Cyber Physical System Security SC4015/CE/CZ4055

Anupam Chattopadhyay
CCDS, NTU

Contents

NANYANG TECHNOLOGICAL UNIVERSITY

Tutors, and, Assistants

- **Lecturers**
  - Anupam Chattopadhyay (anupam at ntu.edu.sg)

- **Teaching Assistants**
  - Sayan Das (sayan005 at e dot ntu dot edu dot sg)
  - Prasanna Ravi Kant (prasanna dot ravi at ntu dot edu dot sg)
  - Peizhou Gan (peizhou dot gan at ntu dot edu dot sg)
  - Kamal Raj (kamal dot raj at ntu dot edu dot sg)

Schedule

- **Lectures**
  - Thursdays 14:30 - 16:30 PM (LT27)
- **Tutorials** *(starts from Week 2)*
  - Thursdays 16:30 - 17:30 PM (LT27)
- **Laboratory Assignments** *(starts from Week 8)*
  - Tuesdays 12:30 – 16:30 PM (TEL1, TEL3 – HWLAB1)
  - Fridays 12:30 – 16:30 PM (TEL2, TEL4 – HWLAB1)
- *(check for updated schedule in NTULearn)*

Schedule (*Part-Time)*

- **Lectures**
  - Thursdays 18:30 - 20:30 PM (TR+29)

- **Tutorials** *(starts from Week 2)*
  - Thursdays 20:30 - 21:30 PM (TR+29)

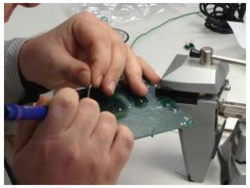
- **Laboratory Assignments** *(starts from Week 6)*
  - Thursdays 18:30 – 21:30 PM (HWLAB1)

- *(check for updated schedule in NTULearn)*

NANYANG TECHNOLOGICAL UNIVERSITY

What will we learn?

- Cyber Physical Systems are everywhere around us
  - You are using it
  - You will possibly *design/secure* it as part of your future career
  - You may end up discovering/innovating/using it



- We will learn
  - ***Basic principles*** of their design
  - How to address the ***Security issues***
  - ***Abstract concepts*** with tutorials
  - ***Practical concepts*** with prototyping boards

NANYANG TECHNOLOGICAL UNIVERSITY

Course Evaluation

• **2-hour Written Examination (closed book)**	**50%**
• **(New) Class Attendance through Wooclap**	**5%**
• **Quiz 1**	**10%**
• **Quiz 2**	**10%**
• **Lab 1+2 Report**	**5%**
• **Lab 3+4 Report**	**5%**
• **Project Report**	**15%**

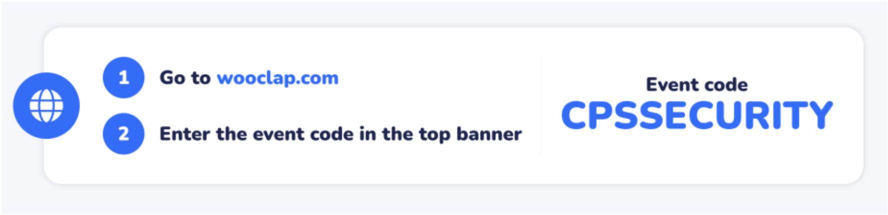
  - Project problems will be introduced during the labs

- Note 1: All practical sessions will be held at HW Lab 1
- Note 2: All practical and projects can be performed in a group of size 1/2/3

NANYANG TECHNOLOGICAL UNIVERSITY

Course Feedback, Discussions

- Your opinion matters
  - Provide feedback to the tutor/assistants on things you (dis)liked
  - Share your opinion through NTU student feedback system
- Discussion
  - It is important that you participate in course discussions
    - In classroom (through wooclap *or* after the lecture)
    - By Email/Course Discussion Board
    - By appointment with tutors/assistants



Attendance

NANYANG TECHNOLOGICAL UNIVERSITY

Course Contents

- Introduction
  - Cyber Physical Systems, Internet-of-Things; Security
- Attack Surfaces
  - Network, Control, Computing, Storage
- Device-level Security
  - Microprocessors
- Secure Key Management
  - Distributed CPS, Biometrics
- Secure Communication
  - Communication protocols and attacks
- CPS Security Applications
  - Smart Card, Smart Grid, Smart Vehicle
- Guest Lectures (will not be tested)
  - Side-channel Attacks; AI Security

NANYANG TECHNOLOGICAL UNIVERSITY

Reference Materials

- Books
  - Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC press, fifth printing, August 2001, http://cacr.uwaterloo.ca/hac/
  - Digital Integrated Circuits (2nd Edition), Jan M. Rabaey, A. Chandrakasan and B. Nikolic, Pearson, https://www.amazon.com/Digital-Integrated-Circuits-2nd-Rabaey/dp/0130909963
  - Edward A. Lee and Sanjit A. Seshia, Introduction to Embedded Systems, A Cyber-Physical Systems Approach, Second Edition, http://LeeSeshia.org, ISBN 978-1-312-42740-2, 2015
  - High-Performance Embedded Computing: Applications in Cyber-Physical Systems and Mobile Computing by Marilyn Wolf, Morgan Kaufmann, 2nd Edition, 2014
- Reference materials and links will be indicated for each topic in the slides/ lecture notes.

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- Course Organization
- *Cyber Physical Systems*
- Security
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

Where are the Cyber Physical Systems?

NANYANG TECHNOLOGICAL UNIVERSITY

Principle I: Hidden

- Embedded Systems are designed to be "embedded", i.e., these are not explicit like a desktop

- Example: for a sailing boat, embedded system is needed for
  - Wind direction/speed assessment/prediction
  - Current sailboat position/direction/speed/acceleration assessment
  - Competitors' position/speed assessment
  - Strategy evaluation and execution (speed/direction)

NANYANG TECHNOLOGICAL UNIVERSITY

Tae Kwon Do: Who is the Winner?

NANYANG
TECHNOLOGICAL
UNIVERSITY

The Electronic Scoring System

Where is the CPS?

NANYANG TECHNOLOGICAL UNIVERSITY

Principle II: Everywhere

- Embedded Systems can be found/everywhere. It is pervasive.
- For a taekwondo armor, it is used for
  - Impact detection (scoring)
  - Concussion detection (medical emergency)
  - Heart rate, body vital sign detection, audio/video recording (training)

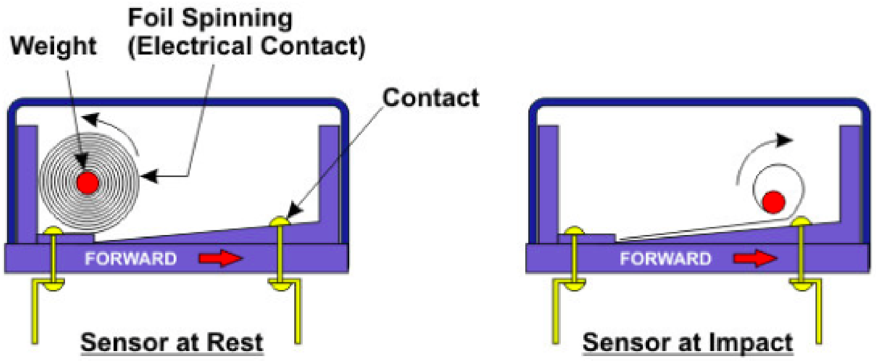


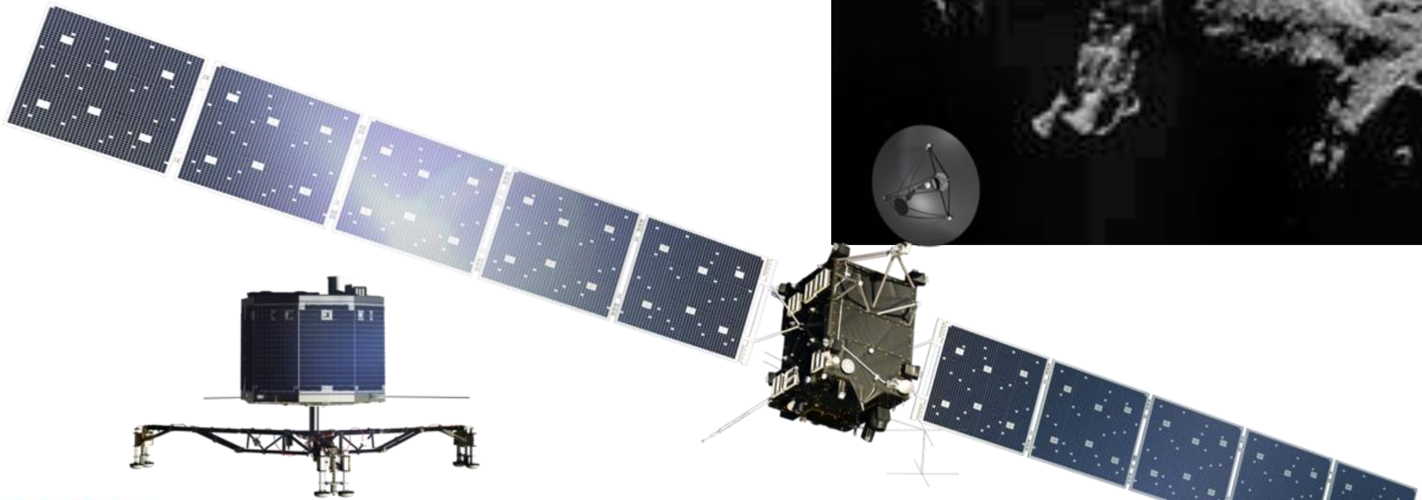
Figure 2. *Functional principle to a typical roller type airbag sensor. Source: Erjavec, J. (2010). Automotive Technology: A Systems Approach. New York: Delmar, Cengage Learning.*

NANYANG TECHNOLOGICAL UNIVERSITY

Principle III: Complex

Complexity is the enemy of Security

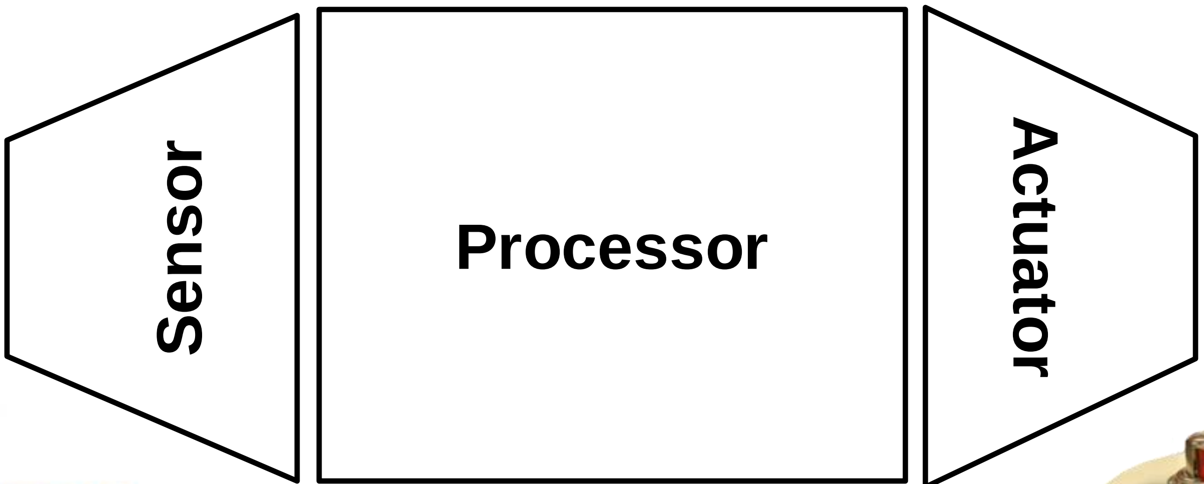
- Comet Churyumov-Gerasimenko
- Satellite Rosetta (Launched 2004)
- Lander Philae (Landed 2014)

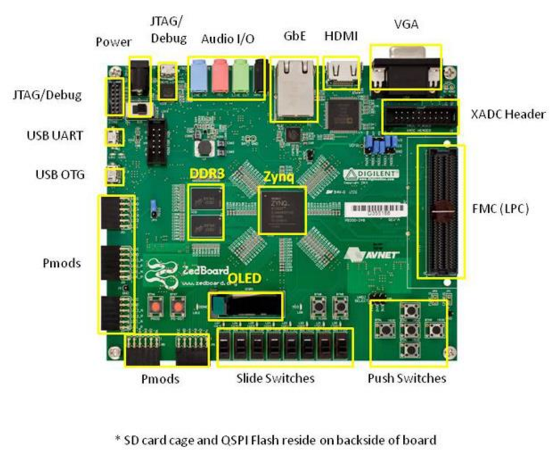


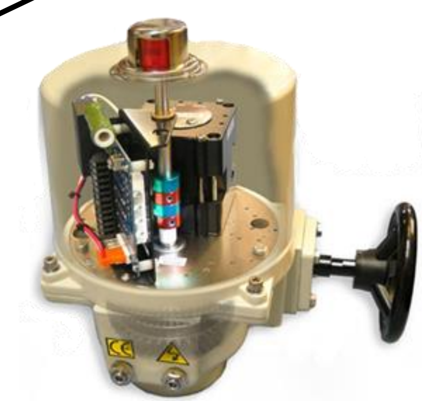
Embedded Systems (CYBER PHYSICAL SYSTEM)

everything here is important!

- **Complex, Hidden, Everywhere**

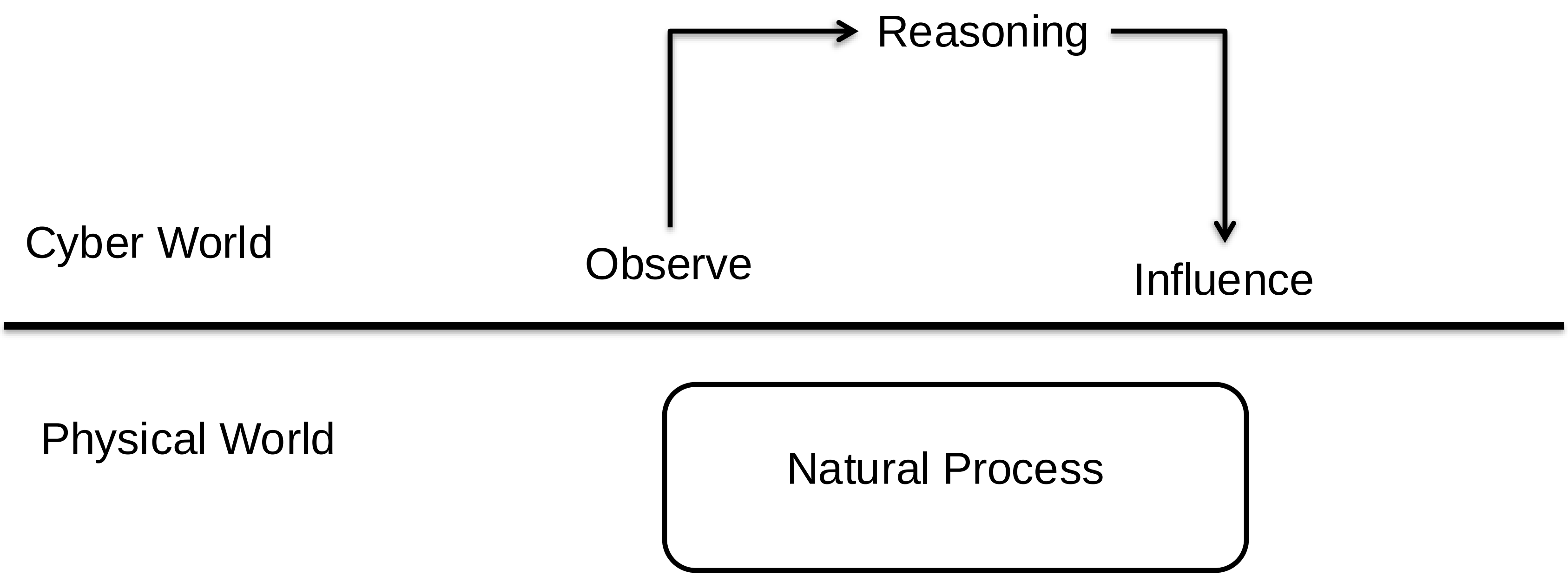






NANYANG TECHNOLOGICAL UNIVERSITY

Why **Cyber-Physical Systems**



Characteristics of CPS

- Must be ***robust***:

- Reliability: $R(t)$ = probability of system working correctly, provided that it was working at $t=0$
- Maintainability: $M(d)$ = probability of system working correctly d time units after error occurred.
- Availability: probability of system working at time t
- Safety: no harm to be caused
- Security: confidential and authenticated communication, control and storage

NANYANG TECHNOLOGICAL UNIVERSITY

Characteristics of CPS *(contd.)*

- ***Must be efficient:***
  - Energy efficient
  - Code-size and data memory efficient
  - Run-time efficient
  - Weight efficient
  - Cost efficient

- ***Dedicated towards a certain application:*** Knowledge about behavior at design time can be used to minimize resources and to maximize robustness.

NANYANG TECHNOLOGICAL UNIVERSITY

Characteristics of CPS *(contd.)*

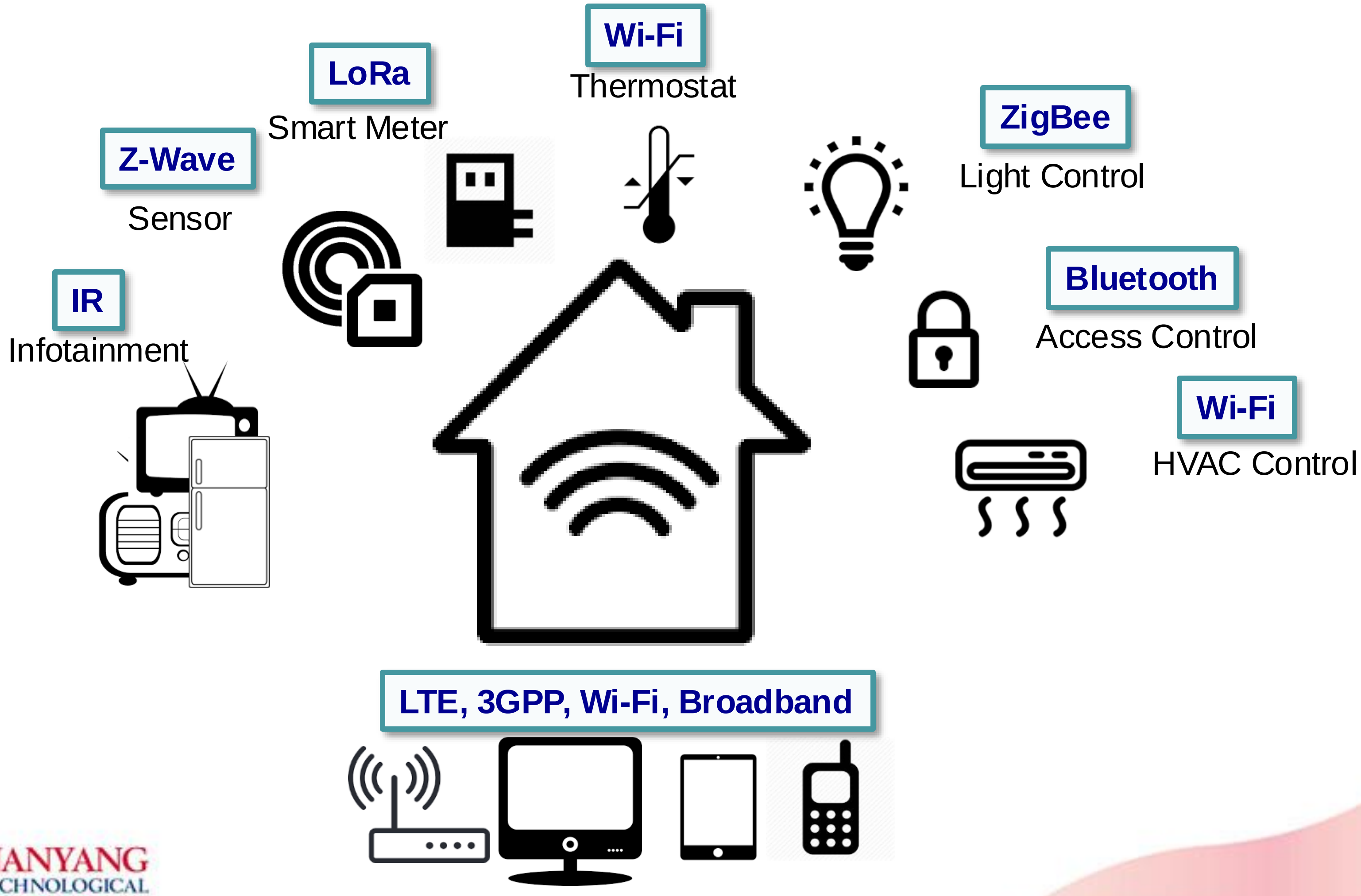
- Many CPS ***must meet real-time constraints***:
  - A real-time system must react to stimuli from the controlled object (or the operator) within the time interval dictated by the environment.
- For real-time systems, right answers arriving too late are wrong.
  - ”A real-time constraint is called ***hard***, if not meeting that constraint could result in a catastrophe“ [Kopetz, 1997].

- All other time-constraints are called ***soft***.

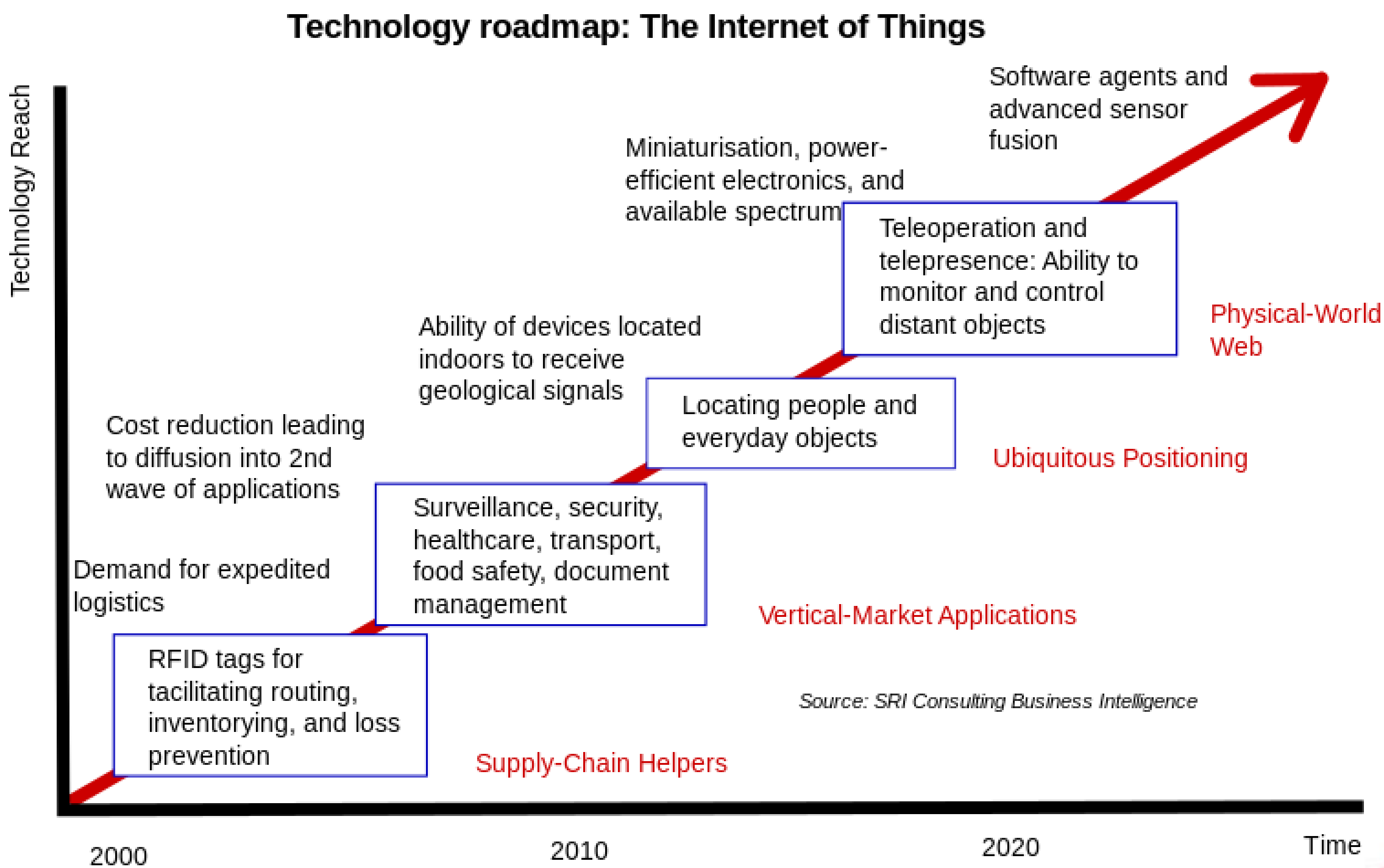
NANYANG TECHNOLOGICAL UNIVERSITY

What about Internet-of-Things (IoT) ?

Internet of Things (IoT)



IoT Proliferation



IoT + AI: Distributed and Autonomous Agents

- Spoofing cameras through adversarial objects
  - Multiple cameras is a potential solution but, no guarantee
  - Explored hybrid solutions, including color palette reduction

Cao, Y., et al Invisible for both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks. 2021 IEEE Symposium on Security and Privacy (S&P)

NANYANG TECHNOLOGICAL UNIVERSITY

What did we learn so far?

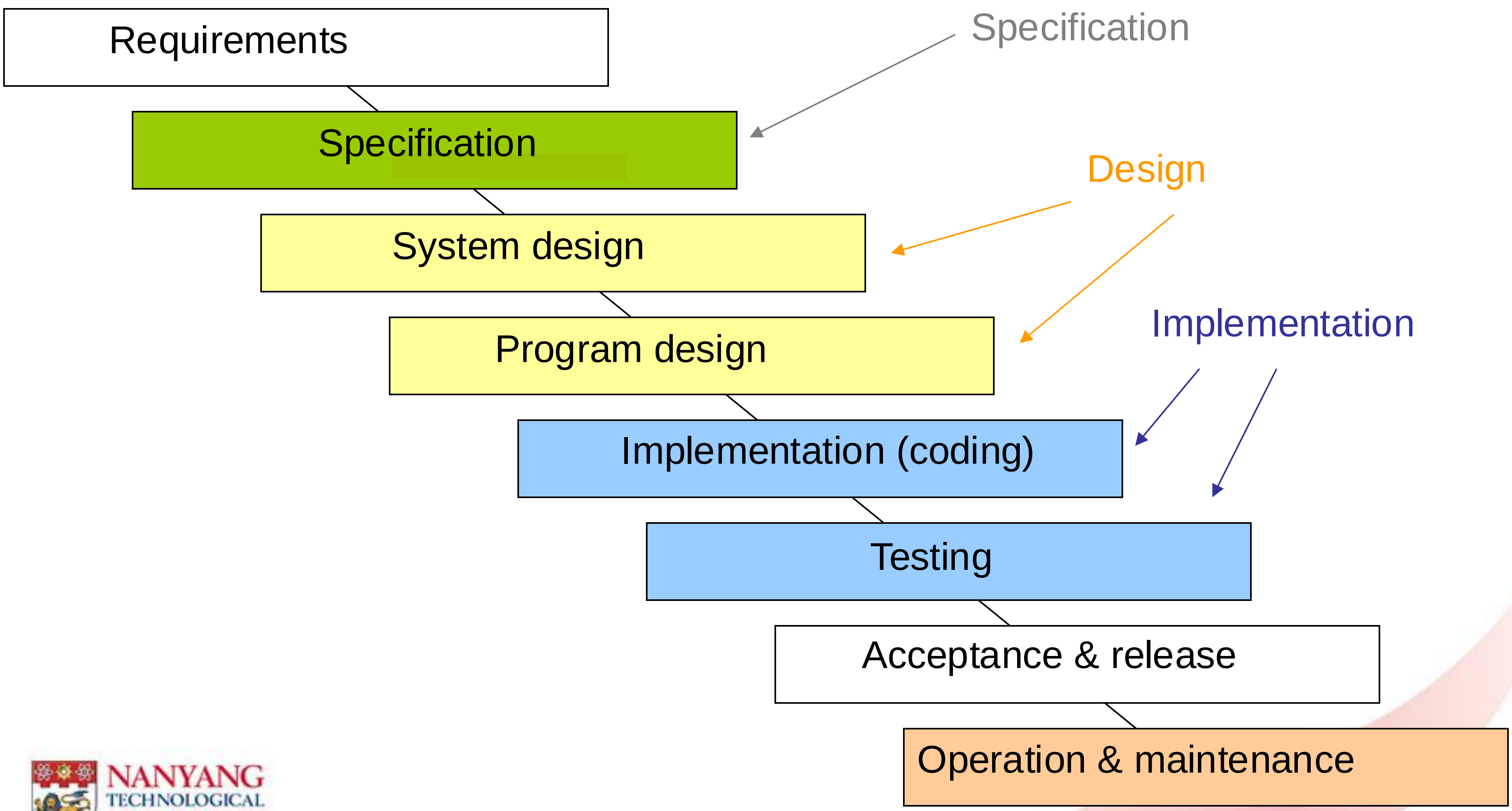
- What is Cyber-Physical Systems/Internet-of-Things ?
- Where can we find it?
- How to design/secure one?
  - ***Next slides…***

Contents

- Course Organization
- *Cyber Physical Systems*
    - ***Design Techniques***
- Security
- Discussion

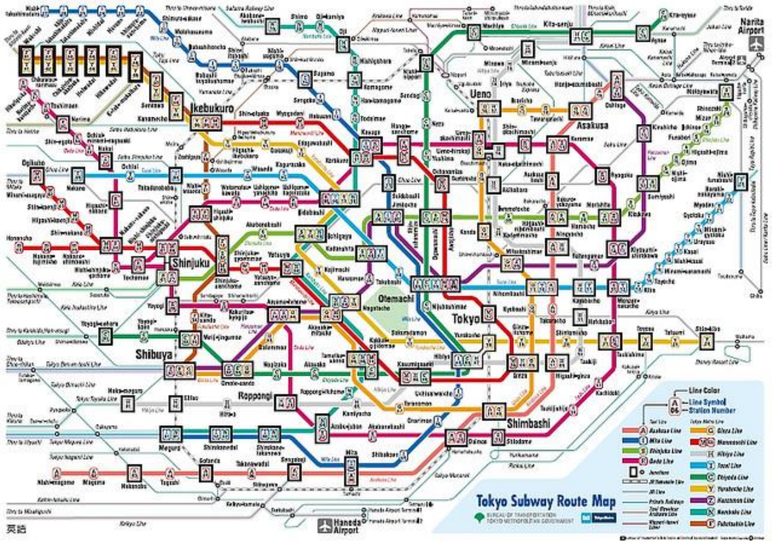
Partly covered in CE4051

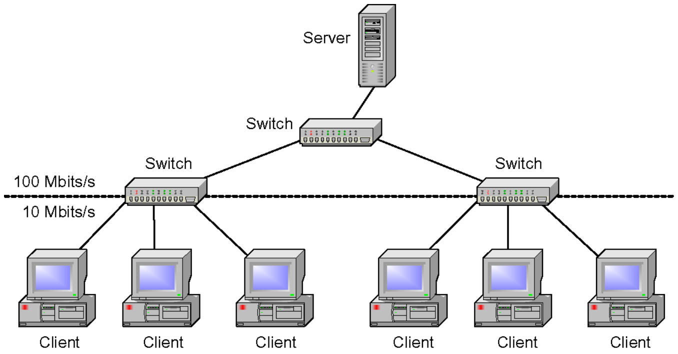
Design Technique: Waterfall Model



Specification

- Represent hierarchical computation and communication
  - Humans are not capable of understanding systems containing more than a few objects
  - Most actual systems require more objects → Hierarchy



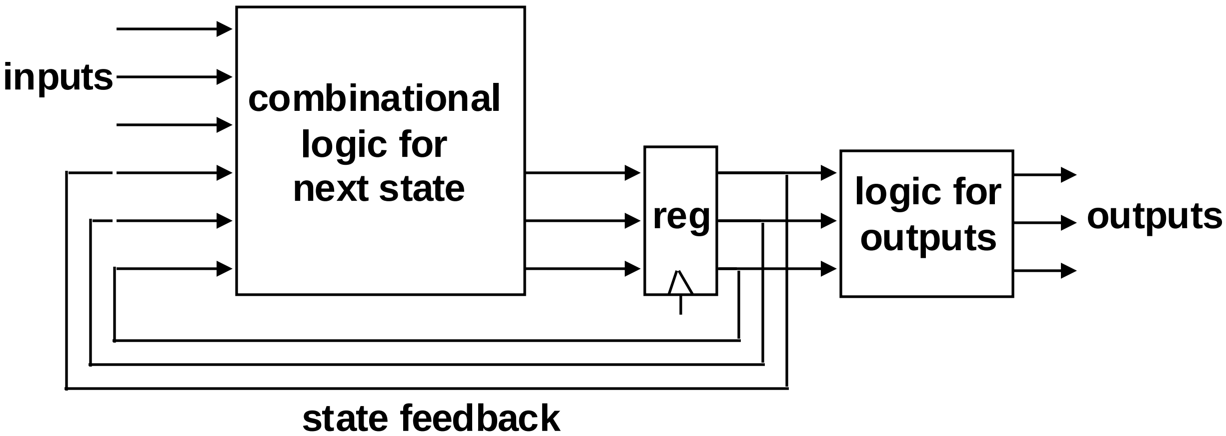


NANYANG TECHNOLOGICAL UNIVERSITY

FSMs: Mealy/Moore

- Moore/Mealy machines
- These are two different ways to express the FSMs with respect to the output.
- Both have different advantages so it is good to know them.

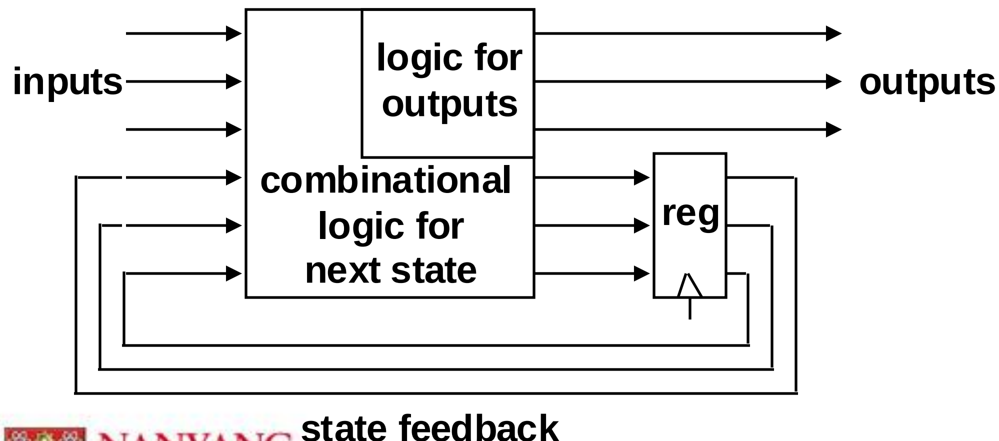
Moore versus Mealy machines



Moore machine

Outputs are a function of current state

Outputs change synchronously with state changes



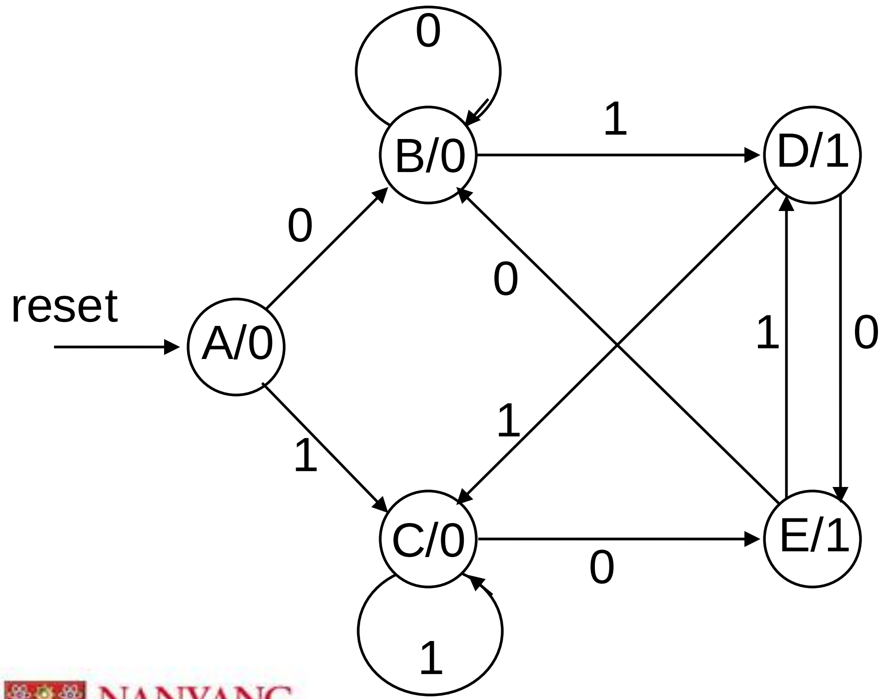
Mealy machine

Outputs depend on state and on inputs

Input changes can cause immediate output changes **(asynchronous)**

Example "01 or 10" detector: a Moore machine

- Output is a function of state only
  - Specify output in the state bubble

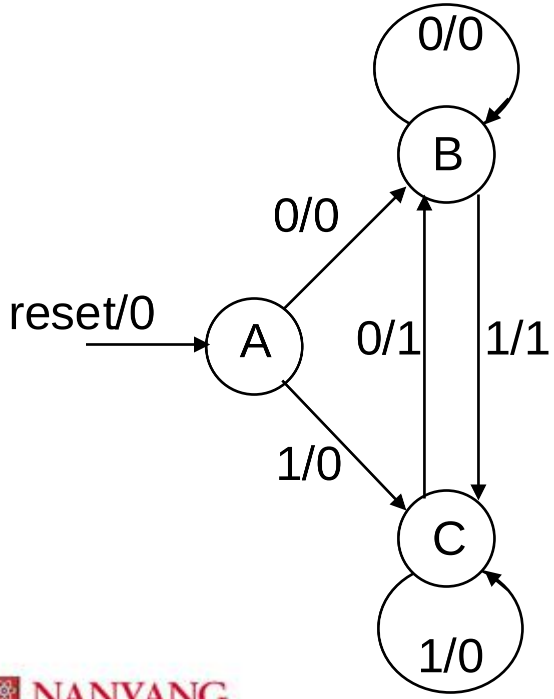


reset	input	current state	next state	current output
1	–	–	A	0
0	0	A	B	0
0	1	A	C	0
0	0	B	B	0
0	1	B	D	0
0	0	C	E	0
0	1	C	C	0
0	0	D	E	1
0	1	D	C	1
0	0	E	B	1
0	1	E	D	1

NANYANG TECHNOLOGICAL UNIVERSITY

Example "01 or 10" detector: a Mealy machine

- Output is a function of state and inputs
  - Specify outputs on transition arcs

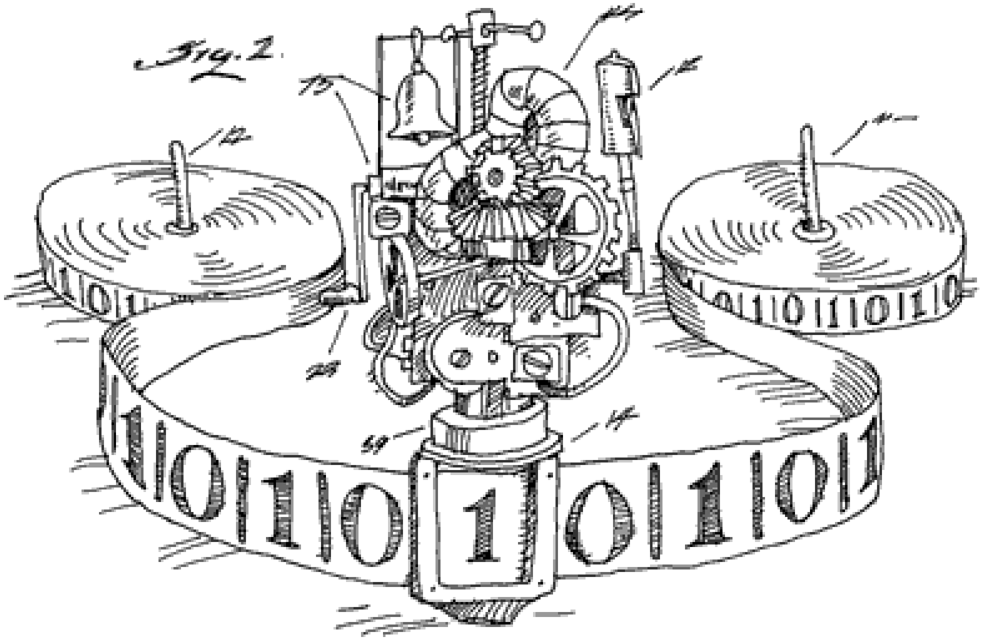


reset	input	current state	next state	current output
1	–	–	A	0
0	0	A	B	0
0	1	A	C	0
0	0	B	B	0
0	1	B	C	1
0	0	C	B	1
0	1	C	C	0

NANYANG TECHNOLOGICAL UNIVERSITY

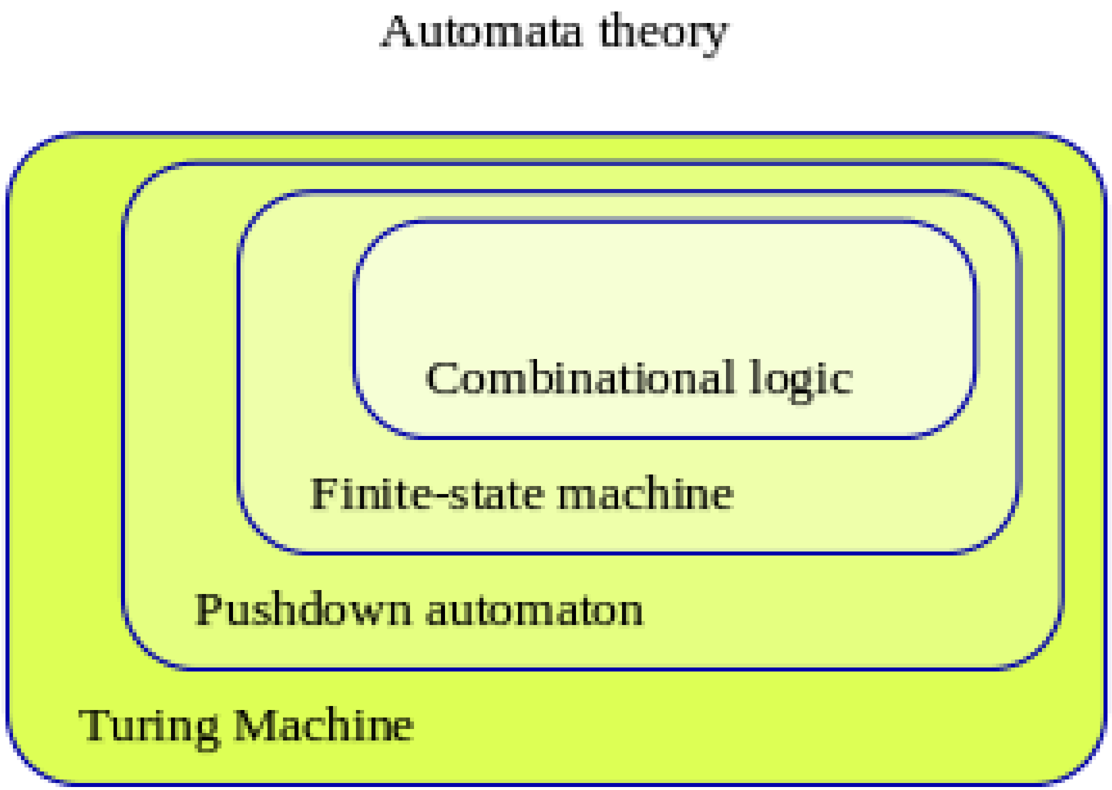
Component

- Turing Machine



On Computable Numbers, With An Application To The Entscheidungsproblem, by A. M. Turing, 1936

Computing power of components



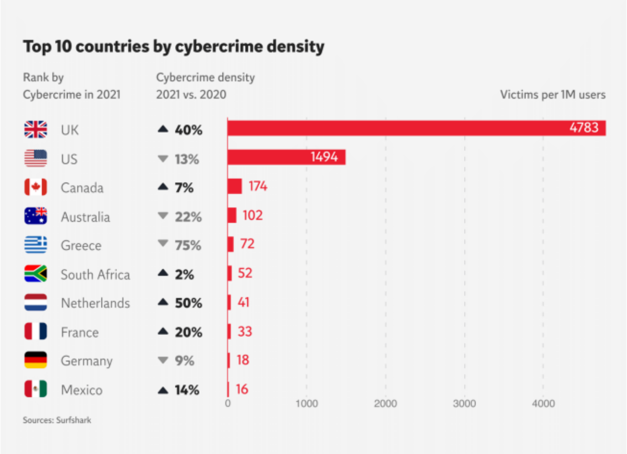
Contents

- Course Organization
- Cyber Physical Systems
- *Security*
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

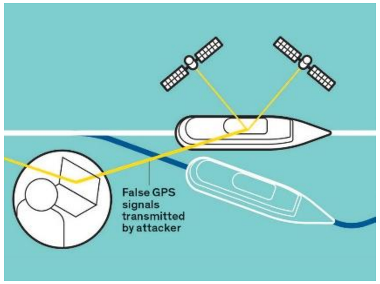
Cyber Crime

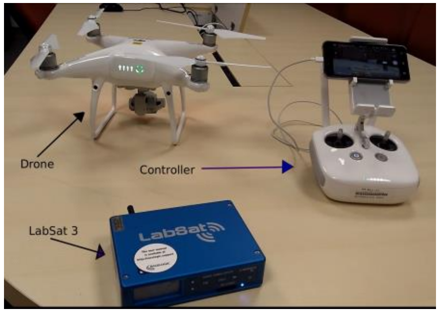
- Global annual cost of cyber crime to reach **$8 Trillion/year** in 2023.

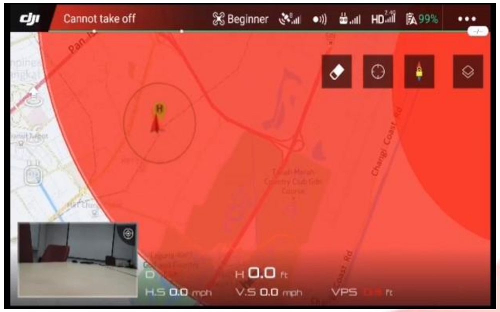


CPS/IoT Systems View

- Example: GPS Spoofing

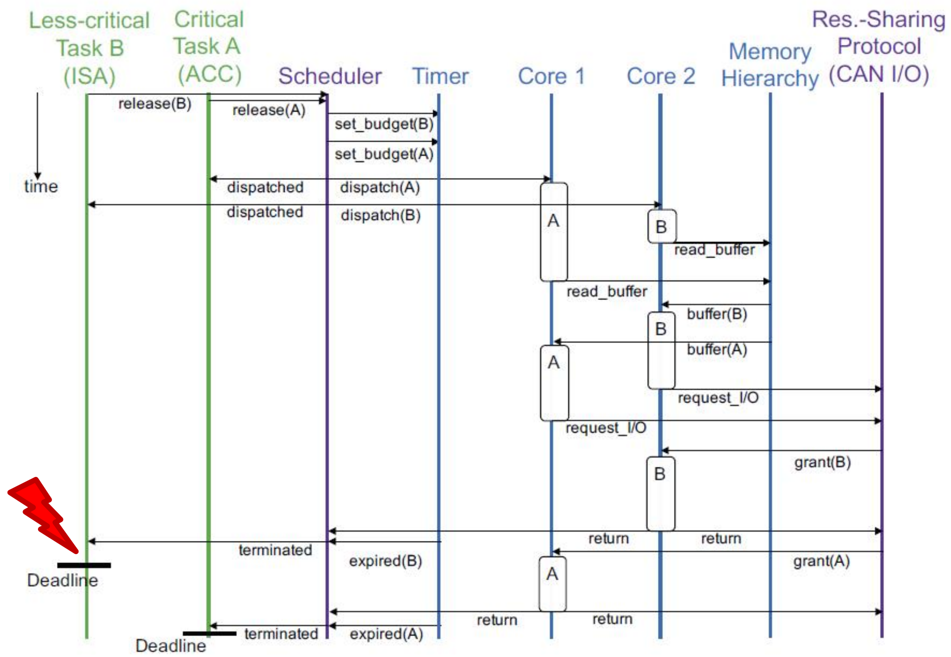






Real-Time Systems View

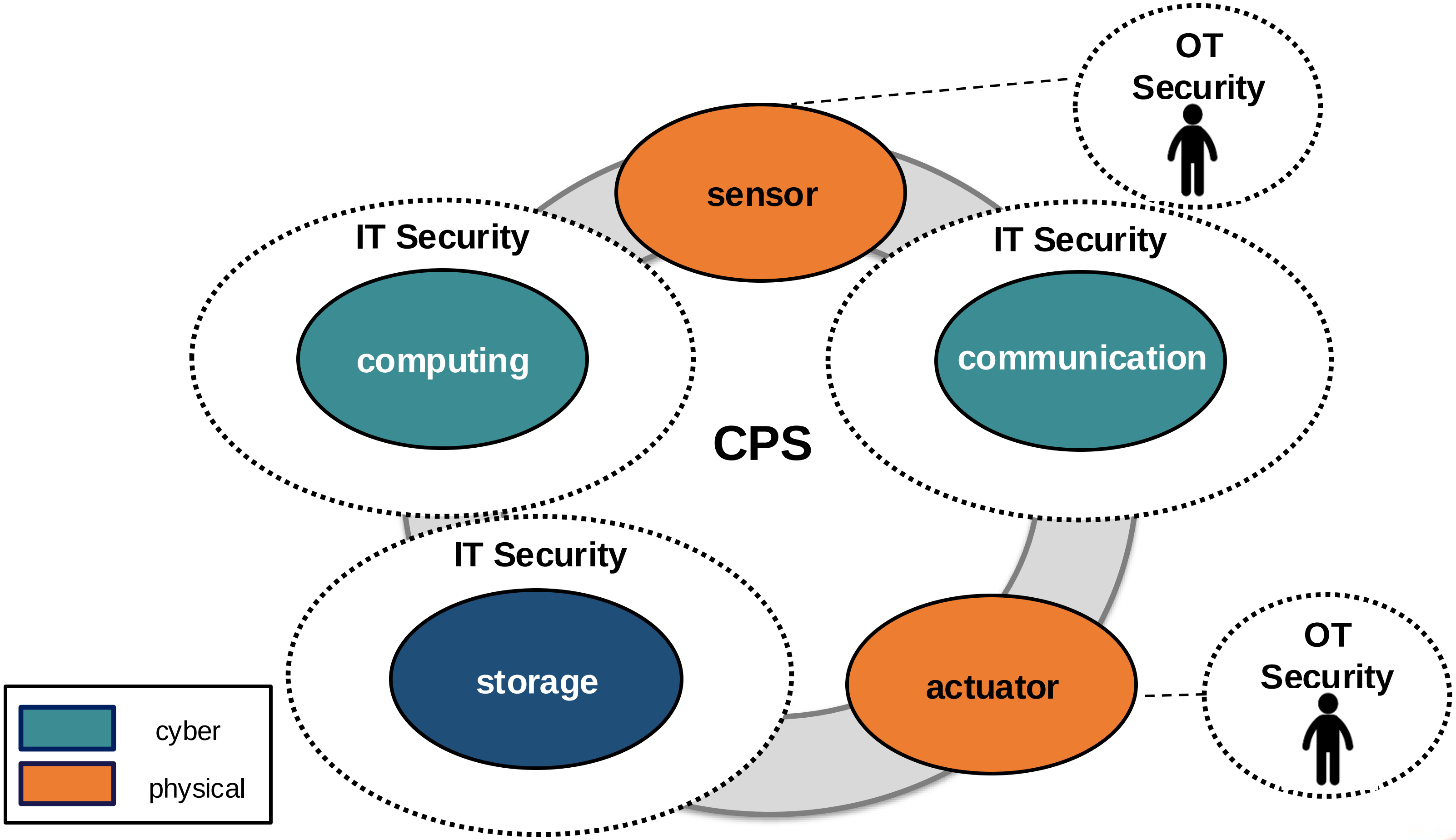
- Example: Deadline Miss



Arvind Easwaran, Anupam Chattopadhyay and Shivam Bhasin: A systematic security analysis of real-time cyber-physical systems. [*ASP-DAC 2017*]

NANYANG TECHNOLOGICAL UNIVERSITY

CPS Security View



What is Privacy?

- **Definitions**
  - "***Privacy is a basic psychological need***" S. M. Jourard, 1966
  - "***Privacy is necessary for managing social ties***", Chaikin, 1977
  - "***Privacy is critical for flexibly projecting and designing our self to others***", Goffman 1959, Vitak 2015

- **Privacy Laws**

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

France fines Google and Facebook €210m over user tracking

Data privacy watchdog says websites make it difficult for users to refuse cookies

China fines Didi $1.2 billion for violating cybersecurity and data laws

By Yong Xiong, Larry Register and Laura He, CNN Business
3 minute read · Updated 9:07 AM EDT, Thu July 21, 2022

NANYANG TECHNOLOGICAL UNIVERSITY

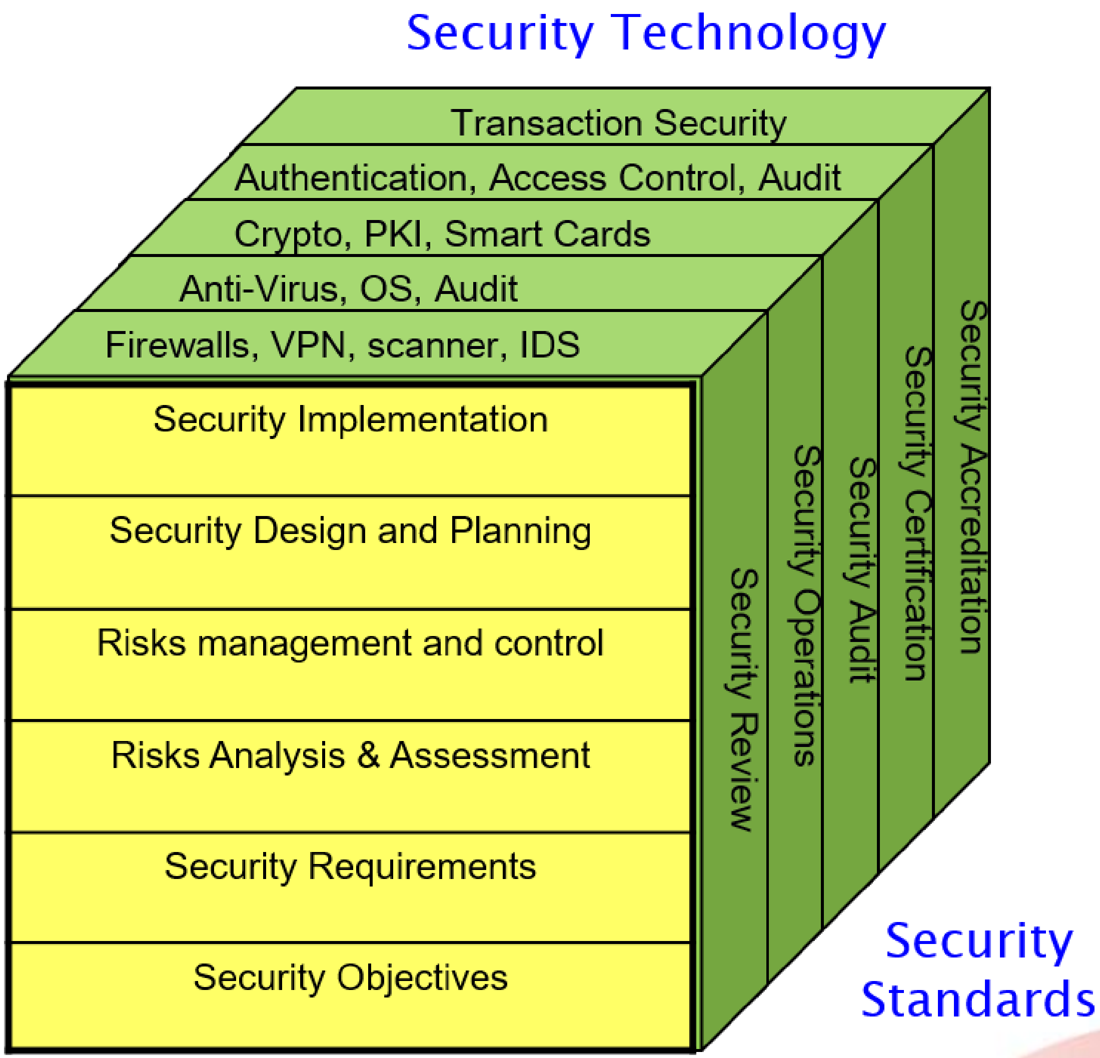
TVR Analysis

Rating system to quantify the security hazards

- **Threat**
  - External/Internal; Human/Machine
  - Example: Inadequately trained staff, Overheating
- **Vulnerability** Design Part
  - Exposure: Affects one/multiple components
  - Severity: Requires little/heavy resources to exploit, huge/minor loss. Cost/Impact Ratio and Adversarial Model.
- **Risk** Consequences
  - Organizational Impact. Economic, Brand Value, Life-threatening

NANYANG TECHNOLOGICAL UNIVERSITY

Security Management



What did we learn?

- **What is Model of Computation?**
  - What is CPS?
  - Components (FSM, Turing)
  - *Is your computer a Turing machine?*
- **What are the real-world implications of security?**
  - CPS security perspective from IT and OT
  - Real-time system perspective
  - TVR Model
  - Privacy

NANYANG TECHNOLOGICAL UNIVERSITY

Further Reading

- Turing Machines, Automata Theory
  - http://www.doc.ic.ac.uk/~imh/teaching/Turing_machines/240.pdf
  - https://en.wikipedia.org/wiki/Turing_machine
  - http://theory.stanford.edu/~trevisan/cs154-12/turing-machines-1.pdf
    - Follow how a multi-tape Turing machine is proved to be equivalent to a Turing machine
- SANS Institute: Threat and Risk Assessment
  - https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

The End