Cyber-Physical Resilient Systems

From Malware & Operational Security to Feedback Truthfulness Distinguishability

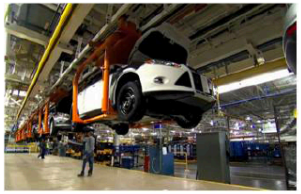
Joaquin Garcia-Alfaro

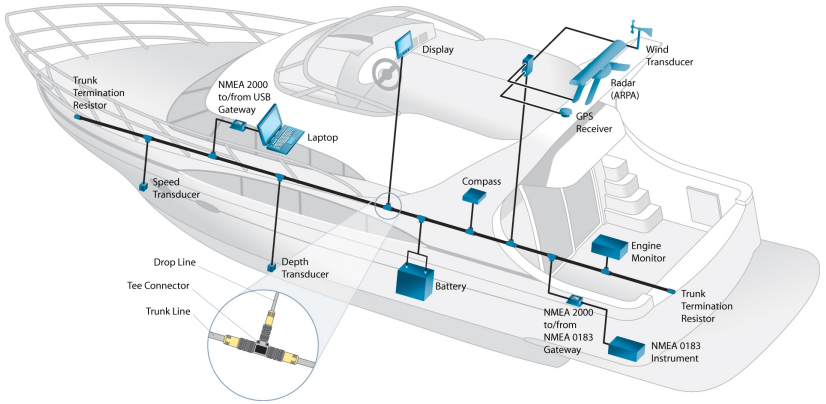
Institut Mines-Télécom (Télécom SudParis)
& Université Paris-Saclay

ETIC-UPF Seminars, Barcelona, 01/03/2018

Today's Talk: Cyber-Physical Resilience

- Cyber-Physical Systems*
  - **ICT** components monitoring & controlling **physical** resources
  - **Physical** & **ICT** elements that interact with **humans**





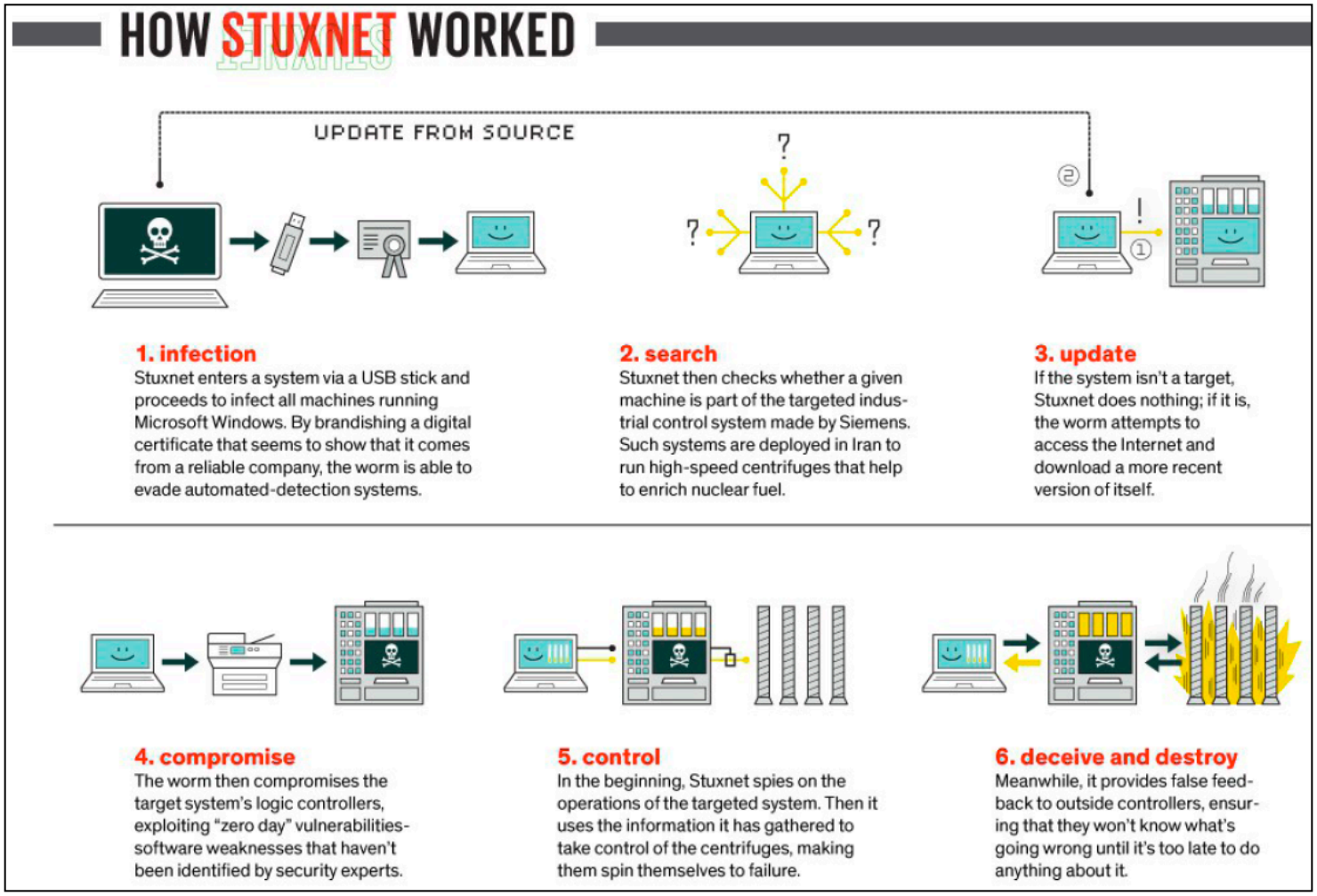
* H. Gill, National Science Foundation, 2006.

Today's Talk: Cyber-Physical Resilience

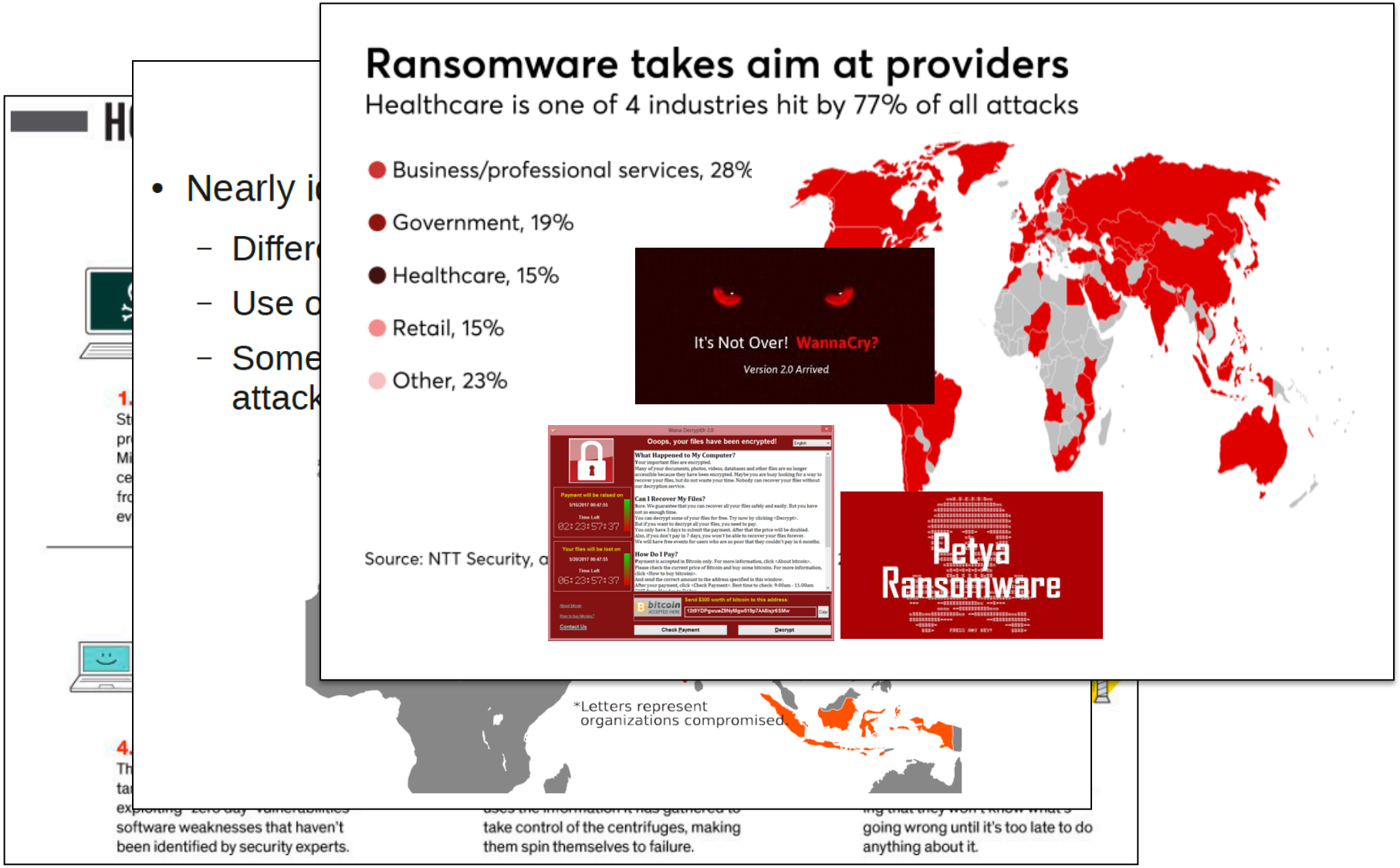
Subtitle was:

From **Malware & Operational Security**
to Feedback Truthfulness Distinguishability

Malware & Operational Security



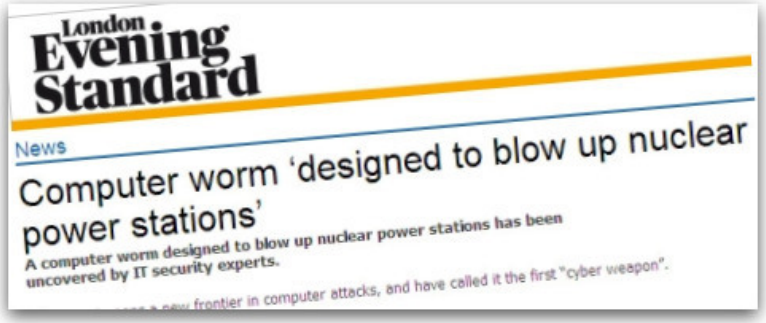
Malware & Operational Security



In addition to malware ...

- *Malware moving from IT Systems to Operational Systems*

- Wrong configurations, lack of encryption, legacy (vulnerable) systems, ***intentionality***...

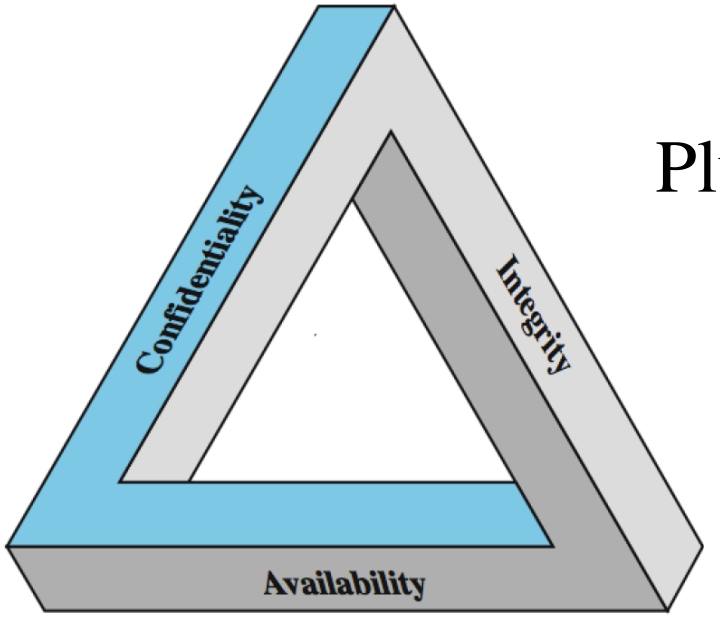

London Evening Standard

News

Computer worm 'designed to blow up nuclear power stations'

A computer worm designed to blow up nuclear power stations has been uncovered by IT security experts.

IT & OT together ...

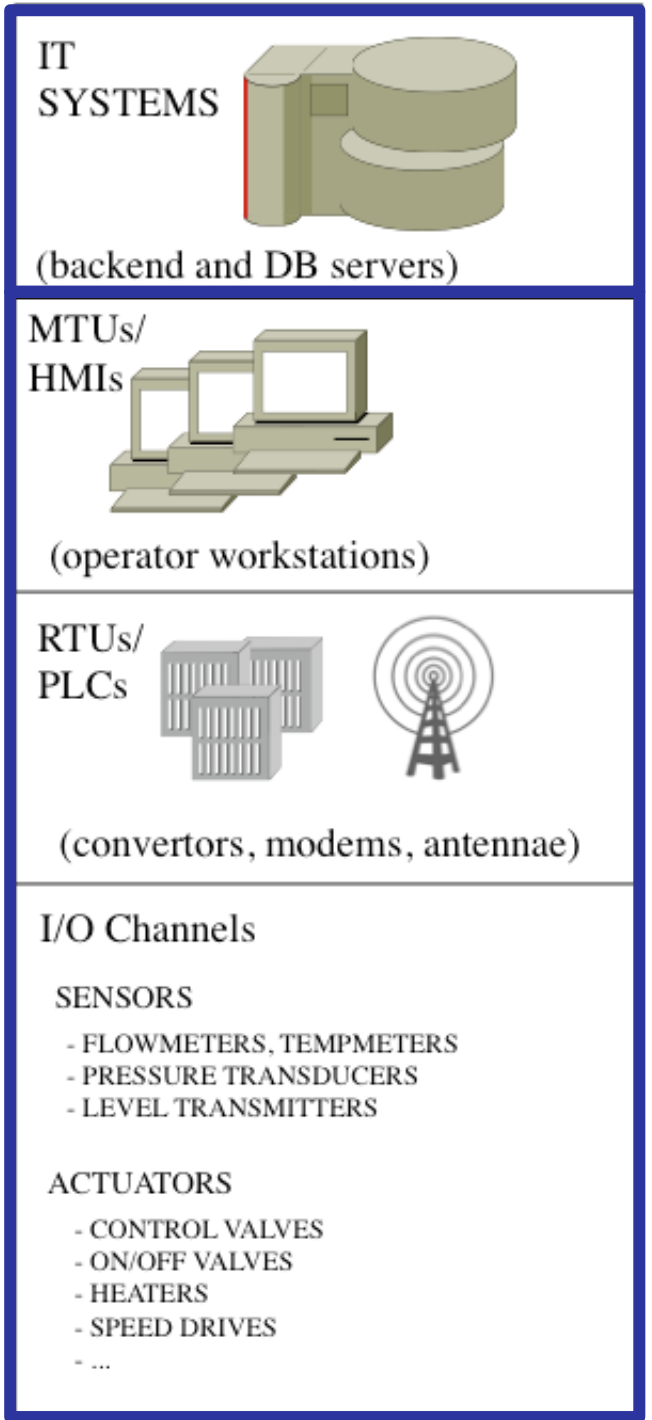


Plus

- Reliability,
- Safety,
- Performance, ...

Asset to protect: Information Process

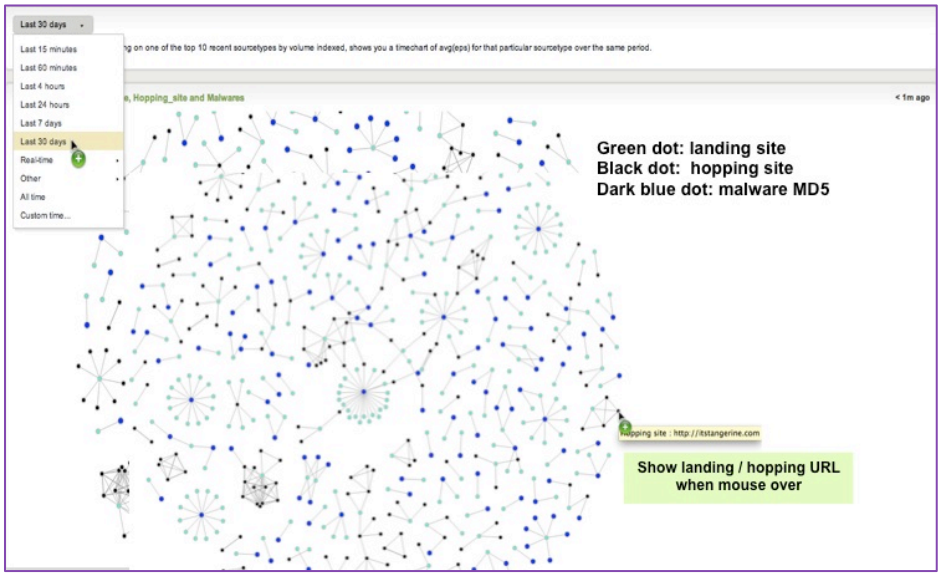
Priority	IT Systems	MTUs to I/O
#1	Confidentiality	Availability
#2	Integrity	Integrity
#3	Availability	Confidentiality



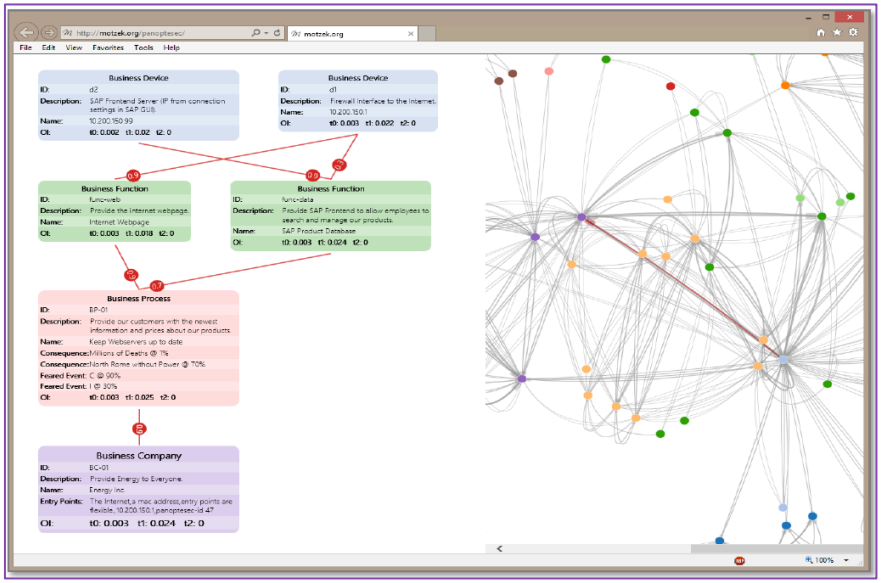
[1] HIRSCHMANN, Why is Cyber Security Still a Problem? *TOFINO Security Series*

Dynamic Risk Assessment example

- Prevent threats (e.g., preempt exploitation of vulnerabilities)
- Use of Attack & Mission Graphs to support network administrators towards semi-automated decisions



IT Security Oriented



OT Security Oriented

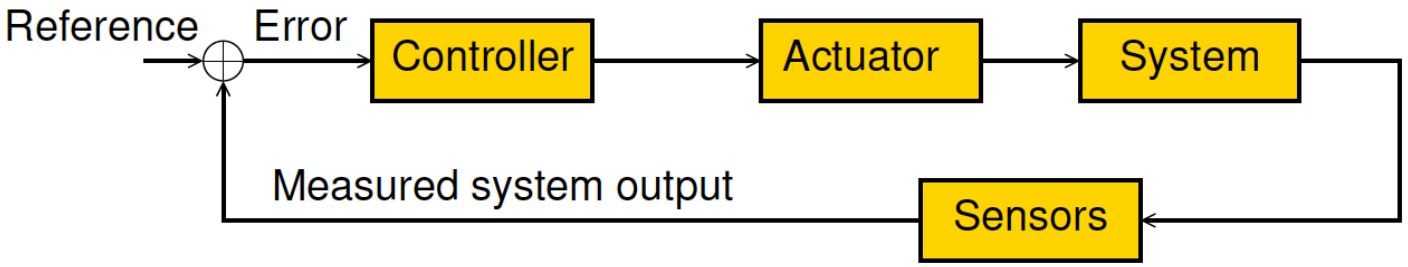
http://j.mp/DRDMS

Outline

- Experience & Context
  - Cyber-Physical Systems
- **Feedback Truthfulness (FT)**
- **Ongoing Work on FT Distinguishability**
- **Summary & Perspectives**

The key ingredient in a CPS: Control

- **Control** means making a (dynamical) system to work as required
- **Feedback** is used to compute a corrective **control action** based on the distance between a *reference signal* and the *system output*



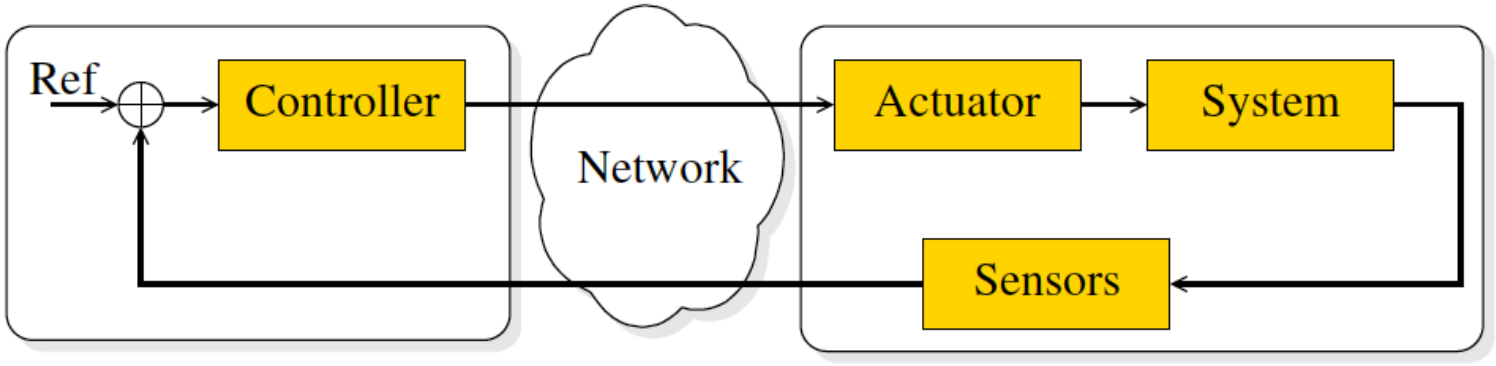
- Examples: dynamically follow a trajectory (robotics), regulate a temperature, regulate the sending rate of a TCP sender (TCP cong. control), controlling a pendulum in its unstable equilibrium, etc.

Networked Control System

- From a methodological standpoint, we can model a CPS using a Network Control System (NCS)

NCS definition

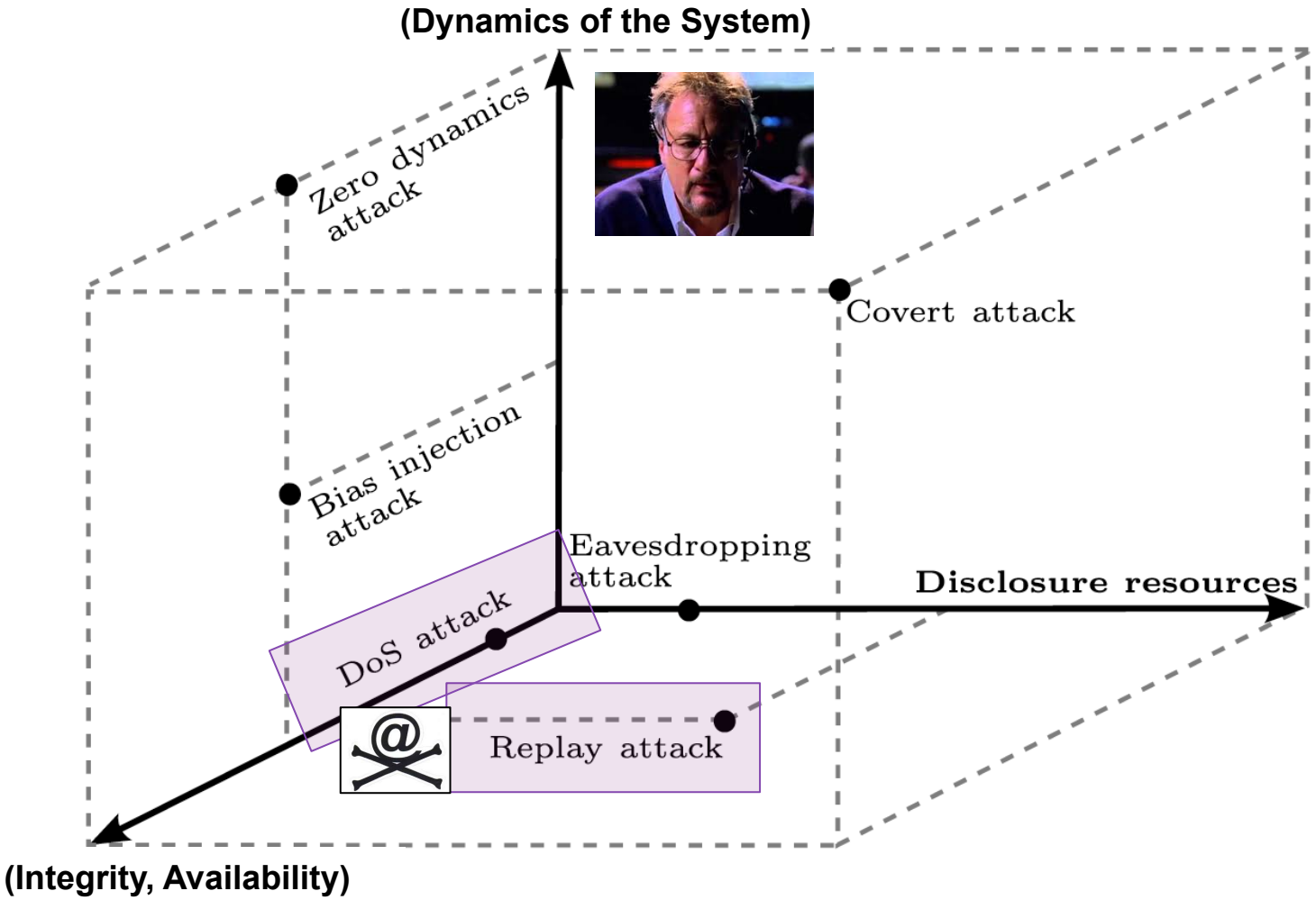
Control system whose control loops are connected through a communication network



Traditional Issues Studied in the NCS Literature

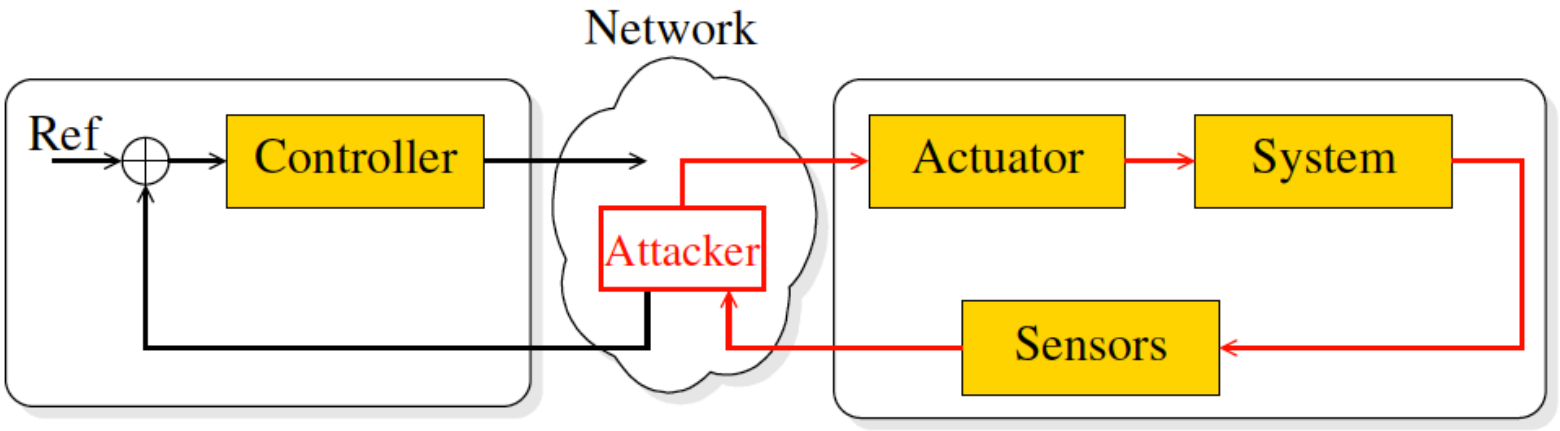
- Stabilizing a system under network delays & packet losses
- Techniques to limit data rate (e.g., from control to plant)
- Energy efficient networking for Wireless NCS
- Security?
  - Since the *stuxnet* incident, the control community seems to be heavily working as well on security issues of NCSs & CPSs
  - Control-theoretic security taxonomies?

Sample Attacks*



** A secure control framework for resource-limited adversaries. Texeira et al., Automatica, 51(1):135-148, 2015.*

Replay Attack



- Step 1: Sensors output is recorded
- Step 2: Recorded sensors output is replayed and sent to the controller
- Step 3: A control signal is sent to disrupt system functionalities

Prevention & Mitigation of CPS Attacks

- A well-designed control system shall resist external disturbances (failures & attacks), to a certain degree
- Several control-theoretic techniques to prevent cyber-physical attacks have been proposed in the literature*
- Most of the techniques aim at injecting authentication to the control signal & discover anomalous measurements
  - E.g., use a noisy control authentication signal to detect integrity attacks on sensor measurements
  - In the following, we elaborate further on the aforementioned technique

** A survey on the security of cyber-physical systems. Wu, Sun, and Chen. Control Theory and Technology, 14(1):2–10, February 2016.*

Watermark Approach by Mo et al.

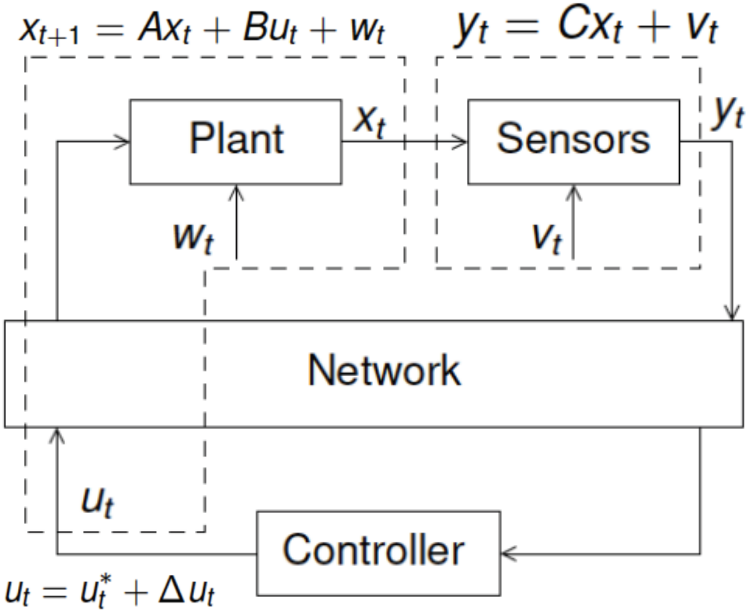
Idea [Mo et al., 2009, 2015]

Adding a watermark signal to the control signal which serves as an authentication signal

- Conceptually similar to a challenge-response authentication scheme
- In this case the watermark is the challenge the response is the sensor output
- Main advantages:
  - Only the controller has to be changed
  - It does not require encryption

** Physical Authentication of Control Systems. Mo, Weerakkody and Sinopoli. IEEE Control Systems, Vol. 35, pages 93–109, 2015.*

In a nutshell ...



- **Challenge-Response** (slight modification of normal behavior w.r.t. system dynamics)
  - Control Theory & LTI models (*linear time invariant models*)
- Challenge: u_t ; Response: y_t
- Then, statistical analysis w.r.t. u_t & y_t :

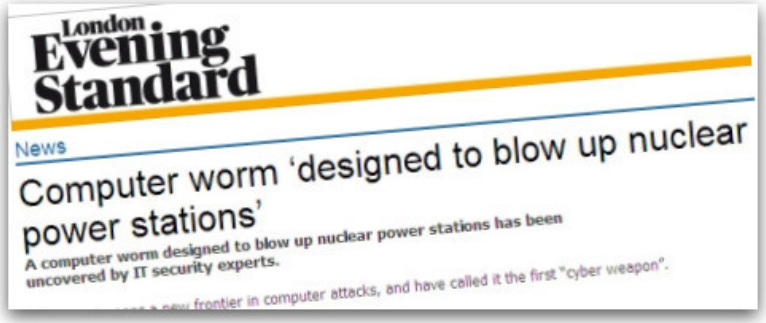
$$g_t = \sum_{i=t-w+1}^{t} (y_i - C\hat{x}_{i|i-1})^T \mathcal{P}^{-1} (y_i - C\hat{x}_{i|i-1})$$

- **If g_t exceeds the threshold ⇝ raise alert**

[*] Garcia-Alfaro *et al.*, « Cyber-Physical Attacks & Watermark-based Detection », *11th Intl. ARES Conference*, ***Best Paper Award***, Aug 2016 ; & **Keynote** ESORICS 2016 workshops, Sep 2016

Initial Motivations

- Malware moving from IT Systems to Operational Systems
- Wrong configurations, lack of encryption, legacy (vulnerable) systems, third party access, ...


London Evening Standard

News

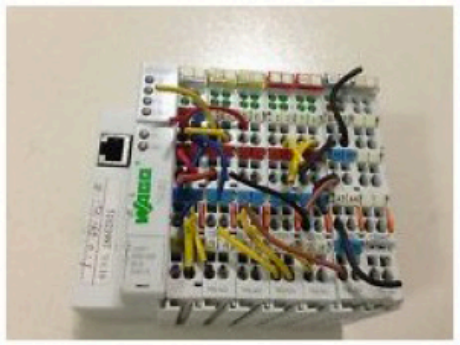
Computer worm 'designed to blow up nuclear power stations'

A computer worm designed to blow up nuclear power stations has been uncovered by IT security experts.

Proposed Methodology

- Foster new theoretical models,
- simulate/emulate case scenarios,
- ***validate results using training & testbeds***

Preparing the Testbeds



WAGO I/O system 750-842 750-402
750-404 750-559 -750-600

From China

Top-rated seller

$400.00
Buy It Now

Free shipping

http://j.mp/1vGPIVp

Siemens S7 300 PLC Trainer, 8
inputs 8 outputs USB/MPI

Learn how to program Siemens PLC's,
NO Software

Top-rated seller

$499.99
Buy It Now

http://j.mp/1qViIsG

LEGO Mindstorms EV3 Intelligent Brick # 95646c01
Brand New

Top Rated
Plus

$159.98
Buy It Now

36 Watchers

http://j.mp/1lEAxDP

SCADA Protocols (non exhaustive list)

- Siemens quad 4 meter
- CONITEL 2000
- CONITEL 2100
- CONITEL 3000
- CONITEL 300
- HARRIS 5000
- HARRIS 5600
- HARRIS 6000
- UCA 2.0 or MMS
- PG & E 2179
- **MODBUS**
- **DNP3**
- IEC 61850
- …

Sample protocols

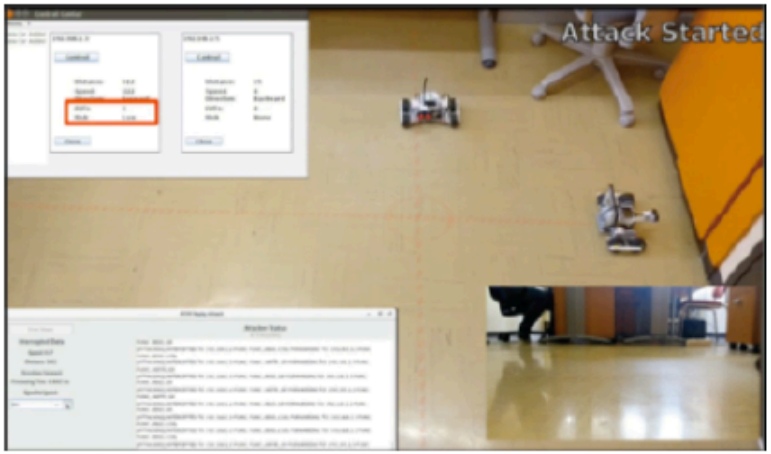
- MODBUS -Primitive with no security and not very extensible
- DNP3 –Advanced SCADA protocol
  - DNP1 and 2 are proprietary protocols

Sample Testbeds

(a) Bridge and toll testbed

(b) Industrial chain testbed

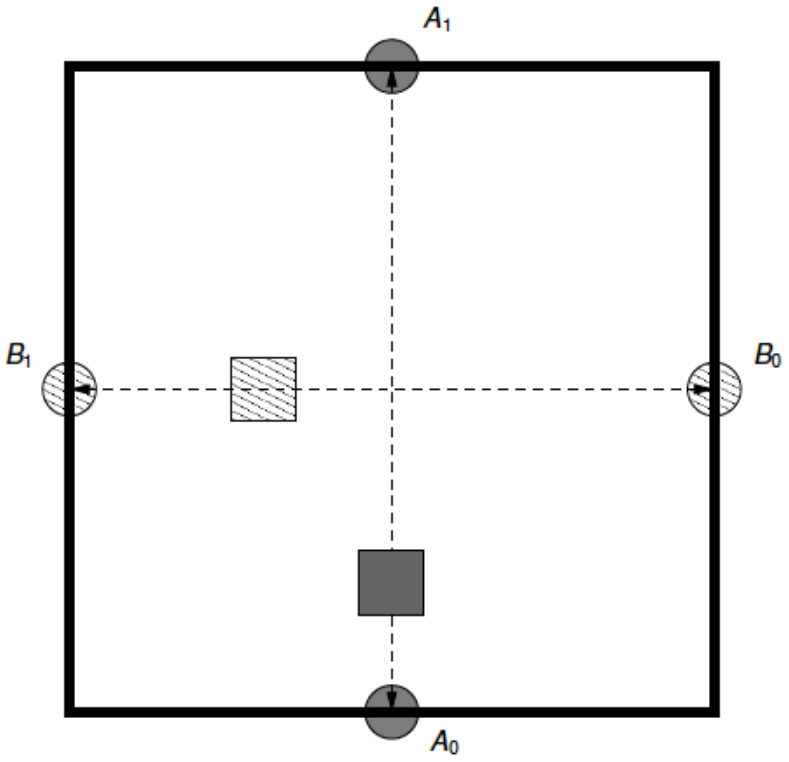
(c) Railway control testbed



(d) Autonomous industrial agents testbed

http://j.mp/TSPScada

Sample Testbed (autonomous agents testbed)



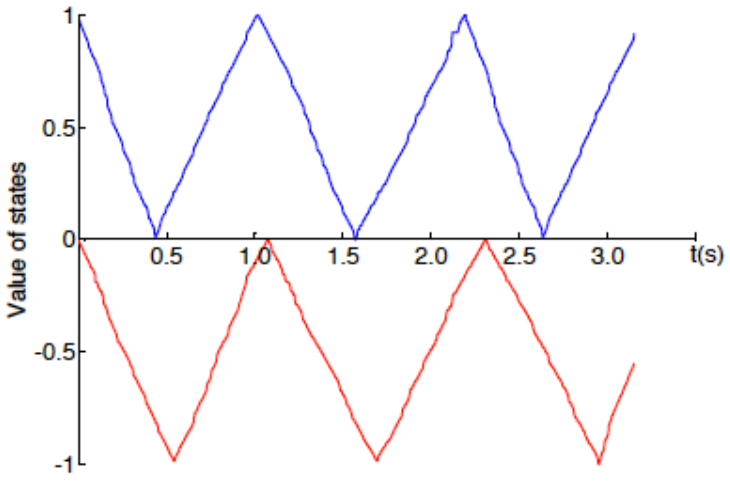
Cyber-physical industrial scenario implemented in the testbed

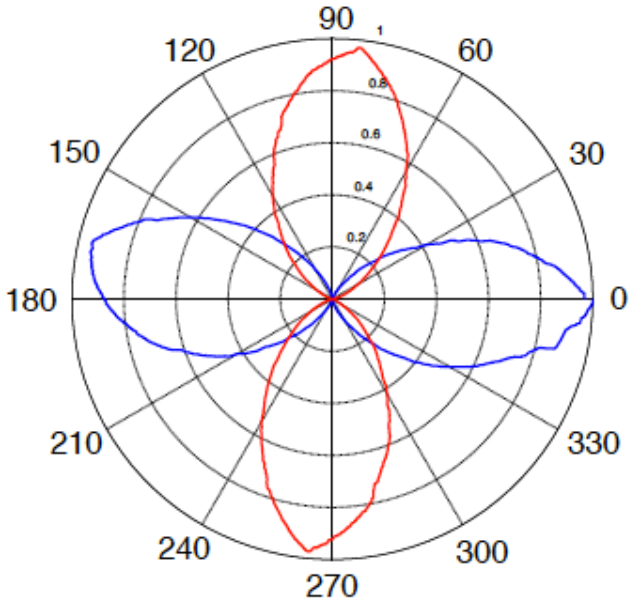
Attacks & Adversaries Implemented

- *Replay Attack*
  - Watermark Disabled
  - Watermark Enabled
- *Non-parametric Attack*
  - Stationary Watermark
  - Non-stationary Watermark
- *Parametric Attack*
  - Stationary Watermark
  - Non-stationary Watermark
- *New Parametric Attack*
  - PIETC-WD strategy

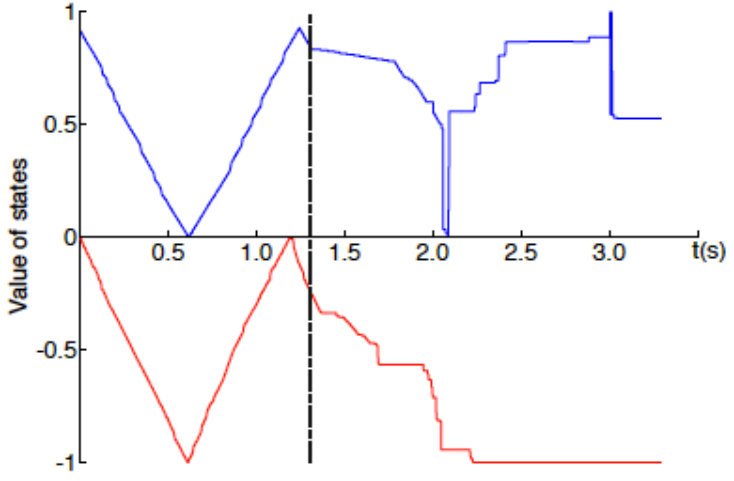
http://j.mp/TSPScada

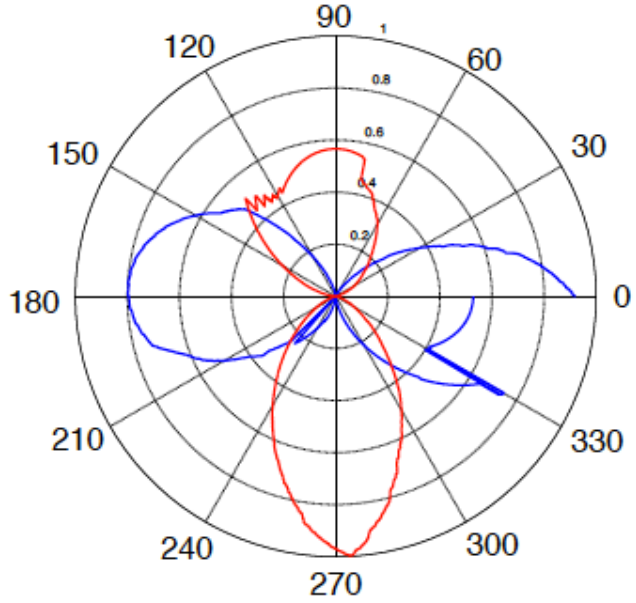
Linear & Polar Representation





Normal Mode

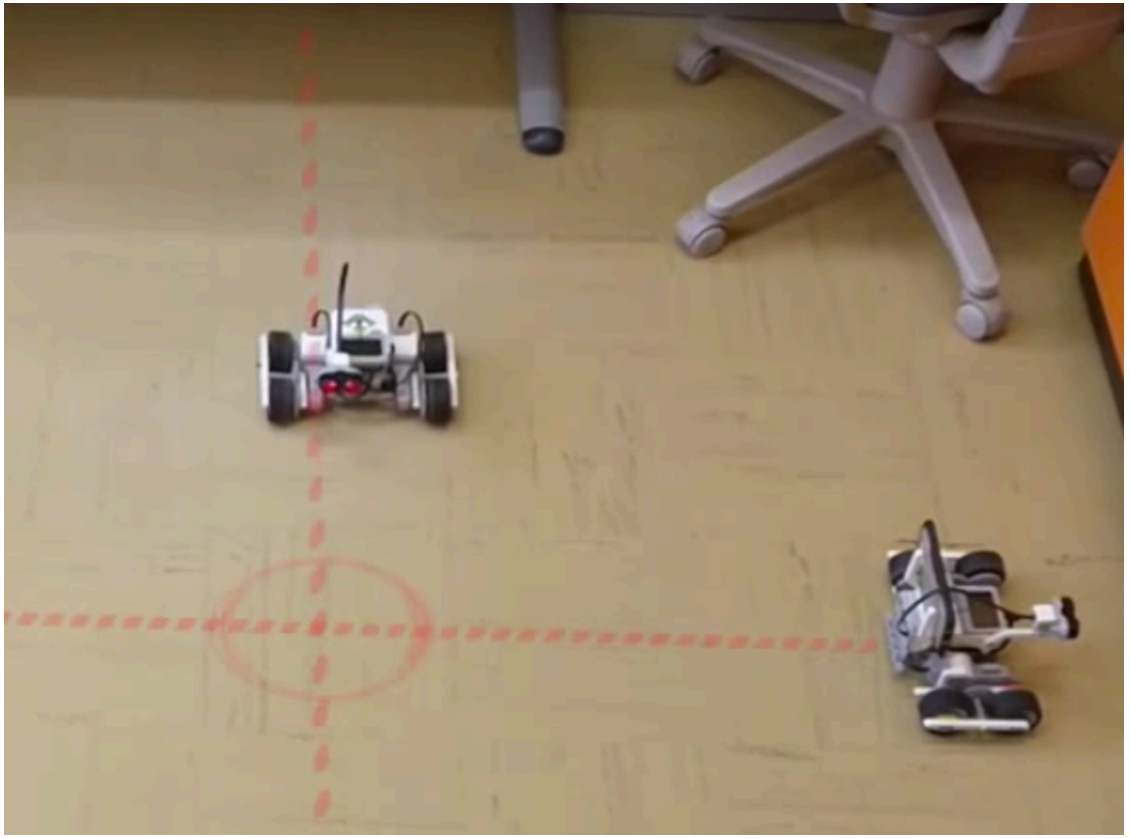




Under Attack

Testbed Validation

- Modeled as games?
  - http://j.mp/WikiGTP
- Defender
  - Avoid collisions
- Attacker
  - Force collisions



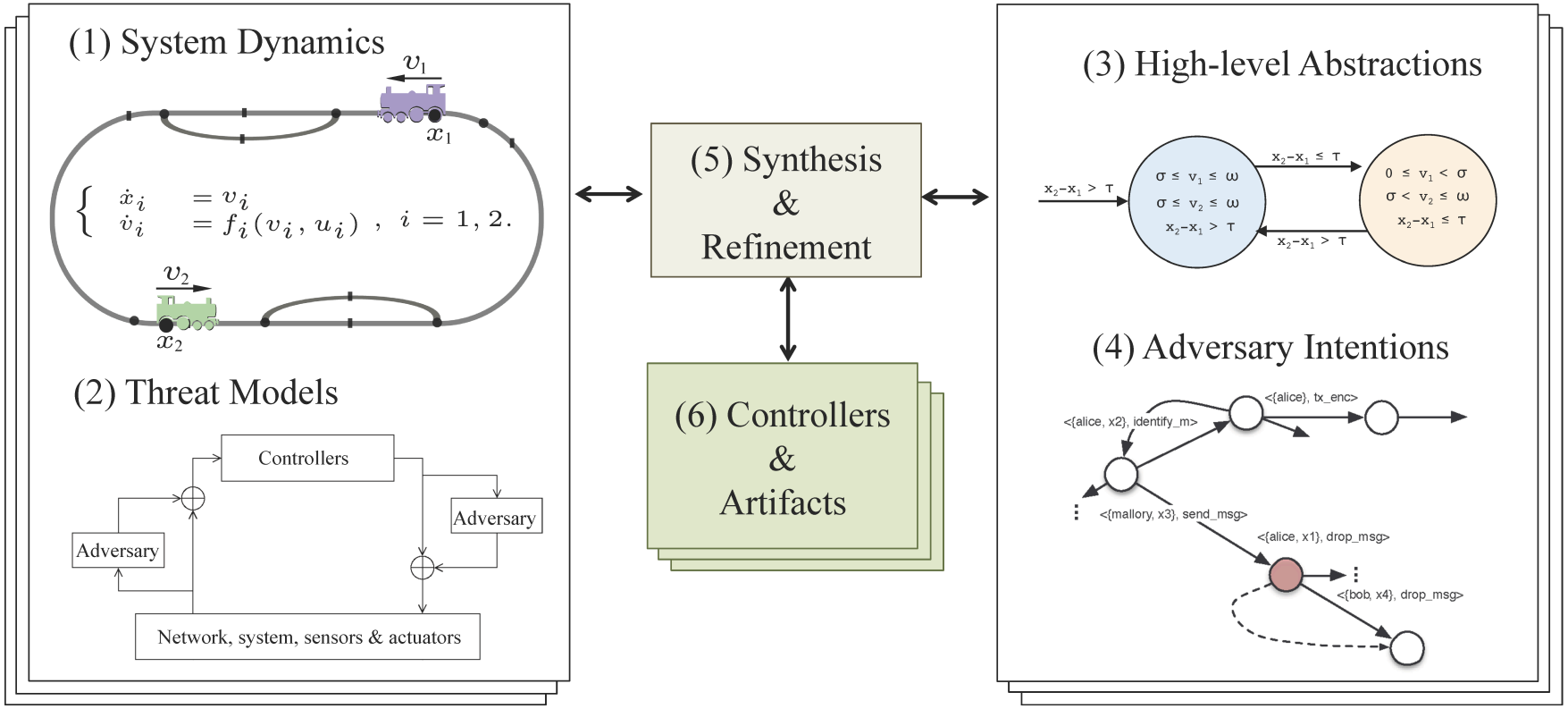
http://j.mp/TSPScada

Outline

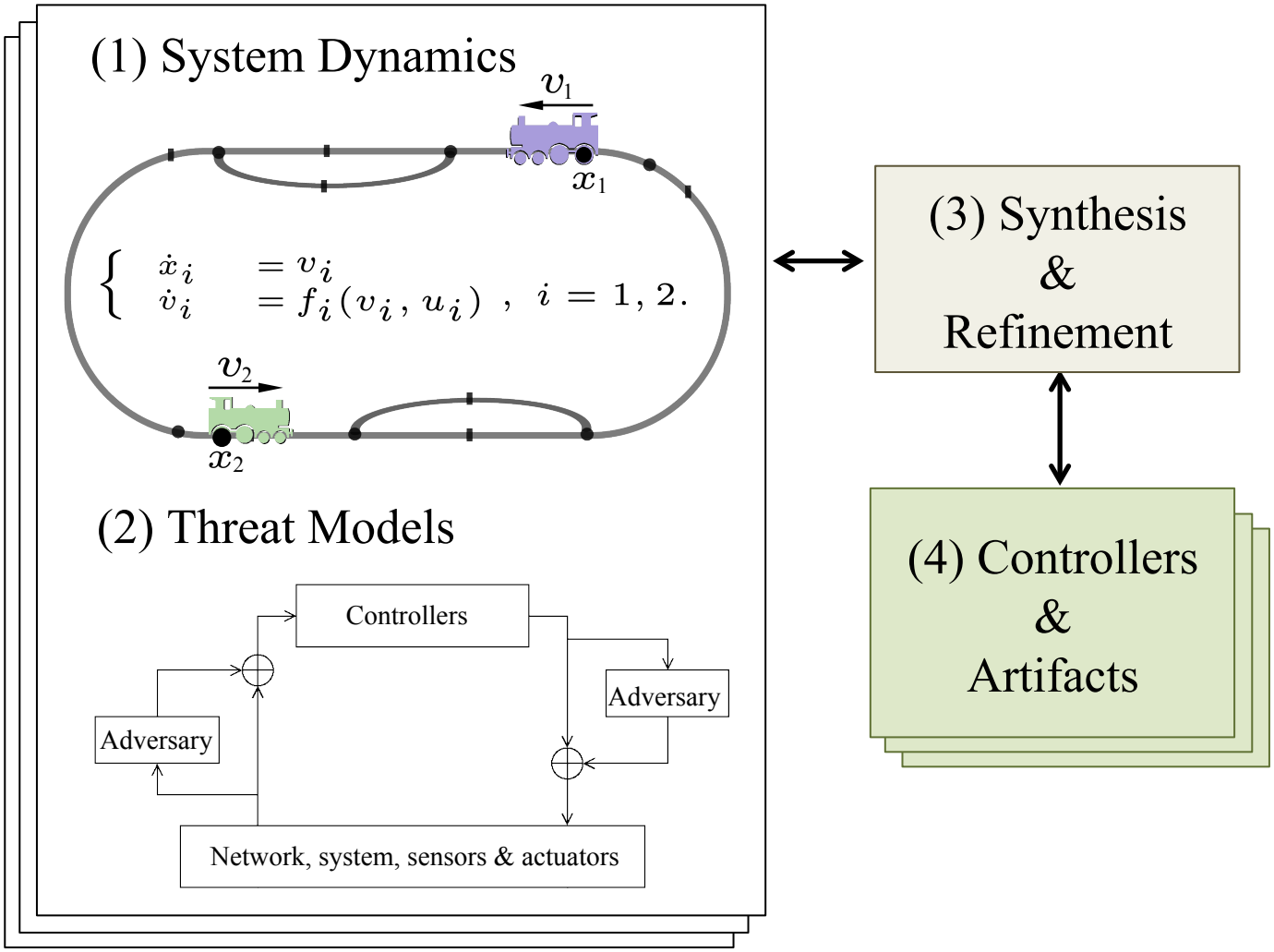
- Experience & Context
  - Cyber-Physical Systems
- Feedback Truthfulness (FT)
- **Ongoing Work on FT Distinguishability**
- **Summary & Perspectives**

Feedback Truthfulness Distinguishability

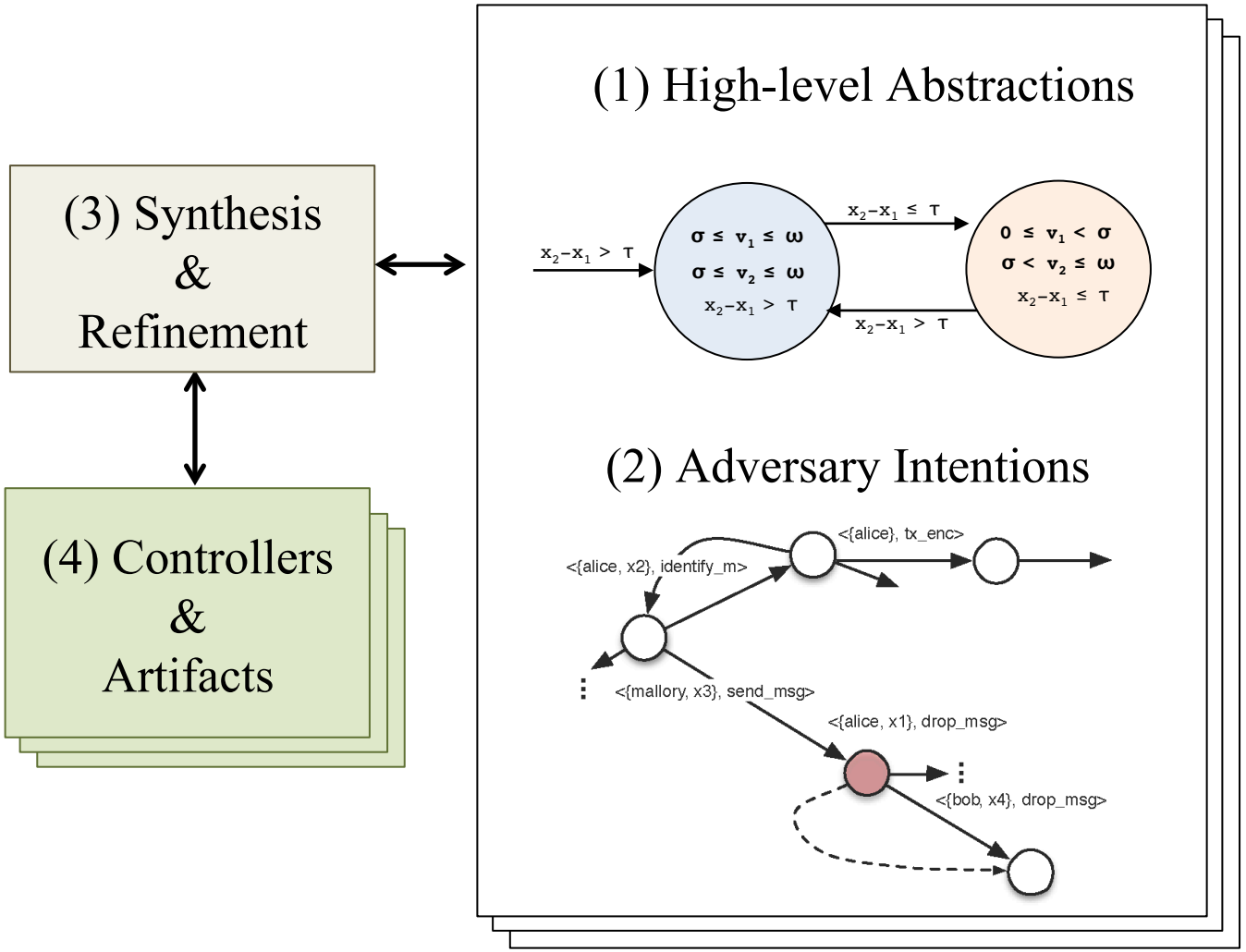
- Distinguishing accidental failures and intentional manipulation
- Top-down refinement of automated runtime verification



Feedback Truthfulness Distinguishability



Feedback Truthfulness Distinguishability



Outline

- Experience & Context
  - Cyber-Physical Systems
- Feedback Truthfulness (FT)
- Ongoing Work on FT Distinguishability
- **Summary & Perspectives**

Summary

- Challenging, multidisciplinary topic
  - Dynamic (networked-control) systems & data truthfulness
- Traditional ICT-based security may still be applicable
  - However, they cannot solve the problem completely
    - Fundamental differences between IT systems & CPSs
- Modeling, from a control-theoretic perspective, shall
  - Pay attention to adversary strategies from the attacker's angle
  - Assume attackers with knowledge about information systems & physical systems at the same time
- Perspectives
  - Automated techniques for the verification of feedback truthfulness distinguishability is a *must*

Thank You. Questions?

References

- Hirschmann. Why is Cyber Security Still a Problem? *TOFINO Security Series, 2010*
- Kim & Kumar. Cyber–Physical Systems: A Perspective at the Centennial. *Proceedings of the IEEE*, Vol. 100, pages 1287-1308, May 2012.
- Krotofil & Larsen. Hacking Chemical Plants for Competition and Extortion, *DefCon23, 2015*
- Texeira et al. A secure control framework for resource-limited adversaries. *Automatica*, 51(1): 135-148, 2015.
- Wu, Sun & Chen. A survey on the security of cyber-physical systems. *Control Theory and Technology*, 14(1):2–10, February 2016.
- Rubio, De Cicco, & Garcia-Alfaro. Revisiting a Watermark-based Detection Scheme to Handle Cyber-Physical Attacks. *ARES 2016*, ***(best paper award)***, August 2016.
- Mo, Weerakkody & Sinopoli. Physical Authentication of Control Systems. *IEEE Control Systems*, Vol. 35, pages 93–109, 2015.