Confidentiality: Ability to maintain secrecy from unauthorized users.

Integrity: Trustworthiness of data received; lack of this leads to deception.

Availability: Ability of the system being accessible

# CPS

Timeliness: responsiveness, freshness of data

Availability: unexpected outages

Integrity: genuine data displayed and received by the controller

Confidentiality: Information regarding SCADA not available to any unauthorized individual

Graceful degradation

Ref: A Taxonomy of Cyber Attacks on SCADA Systems, Zhu et al., UC Berkeley.

# Industrial Control Systems

# SCADA

Supervisory Control and Data Acquisition System

It is an industrial control system that consists of RTUs, PLCs, and HMIs to control an industrial process.

Use: Manufacturing, power generation, fabrication, oil and gas pipelines, etc.

# RTU

Microprocessor controlled Remote Terminal/Telemetry Unit

Interface between  physical objects and a SCADA.

Transmits telemetry data to SCADA. Example: water quality.

Siemens LC150
Pump Control
Telemetry Unit

# PLC

Programmable Logic Controller

A computer to control the operation of electro-mechanical devices such as pumps, motors, switches

Hard real-time system

Programs stored in non-volatile memory, battery backup

Programmed using State Logic, Basic, C:
IEC 61131-3 programming standard

Siemens S7-mEC embedded controller

# PLC Programming

Programs stored in non-volatile memory, battery backup

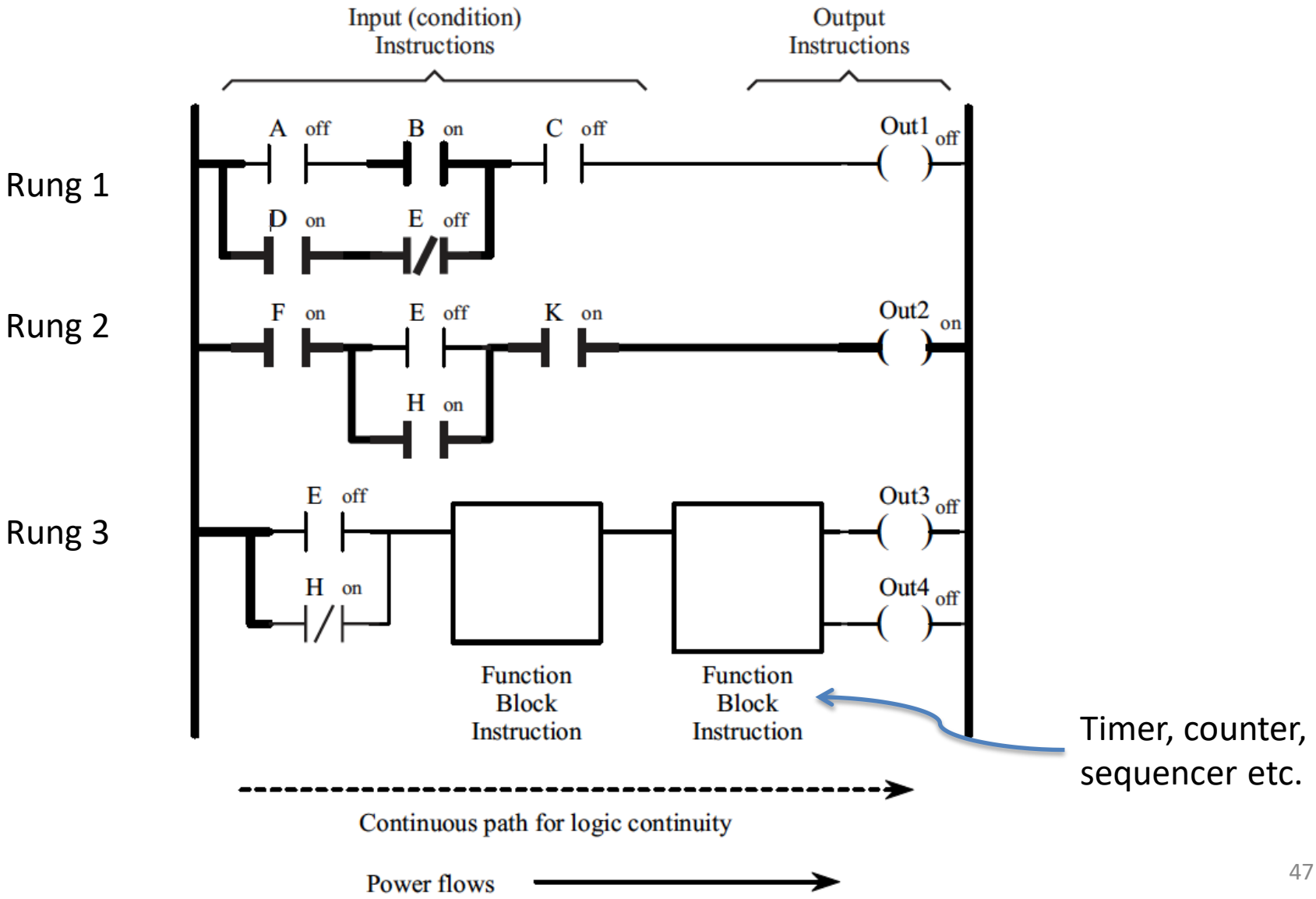
Programmed using IEC 61131-3 programming standard

Languages: graphical (e.g., Ladder diagram) and textual (e.g., Structured Text, Sequential Function Charts)

Ref: http://www.rtaautomation.com/iec61131-3/

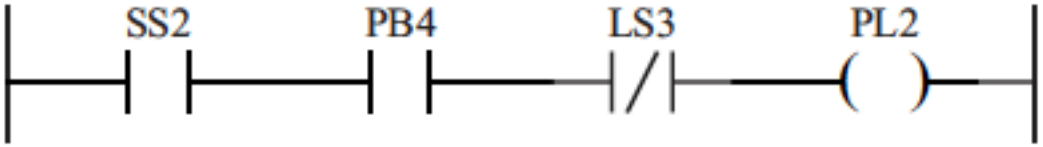
http://www.dogwoodvalleypress.com/uploads/excerpts/03192005214421.pdf

# PLC Ladder Logic Diagram



# PLC Ladder Logic Example

Pilot light PL2 is to be ON when selector switch SS2 is **closed**, push-button PB4 is **closed** and limit switch LS3 is **open**.




Series connection

PL2=SS2 (AND) PB4 (AND) LS3

# PLC Scan

PLC program is scanned continuously while reading the state of physical inputs and setting the state of the physical outputs.

Scan time for one cycle is between 0-200ms.

Larger scan times might miss transient events.

# HMI

Human Machine Interface

Operator panel to display and control of system/device state

Programming software: Example: WinCC from Siemens

# SDR

Software Defined Radio

Radio communication system that has the traditional hardware components implemented in software. These include mixers, filters, amplifiers, modulator/demodulator, etc.

# Network Security in CPS: Siemens Approach

Use the notion of “cell protection.”

Divide plant network into “automation cells.” Inside such a cell all devices are able to communicate with each other.

Access is controlled at the entrance to  each cell using a hardware device

Communication with the outside world is via VPN-protected channel.

# CPS Survivability

Despite these techniques, systems continue to be compromised.

How can a CPS continue to function above a given threshold in the presence of attacks?

Two stories:

North Pole Toys

Stuxnet

# North Pole Toys: Basics

On-line retailer.

Carries specialized toys generally not found elsewhere.

Process: Toy Assembly, Toy Packaging and Toy Shipping

2011: Replaced the old manufacturing system with new automated industrial control system.

Files are carried on USB sticks from main server to the workshop; air gap established

# North Pole Toys: Attack

Day before Thanksgiving 2011…….

Instead of one toy per box, multiple toys were being placed.

Some empty boxes were being wrapped.

Initial suspicion: Incorrect PLC code; but the code found to be correct.

Discovery: ***kAndyKAn3*** worm had infected the PLC and the main office computers.

# Stuxnet

# Uranium and its isotopes

Uranium: Naturally occurring radioactive element

Uranium 238: 99.2739 - 99.2752%

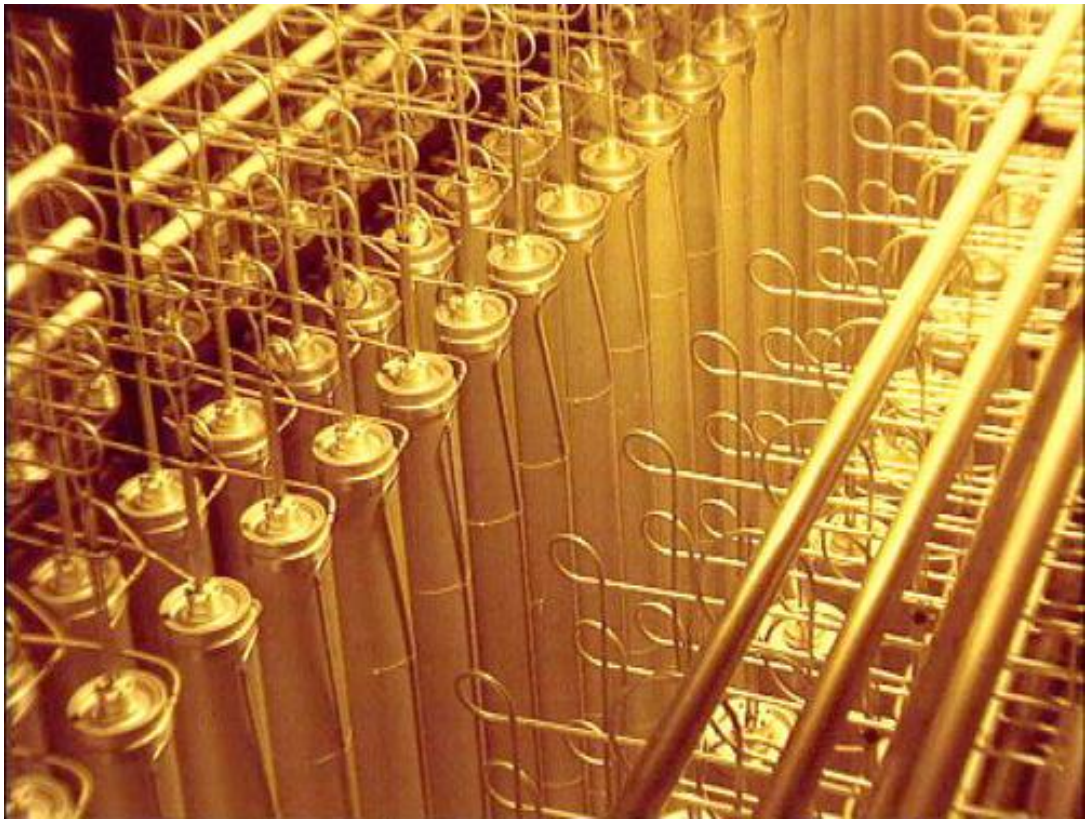
Uranium 235: 0.7198 - 0.7202%

Uranium 234: 0.0050 - 0.0059%

# Uranium 235

Only isotope found in nature in any appreciable quantities; is fissile, i.e., can be broken apart by thermal neutrons.

# Uranium enrichment: Basis

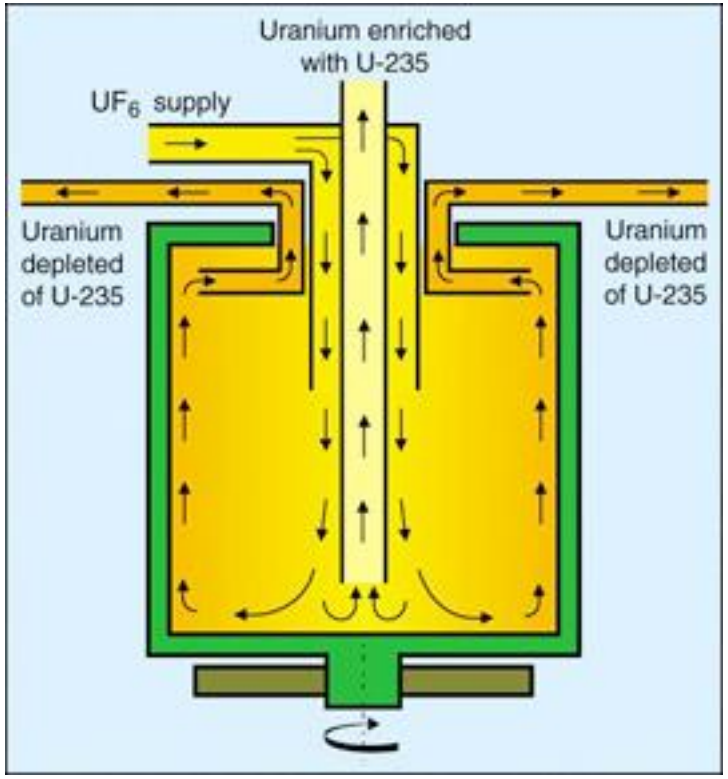


Exploit mass difference (238 versus 235)

Produce $UF_6$

http://www.world-nuclear.org/info/inf28.html

# Uranium enrichment: Zippe Centrifuge




http://en.wikipedia.org/wiki/Zippe-type_centrifuge

Use centrifuges (rapidly revolving cylinders); pulsating magnetic field applied to the rotor; bottom is heated; rotation in vacuum

Heavier U238 atoms down and outward

Lighter U235 atoms move towards center and are collected

Banks of centrifuges used to get the desired amount of U325.

geoinfo.nmt.edu/resources/uranium/enrichment.html

# Iranian nuclear enrichment plant

About 8700 centrifuges installed; replacement rate of 10% per year (approximately 800/yr);

Intl Atomic Energy Commission found over 1000-2000 removed from cascades in a few months!!

What happened?

# Malware suspicion

June 17, 2010: A computer belonging to an Iranian a customer of VirusBlokAda was caught in a reboot loop.

It was found that the virus was using a zero-day vulnerability to spread.

# Stuxnet Spread: .LNK file via USB

Microsoft informed; the virus named Stuxnet using the file names found in the virus (.stub and MrxNet.sys)

The .LNK file drops a new copy of Stuxnet onto other systems

It also drops a rootkit which is used to hide the Stuxnet routines.

Some driver files used a certificate stolen from a company in Taiwan.

# Stuxnet Spread: Vulnerabilities exploited

Print spooler

Windows keyboard file

Task Scheduler file

Static password (Cyber) coded by Siemens into Step 7 software

# Stuxnet..cut short a long story

Designed to target Simatic WinCC Step7 software from Siemens.

A malicious DLL file intercepted commands from Step 7 to PLC that controlled frequency converters; replaced them by their own commands; the screen showed only valid commands.

Stuxnet searched for a specific value—2C CB 00 01, 9500H, 7050; codes used in Profibus communication standard.

The two 1-word codes were of frequency converters made in Finland and Iran.

# Stuxnet..finally

The STL code sent 47F and 1 (command to start the frequency converter and set value to 1 ).

Stuxnet strategy:

Stay quiet for 2-weeks; increase the frequency of the converters to 1,410Hz for 15 minutes; restore them to a normal frequency of 1,064Hz for for 27 days; drop the frequency down to 2Hz for 50 minutes.

Repeat above.

# Control Systems: Basics

Secure control: towards survivable cyber physical systems, Amin et al.,

# Linear feedback system

$$\dot{\mathbf{x}}(t) = A(t)\mathbf{x}(t) + B(t)\mathbf{u}(t)$$
$$\mathbf{y}(t) = C(t)\mathbf{x}(t) + D(t)\mathbf{u}(t)$$

$x_{k+1}=Ax_k+w_k$

$y_k=Cx_k+v_k$

x: state vector
A: state matrix
B: Input matrix
C: Output matrix
D: Feedforward matrix
u: Control input
Y: System output

w: state noise and
v: measurement noise
vectors

Problem: How to ensure optimal state estimation under noisy measurements?

Gaussian random noise, zero mean and
and R, both >0 as covariance

# Linear feedback system: discrete version

$x_{k+1}=Ax_k+w_k$

$y_k=Cx_k+v_k$

w: state noise and
v: measurement noise
vectors

Problem: How to ensure optimal state estimation under noisy measurements?

Gaussian random noise, zero mean and Q and R, both >0 as covariance.

**Assumption: (**A;C**)** is detectable and **(**A;Q**)** is stabilizable,
the estimation error covariance of the Kalman filter converges to a unique steady state value from any initial condition.

# Linear feedback system: robustness

$x_{k+1}=Ax_k+w_k$

$y_k=Cx_k+v_k$

w: state noise and
v: measurement noise
vectors

Every raw measurement of y might not arrive at the controller (estimator), e.g., due to network congestion.

Hence Kalman filters are needed that take into account packet losses (history of packet losses).

Do we know the characteristic of packet losses when under attack (QoS parameters)?

Perhaps consider state of the communications network as a stochastic event and develop new filtering techniques.

# Fault tolerant control (FTC)

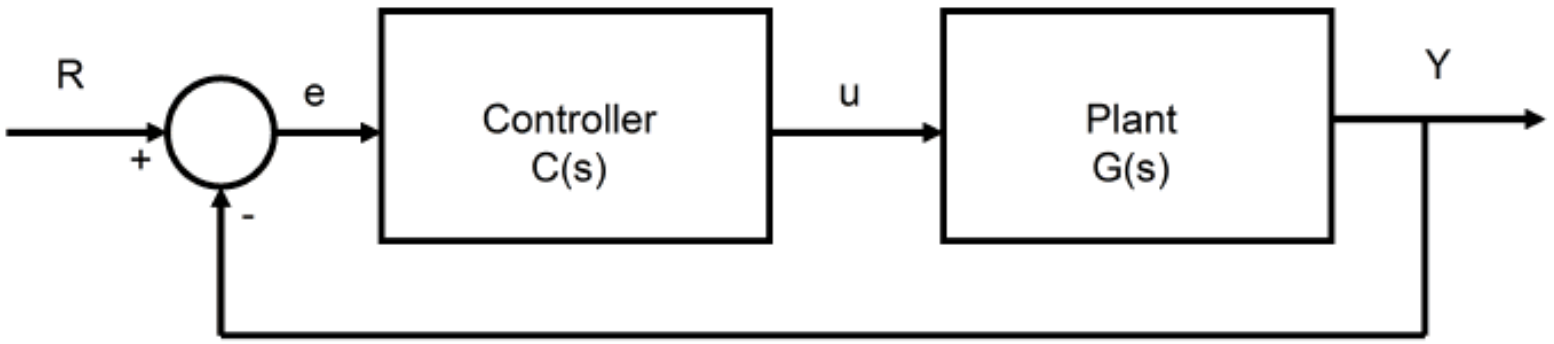
Goal: Maintain stability and acceptable behavior in the presence of component faults by applying physical and/or analytical redundancies.

Passive FTC: Consider a fixed set of fault configurations and design the system to detect and compensate for these.

Example: Control in the presence of sensor malfunction.

Active FTC: Estimate state and fault parameters using measurements and control data and reconfigure the system using different control law.

# PID Controller



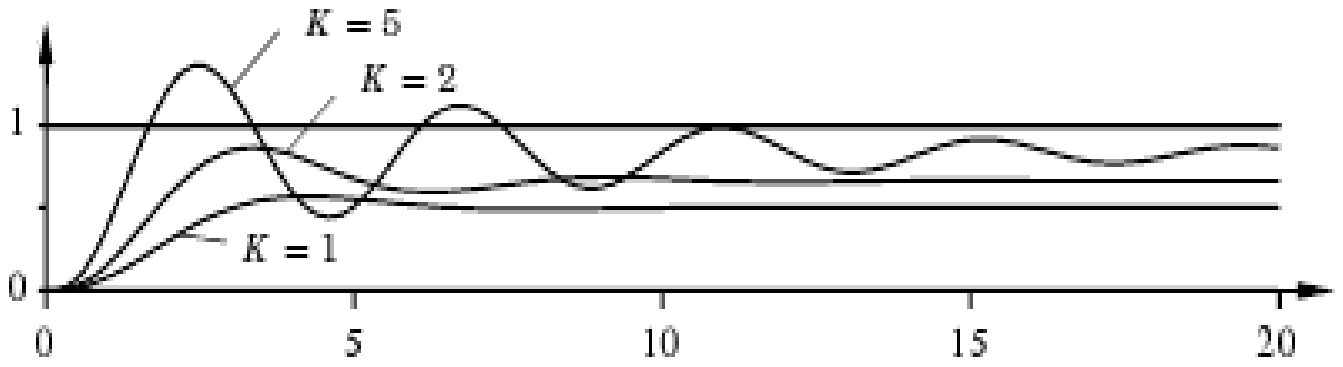

P: Proportional
I: Integral:
D: Derivative
e: Error
u: Control input
Y: System output

$$u = K_P e + K_I \int e\,dt + K_D \frac{de}{dt}$$

Proportionality constants control the rise time, overshoot, settling time, and the steady state error of system output Y.

# Proportional Controller

$$u = K_P e$$



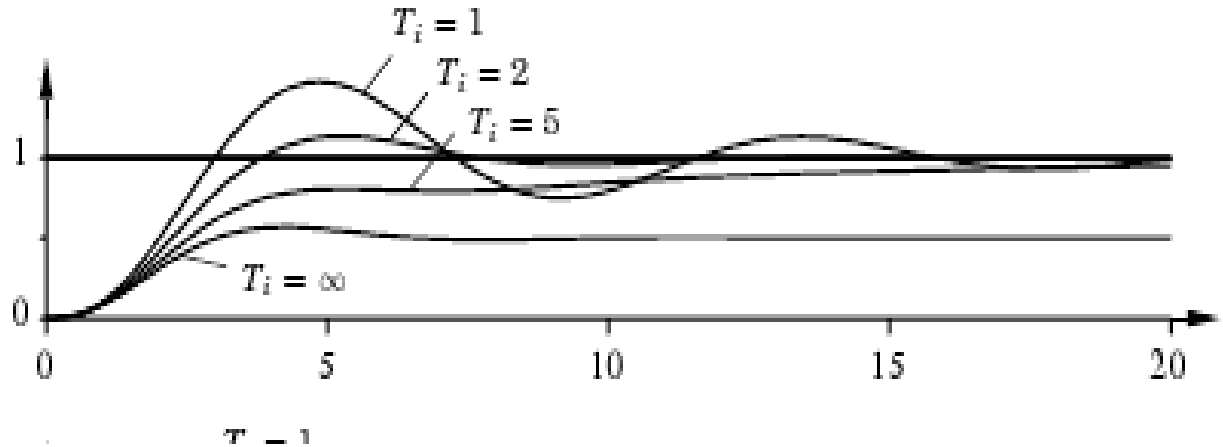

Always a steady state error.

Error decreases with increasing gain.

Tendency to oscillate increases with increasing gain.

# PID Controller

$$u = K_P e + K_D \int e\,dt$$



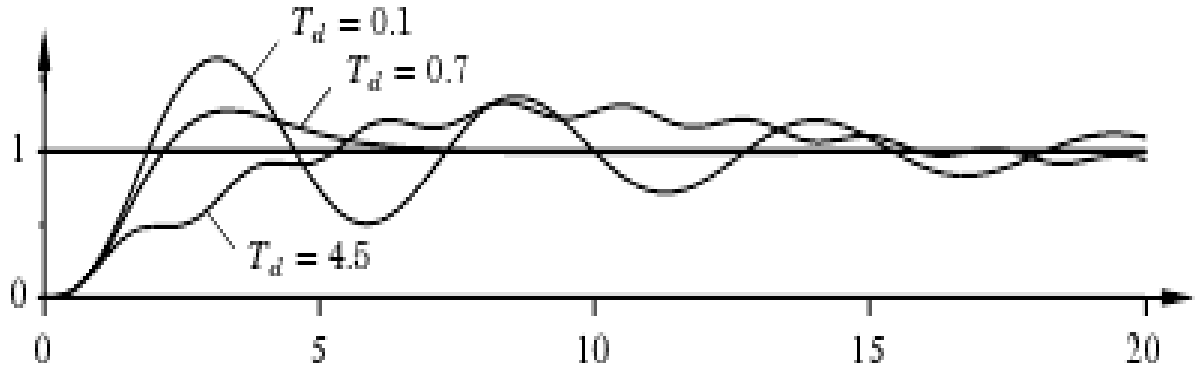

Steady state error vanishes.

Tendency to oscillate increases with increasing $K_D = 1/T_i$, i.e., decreasing $T_i$.

Tendency to oscillate increases with increasing gain.

# PID Controller

$$u = K_P e + K_I \int e\,dt + K_D \frac{de}{dt}$$




KP and KI selected for oscillatory system.

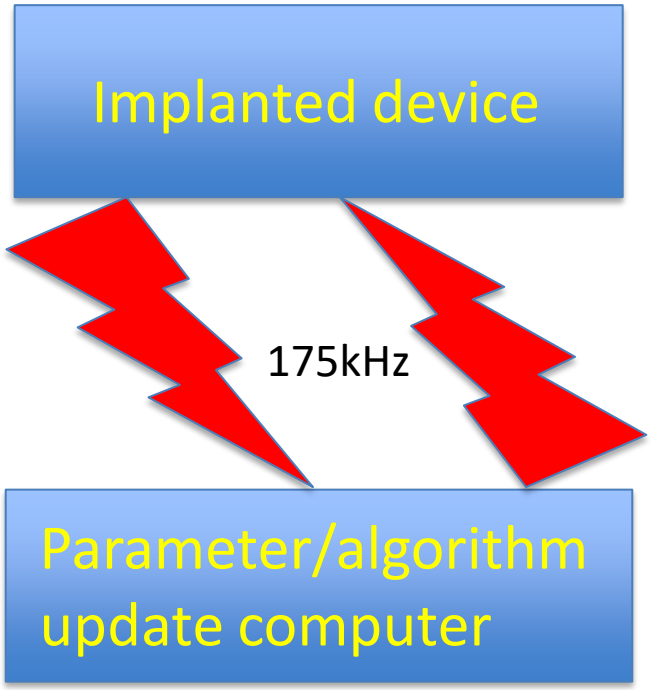
Damping increases with increasing $T_d$ ($K_D$=1/$T_d$).

Derivative term is ineffective when $T_d$ is larger than about 1/6$^{th}$ of the period .

# Attacks on Implantable Medical Devices

Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device Attack




Pumps can be hijacked by hacking radio signals.

Then the device could be switched off

Dangerous dose of medicine could be delivered

Security alerts could be disabled

# CPS: Medical Device Attack Procedure

Reverse engineer the transmissions:

1. Capture RF transmission [175kHz].

2. Oscilloscope allowed identification of transmissions from ICD to ICD Programmer.

3. RF traces analyzed using Matlab and GNU Radio toolchain to obtain symbols and bits.

4. This led to the discovery of the ICD –programmer communications protocol.

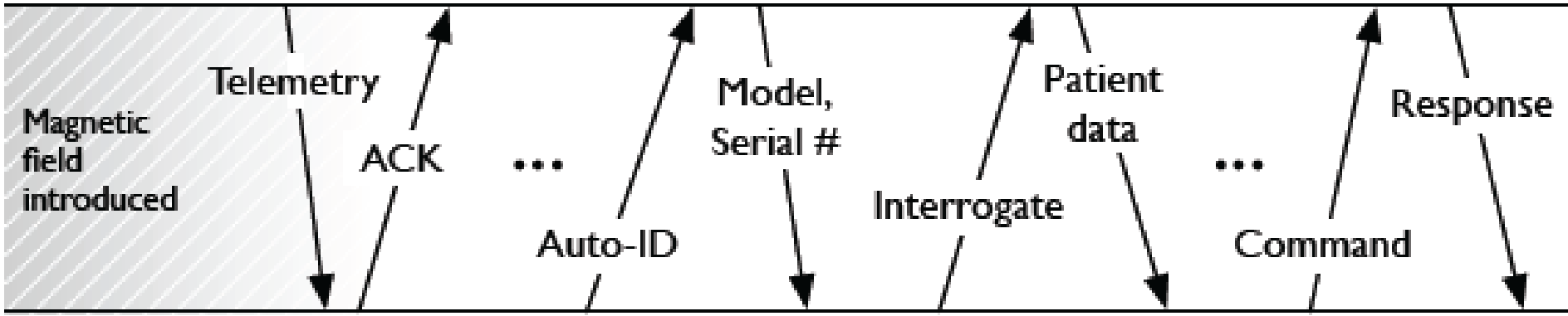
# CPS: Medical Device Attack Procedure

Eavesdropping with a software radio:

1. Built an eavesdropper using GNU radio library.
2. Establish transaction timeline.
3. Decoding not needed; meaning of transactions were deciphered by observing the order in which the programmer acquired the information from the ICD.

# CPS: Medical Device Attacks

ICD-Programmer Communications:




Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device: Attacks

Using Universal Software Radio Peripheral and BasicTX board, several attacks were possible.

Air gap of a few centimeters..

Replay attack: ICT set to a known state, replay the desired transmission and then evaluate the ICD state.

.

Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device: Attacks

Triggering ICD identification: Auto-identification trace was replayed leading to identical responses from the ICD.

Disclosing patient data: Auto-identification followed by interrogation command makes the ICD respond with patient name, diagnosis, and other details.

Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device: Attacks

Disclosing cardiac data: Replaying the start of the interrogation command sequence causes the ICD to transmit cardiac data.

Changing therapies: Therapies could be turned off by replaying captures where the programmer turns off the therapies. Once done, the ICD does not respond to dangerous cardiac conditions.

Halperin et al, 2008 IEEE SS&P, pp129 -142

# Securing Medical Devices: Encryption?

Should the communications between the programmer and the ICD be encrypted?

Halperin et al, 2008 IEEE SS&P, pp129 -142

# Securing Medical Devices: Zero power approaches

Zero-power notification: Alert patient when security-sensitive event occurs; do so by harvesting induced RF to wirelessly power a piezo-element [built on WISP: Wireless Identification Sensing Platform]

Zero-power authentication: Harvest RF energy to power cryptographically strong protocol to authenticate requests from the programmer. [Challenge-response protocol]

Sensible key-exchange: Combine ZPN and ZPA for vibration-based key distribution.

Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device: Protocol

$K_M$: master key (Programmer)

I: IMD serial number

K=f(KM, I); IMD key

f: pseudorandom function

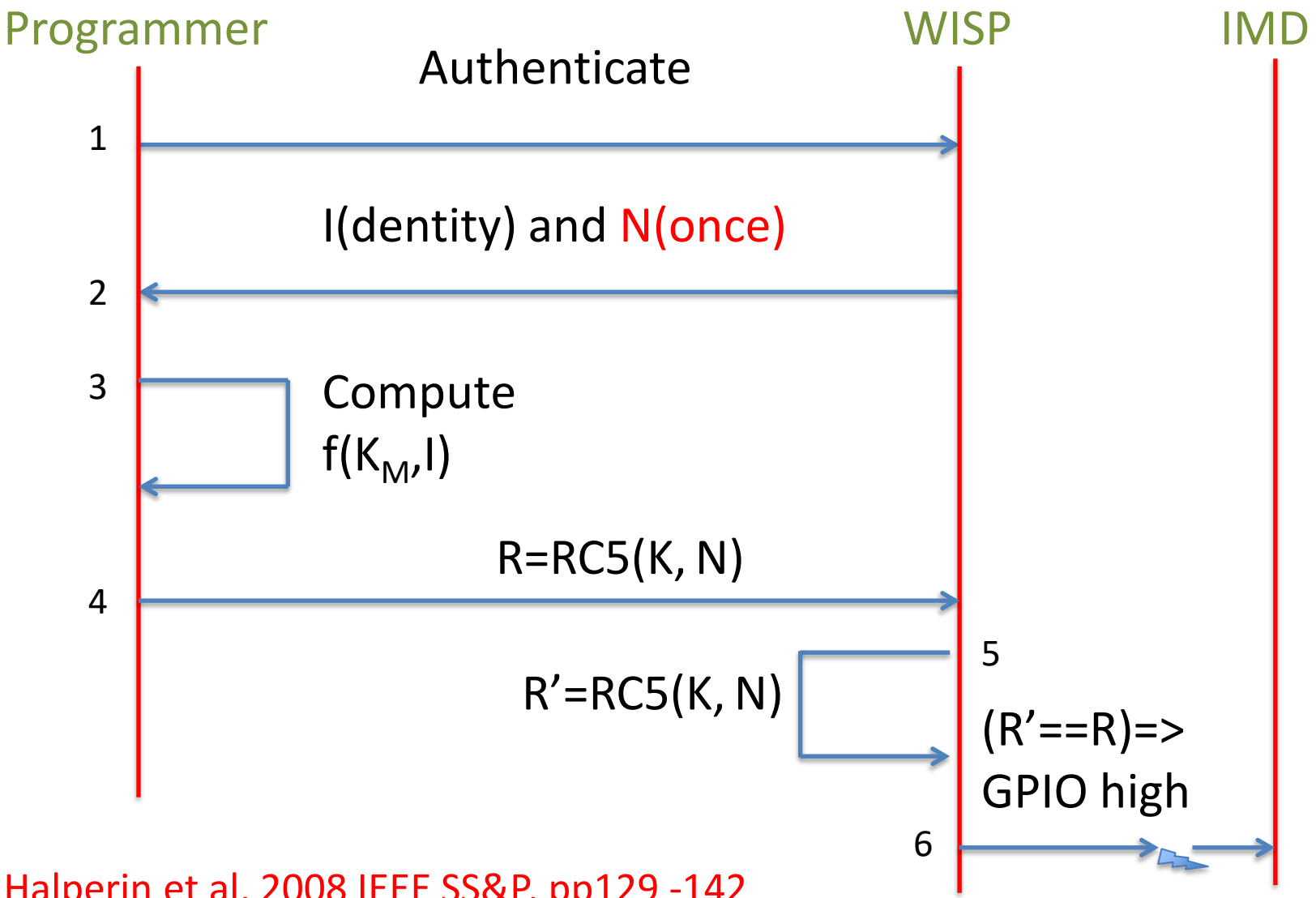
RC5: Block cipher

GPIO: General Purpose IO port

Nonce: Fixed in this implementation

Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device: Protocol




Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device: Key management

Open problem for implantable devices

Halperin et al, 2008 IEEE SS&P, pp129 -142

# CPS: Medical Device Attack: Results

| | Commercial programmer | Software radio eavesdropper | Software radio programmer | Primary risk |
|---|---|---|---|---|
| Determine whether patient has an ICD | ✔ | ✔ | ✔ | Privacy |
| Determine what kind of ICD patient has | ✔ | ✔ | ✔ | Privacy |
| Determine ID (serial #) of ICD | ✔ | ✔ | ✔ | Privacy |
| Obtain private telemetry data from ICD | ✔ | ✔ | ✔ | Privacy |
| Obtain private information about patient history | ✔ | ✔ | ✔ | Privacy |
| Determine identity (name, etc.) of patient | ✔ | ✔ | ✔ | Privacy |
| Change device settings | ✔ | | ✔ | Integrity |
| Change or disable therapies | ✔ | | ✔ | Integrity |
| Deliver command shock | ✔ | | ✔ | Integrity |

Halperin et al, 2008 IEEE SS&P, pp129 -142

# Deception Attacks on Irrigation Systems

On Cyber Security for Networked Control Systems, Amin, Saurabh, Ph.D., UNIVERSITY OF CALIFORNIA, BERKELEY, 2011, 198 pages; 3473864

# The Gignac irrigation canal

# SCADA in irrigation: Physical attacks

Solar panels stolen affecting radio communications

Damaged monitoring bridge that hosts gate controllers

Installing additional pumps

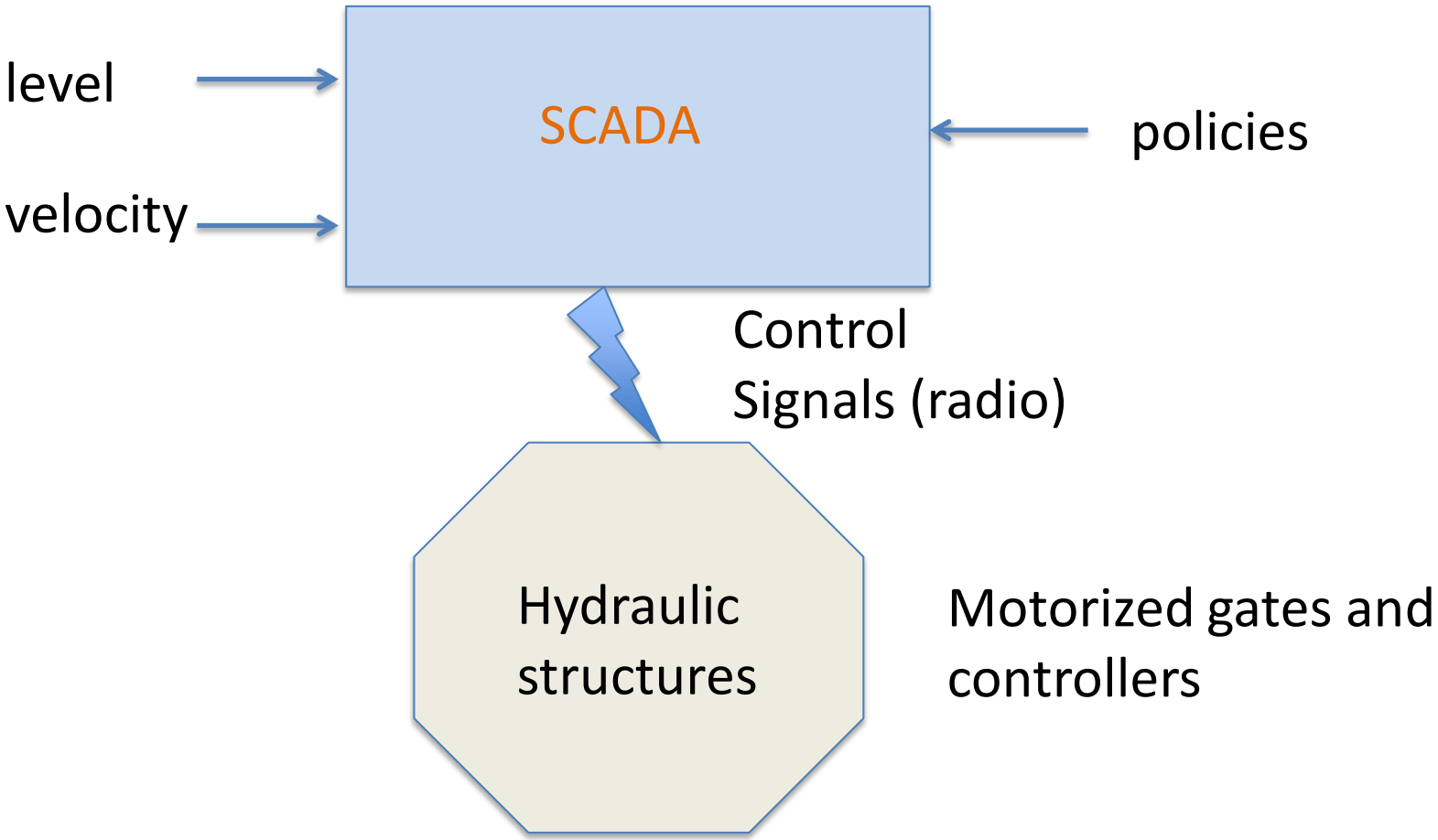
# SCADA in irrigation: Other incidents

Tehama colusa canal, Willows, CA, USA

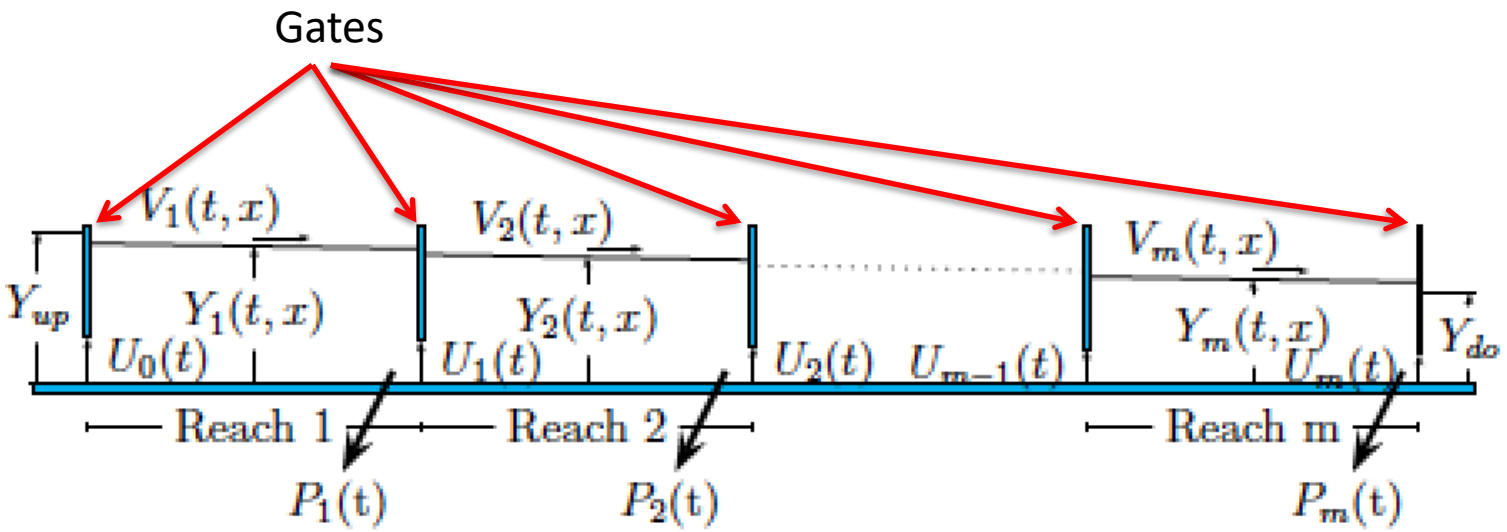
Maroochy water breach, near Brisbane, Australia

Harrisburg water filtering plant, Harrisburg, PA, USA

# SCADA in irrigation



# Irrigation canal model




m: Number of canal pools

T, X: Cross section width and length of each pool (m)

V: Average cross-sectional velocity (m/s)

Y: Water depth

P: Offtake; lateral outflow ($m^2/s$)

$U_{i-1}$, $U_i$: Opening of upstream and downstream gates

# Irrigation canal: Shallow Water Eqns

$$\frac{\partial}{\partial t}\begin{pmatrix} Y_i \\ V_i \end{pmatrix} + F(Y_i, V_i)\frac{\partial}{\partial x}\begin{pmatrix} Y_i \\ V_i \end{pmatrix} = H(Y_i, V_i, P_i)$$

$$F(Y_i, V_i) = \begin{pmatrix} V_i & Y_i \\ g & V_i \end{pmatrix}, \quad H(Y_i, V_i, P_i) = \begin{pmatrix} -P_i/T \\ g(S_b - S_{fi}) \end{pmatrix}$$

g: gravity ($m/s^2$)

$S_f$ : friction slope

$S_b$ : bed slope (m/m)

# Irrigation canal: Control actions

$U_{i-1}$ and $U_i$: can be changed by controlling the actuators:
Y: Known upstream and downstream

Yi(0, t) and Yi(X,t): known measurements

Upstream and downstream discharge:

$$V_1(0,t)Y_1(0,t) = U_0(t)\sqrt{Y_{\mathrm{up}} - Y_1(0,t)},$$
$$V_m(X,t)Y_m(X,t) = U_m(t)\sqrt{Y_m(X,t) - Y_{\mathrm{do}}},$$

$$V_i(X,t)Y_i(X,t) = U_i(t)\sqrt{Y_i(X,t) - Y_{i+1}(0,t)},$$
$$V_i(X,t)Y_i(X,t) = V_{i+1}(0,t)Y_{i+1}(0,t),$$

# Irrigation canal: Boundary conditions

Upstream and downstream discharge:

$$V_1(0,t)Y_1(0,t) = U_0(t)\sqrt{Y_{\mathrm{up}} - Y_1(0,t)},$$
$$V_m(X,t)Y_m(X,t) = U_m(t)\sqrt{Y_m(X,t) - Y_{\mathrm{do}}},$$

Intermediate gates discharge:

$$V_i(X,t)Y_i(X,t) = U_i(t)\sqrt{Y_i(X,t) - Y_{i+1}(0,t)},$$
$$V_i(X,t)Y_i(X,t) = V_{i+1}(0,t)Y_{i+1}(0,t),$$

# Irrigation canal: Feedback actions

Change in gate openings $u_i(t)$

Boundary control actions are decentralized and local to each canal pool; computed using local water level measurements.

# Irrigation canal: Water withdrawal attack

$J_i$: Number of offtakes from pool i

Lateral flow along the length of the ith pool:

$$p_i(x,t) = \begin{cases} p_{i,j}(t) & x \in [\overline{x}_{i,j}, \underline{x}_{i,j}], \quad j = 1\ldots, J_i \\ 0 & \text{otherwise} \end{cases}$$

Indicator for $j^{th}$ offtake in $i^{th}$ canal:

$$\mathcal{X}_{i,j}(x) = \begin{cases} 1 & \text{if } x \in [\overline{x}_{i,j}, \underline{x}_{i,j}] \\ 0 & \text{otherwise .} \end{cases}$$

Total lateral withdrawal from $i^{th}$ canal: $$p_i(x,t) = \sum_{j=1}^{J_i} p_{i,j}(t)\mathcal{X}_{i,j}(x).$$

# Irrigation canal: Water withdrawal attack

Adversary can affect withdrawal from one or more of the $J_i$ offtakes in canal i.

Water is withdrawn by discretely opening and closing the offtake gates.

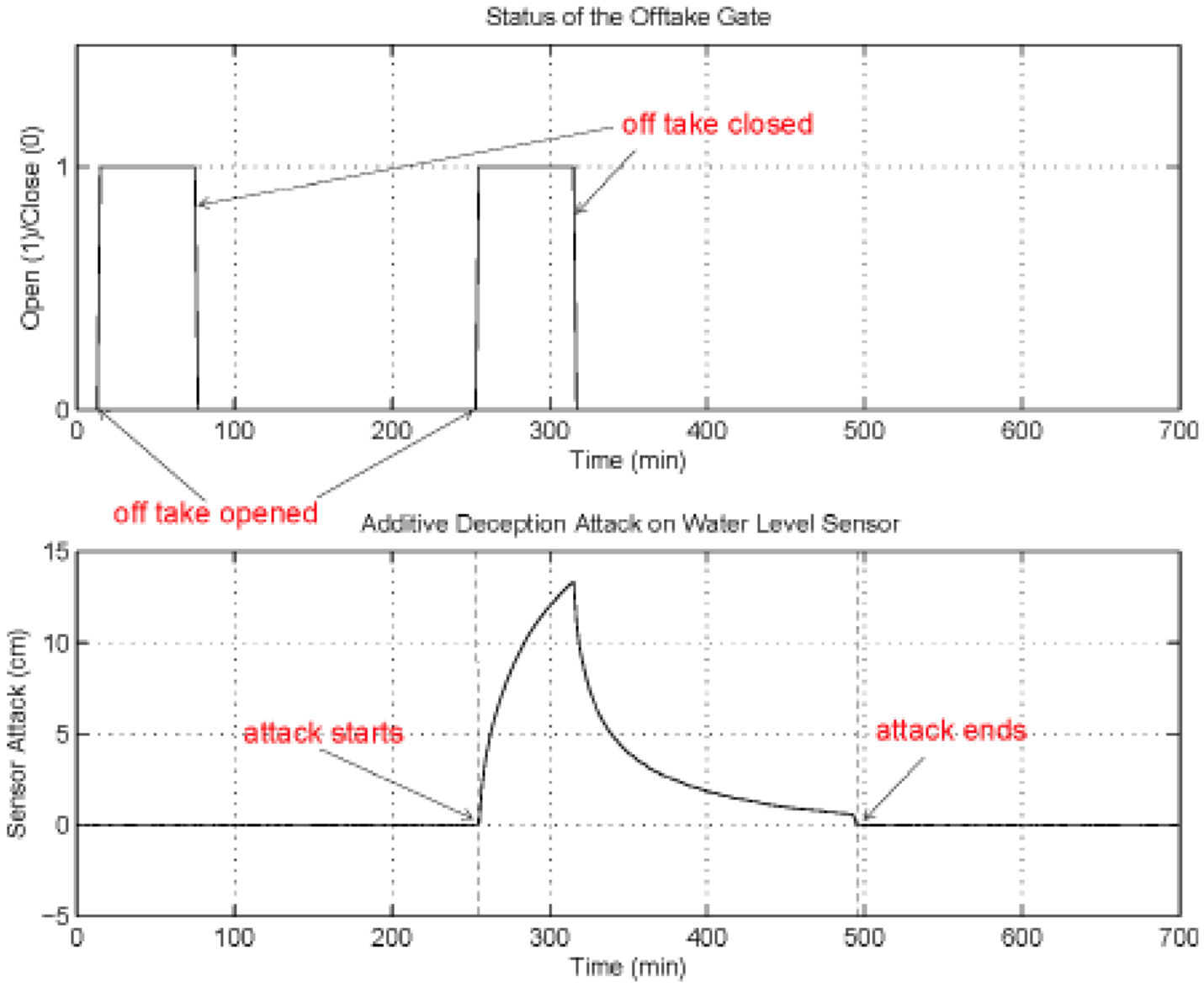
Thus, the offtake withdrawal vector $r(t)$ switches between different modes Q={1, 2,….N}.

# Irrigation canal: sensor deception attack

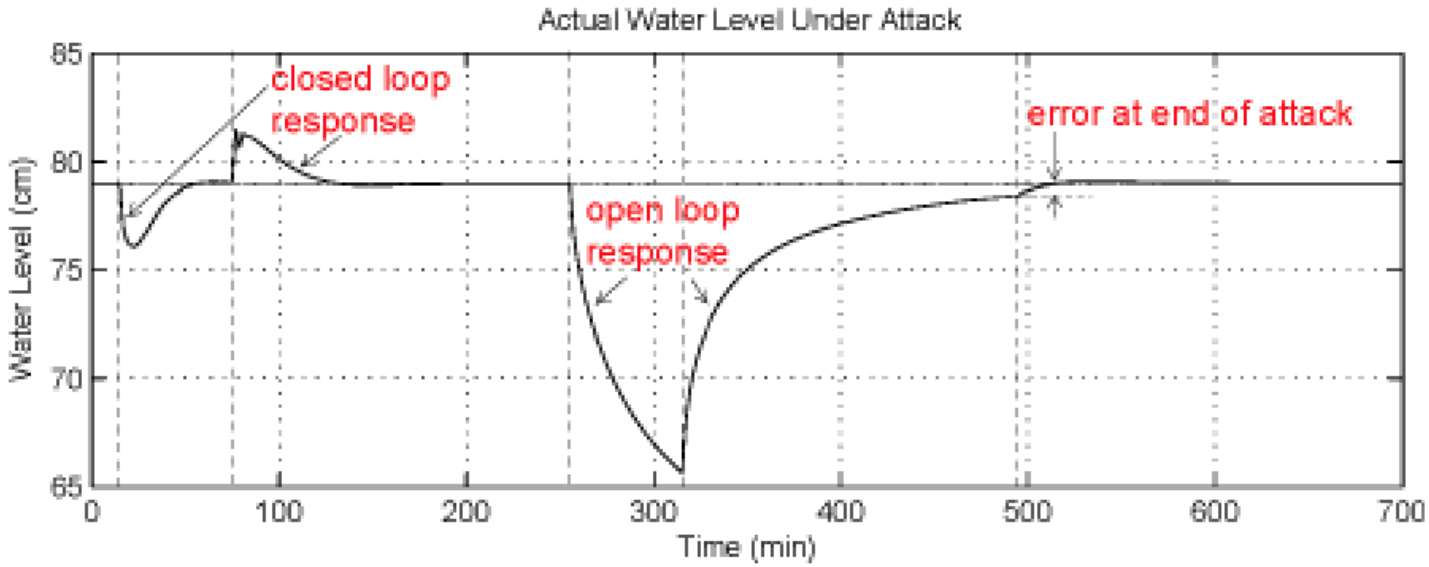
Adversary can affect sensor readings for upstream Yi(0, t) and Yi(X,t) and gate opening Ui(t)

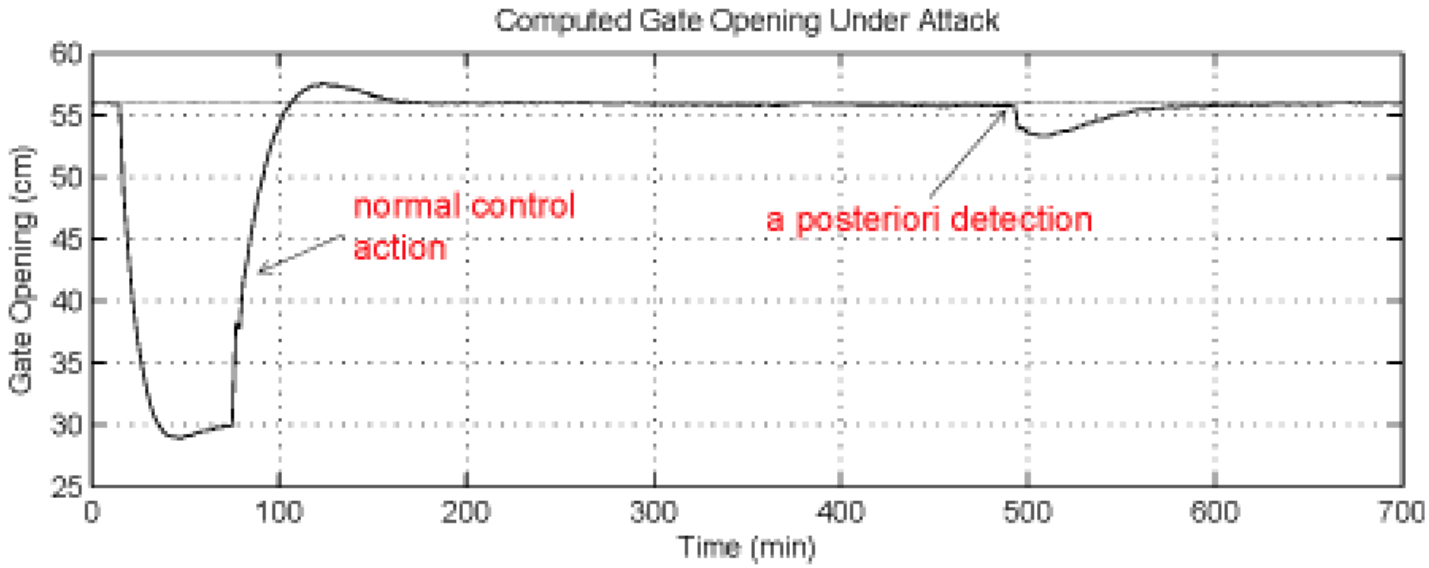
This leads to a transformed water level and gate openings.

# Irrigation canal: Experiments



# Irrigation canal: Experiments



# CPS Design Principles

# Aspects to consider

Adversary models: Restrict the scope; but overly restrictive assumptions will likely limit their aplicability e.g., in DoS attacks.

Trust models: Trust in human users and devices, e.g., sensors and actuators

“Under attack” behavior: Detection and graceful degradation.

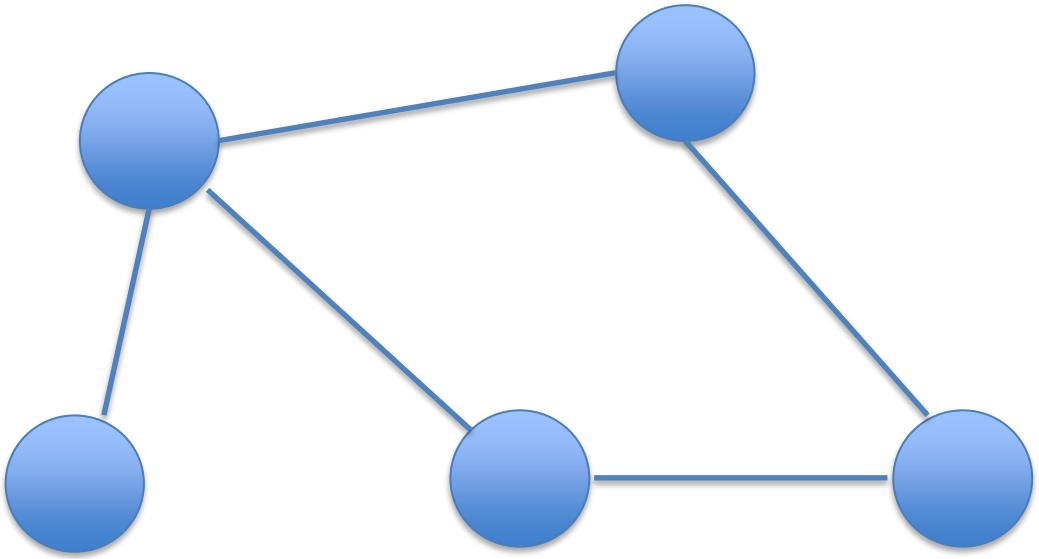
Independence in component design: Redundant authentication mechanisms that are indepenent of each other

# Potential research directions and educational needs

# CPS Gaps?

Study the overall design of selected critical CPS infrastructures and determine security gaps and their impact on functionality and safety of Singapore population.

# CPS Modeling: Network models



What is the state space of reach node (a subsystem)?

What are the constraints across node-states?

If and how could an attacker violate the constraints?

# CPS [Supply chain] Monitoring

How could nodes in a supply chain-- with Singapore as a node-- be compromised?

Are the existing intrusion detection tools adequate for monitoring attacks across a supply chain?

What monitoring tools are need to check the “health” of a supply chain given the possibility of an network attack?

# CPS Attack scenarios

Are there attacks different from the existing ones that could sabotage a supply chain or any CPS?

How to defend against any such attacks?

# CPS Control Robustness

How to design controllers that could continue to function in the presence of deception and denial of service attacks?

# CPS Access Control

Are RBAC and TRBAC models for access control adequate for large distributed CPS and global supply chains?

# CPS: Theoretical Foundations

Control theoretic [e.g., work at Berkeley]

Game theoretic [e.g., work at UT Arlington]

Verification and testing techniques[e.g., work at Purdue]

Specification-based [e.g., work at UIUC]

# CPS: Educational needs

Traditional IT security:

Cryptography, networks, OS, and other CS subjects

CPS security:

Interdisciplinary education needed;

Background in controls, game theory, industrial automation;

Domain background

Most importantly:

Ability to acquire the necessary background through self learning

# Summary

What is a CPS?

Why existing techniques for the detection and prevention of information-related attacks might be inadequate in CPS?

What research directions Singapore ought to consider to ensure the functionality of its CPS and consequently the safety of its people?

# References [Sample]


Secure Control: Towards Survivable Cyber-Physical Systems. Alvaro A. Cárdenas Saurabh Amin Shankar Sastry, The 28th International Conference on Distributed Computing Systems Workshop, IEEE 2008.

Common Cybersecurity Vulnerabilities in Industrial Control Systems. US Department of Homeland Security. May 2011.

Cyber-Physical Systems Security for Smart Grid. White Paper. Manimaran Govindarasu, Adam Hann, and Peter Sauer. February 2012.

Improving the Security and Privacy of Implantable Medical Devices, William H. Maisel and Tadayoshi Kohno, New England Journal of Medicine 362(13):1164-1166, April 2010.

**Guide to Industrial Control Systems (ICS) Security**. Keith Stouffer, Joe Falco, and Karen Scarfone. NIST. 800-02. June 2011.