Security and safety for the Internet-of-Things

Dimitrios Serpanos
Industrial Systems Institute/ATHENA RC, Director
University of Patras, Professor
Patras, Greece

Internet of Things (IoT)

- An information network of physical objects
  - Sensors, machines, cars, buildings, …
- Interaction and cooperation of these objects
- Towards common goals

Internet of Things systems

- Designed for one or a set of applications
  - Not just a collection of Internet-enabled devices
- Take into account the dynamics of physical systems
  - Process signals and time-series data
- Microelectromechanical (MEMS) sensors widely available
  - Low cost and low power consumption
  - Enable new applications
  - Push IoT systems towards signal processing

- Potential economic impact: $ 900B - 2.3T per year, up to 2025

Industrial Internet of Things (IIoT)

- Use of IoT technologies in manufacturing
- Builds on sensors, M2M communication and automation technology
- Smart machines accurately and consistently capturing and communicating data
- Use of big data and machine learning technologies
- Resolution of inefficiencies and problems faster, saving time and money, supporting business intelligence
- Potential for quality control, sustainable and green practices, overall supply chain efficiency

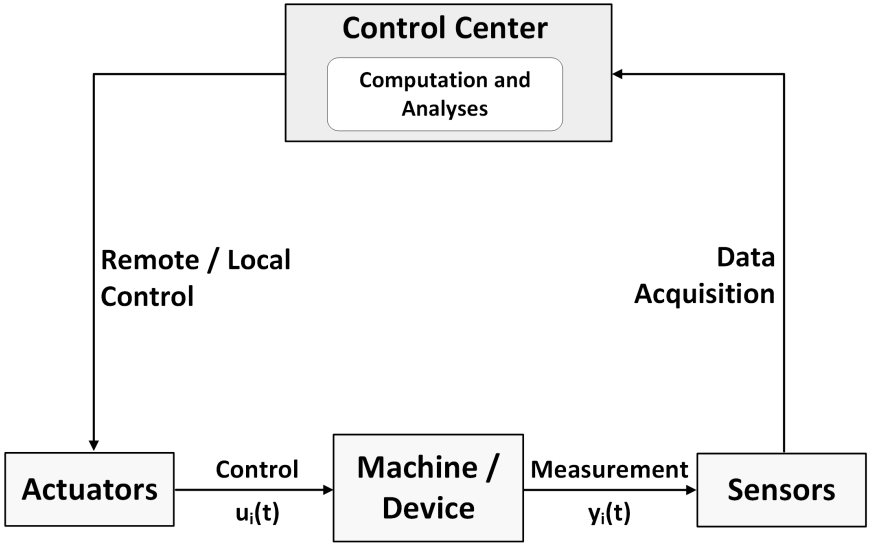
- Potential growth: IIoT market predicted to $ 123B by 2021

IIoT relevant efforts

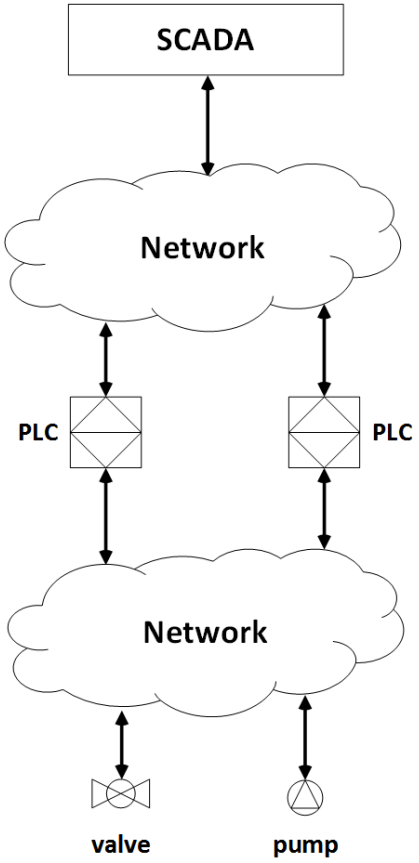
- Industrie 4.0
- Industrial Internet Consortium
- Society 5.0
- Made in China 2025

CPS/Industrial Control Systems

Control view



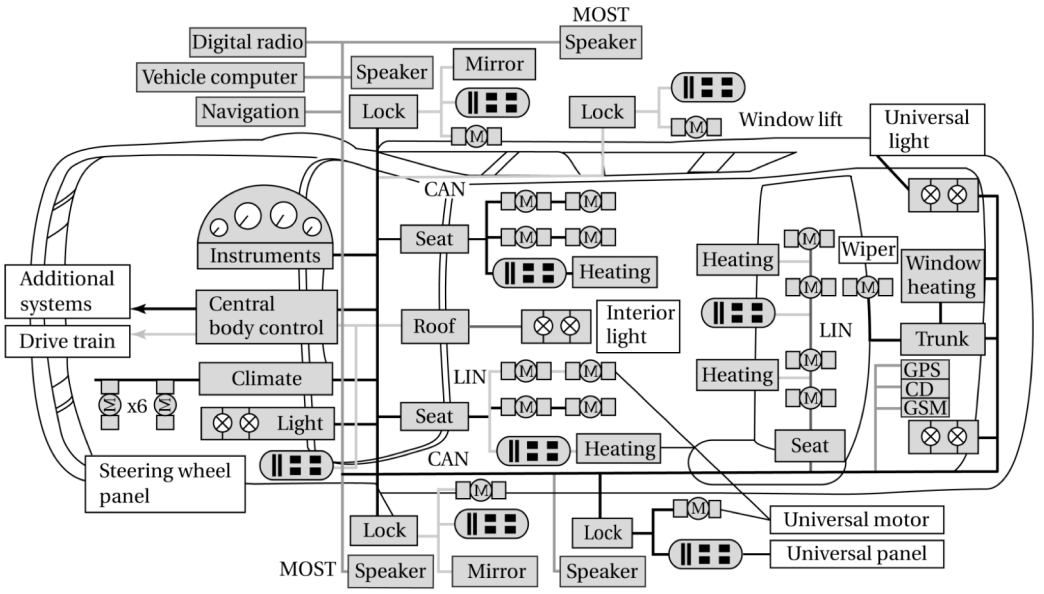
Computational view



Industrial Systems Institute

Safety and security

- Security: integrity and confidentiality of information
- Safety: physical damage/harm
- Safety and security are traditionally handled by very distinct groups of people
- These two characteristics are intertwined in cyber-physical systems
- Highly complex systems
  - Ford F150 ships with 150 million lines of code.
  - Boeing 787 ships with 7 million lines of code.



CAN Controller Area Network
GPS Global Positioning System
GSM Global System for Mobile Communications
LIN Local Interconnect Network
MOST Media-Oriented Systems Transport

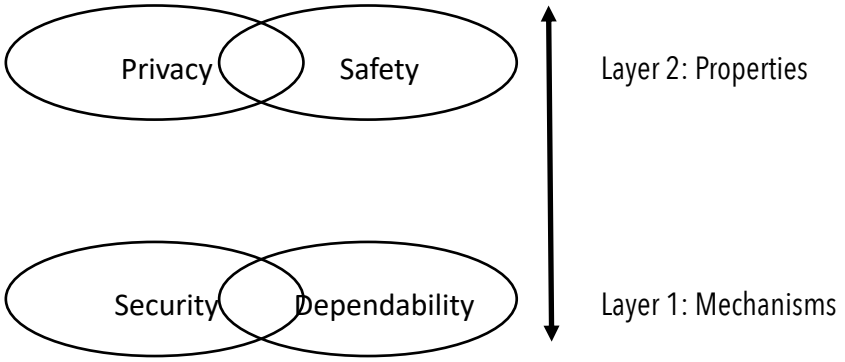
Safety and security requirements

- Safety properties
  - Maintain well-defined state that corresponds to safe operation
- Safety typically expressed as requirements on control loop
- Security is related to safety:
  - Data integrity

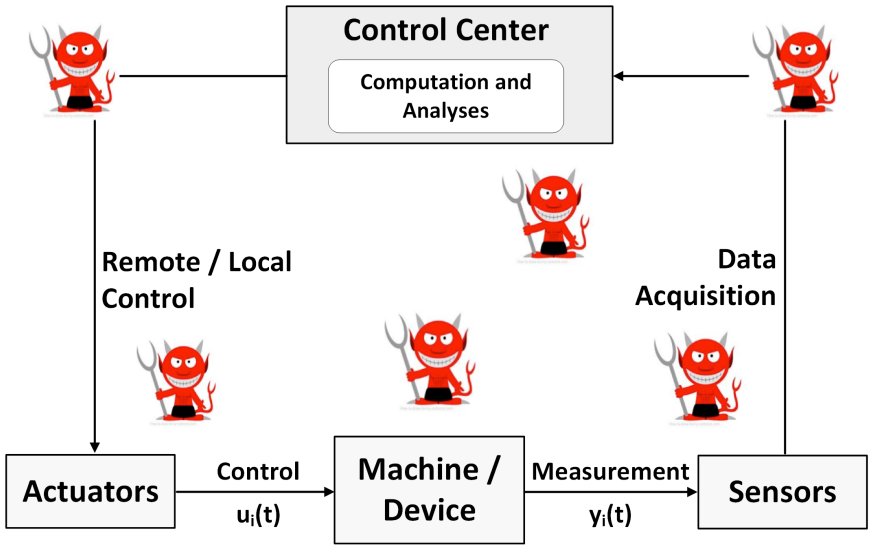
- Security
  - Confidentiality
  - Integrity
  - Authentication
  - Access control
  - Non-repudiation
  - Dependability
  - Safety
  - Privacy

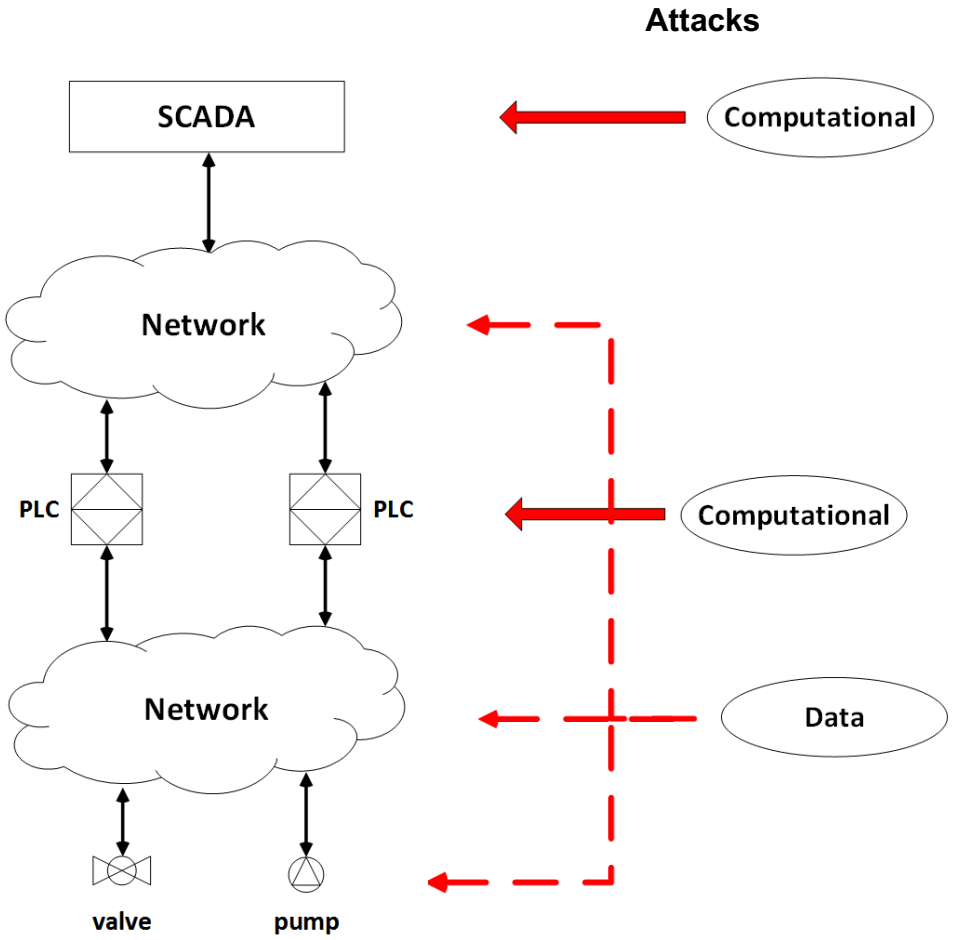
Security property layers

- Security and dependability are mechanisms
- Privacy and safety are system properties
  - Requirements for processes, applications, services
- Privacy and safety depend on security
- Threats:
  - Computational
  - Data



CPS/Industrial Control Systems





Incidents..

- Attacks:
  - Stuxnet (2005-2010)
  - Ukraine power grid (2016)
  - In-flight hack into UA 737 (2015)

- Design flaws:
  - Crash of Airbus A400M due to fuel system software bug (2015)
  - VW Dieselgate (2015)
  - Heartbleed (2014)

Challenges

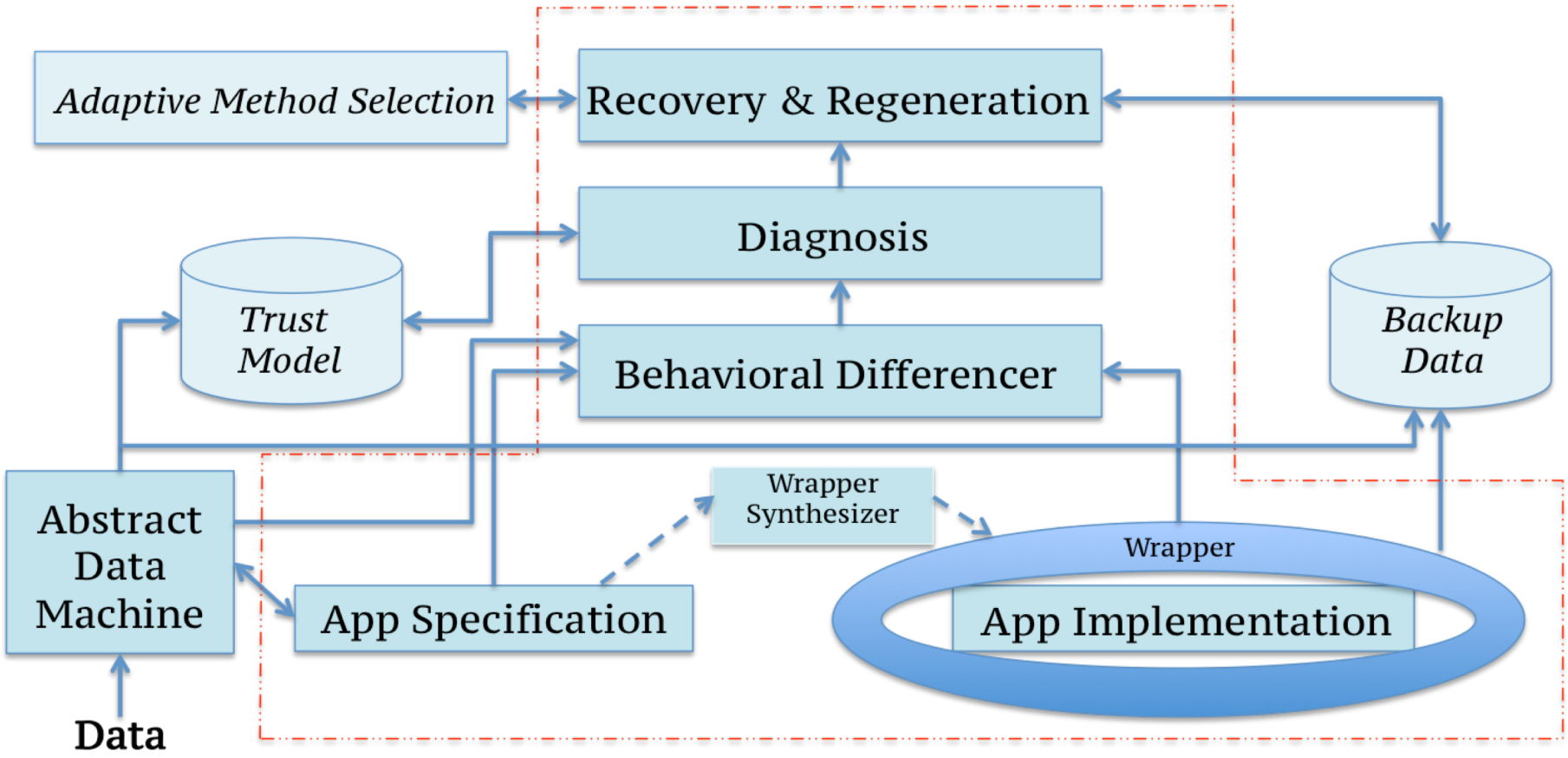
- Attacks:
  - Timing, QoS
  - Designed-in Trojan horses
- Design flaws:
  - Inadvertent or deliberate
  - Numerical, non-linear systems, state, *etc*.
  - Black box components are hard to verify
- Updates:
  - Running systems can't be updated
  - Updates may fix some problems, introduce others
  - Long-lived systems require component replacement, upgrade
- Some challenges due to complexity, others due to Internet connectivity

Strategy and approach

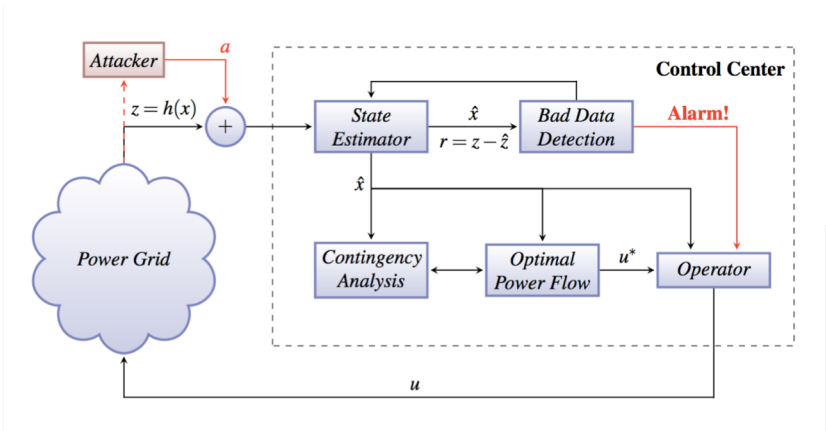
- **Build it right and continuously monitor**
  - *US Federal Government Strategy*

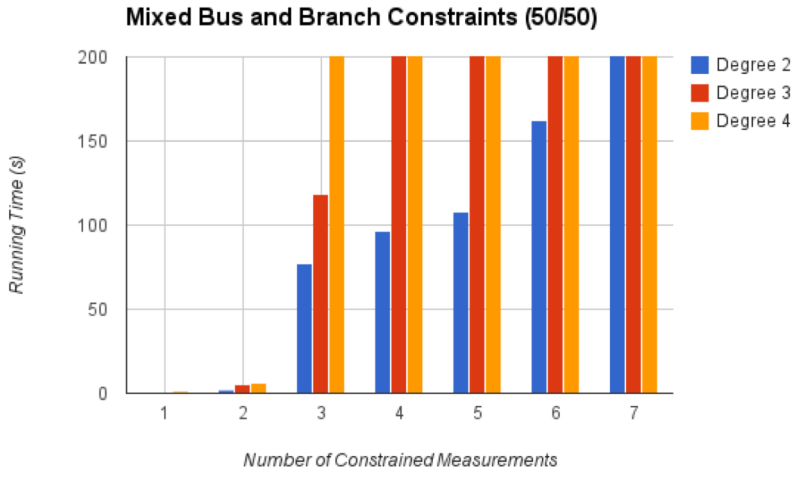
- ARMET approach
  - Programmable (executable) specification with security properties
    - Secure by design
  - Middleware monitoring process (app) execution
    - ARMET compares app and specification execution
  - Specification includes defense against identified process vulnerabilities
    - Novel vulnerability analysis against false data injection attacks

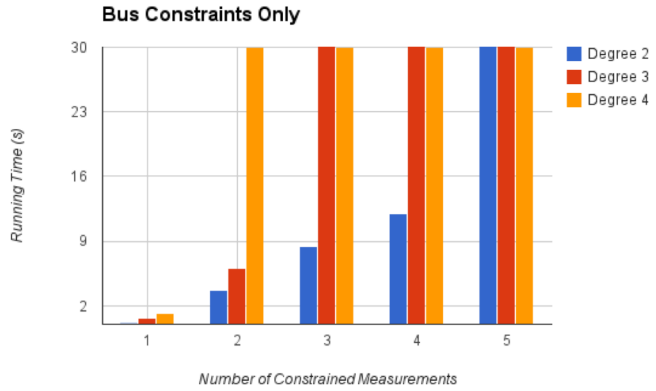
ARMET Architecture



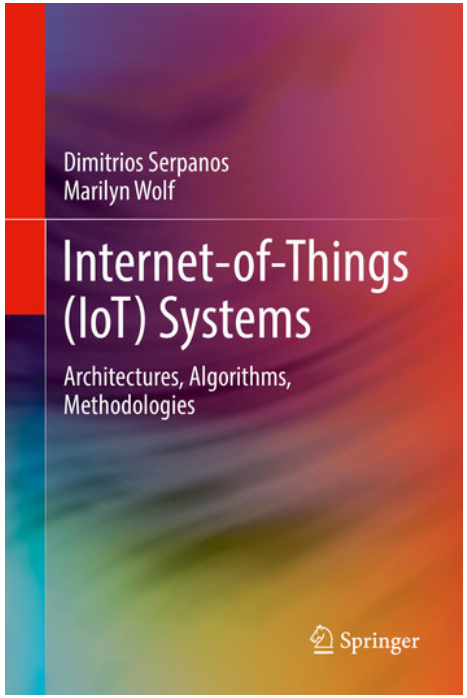
False Data Injection

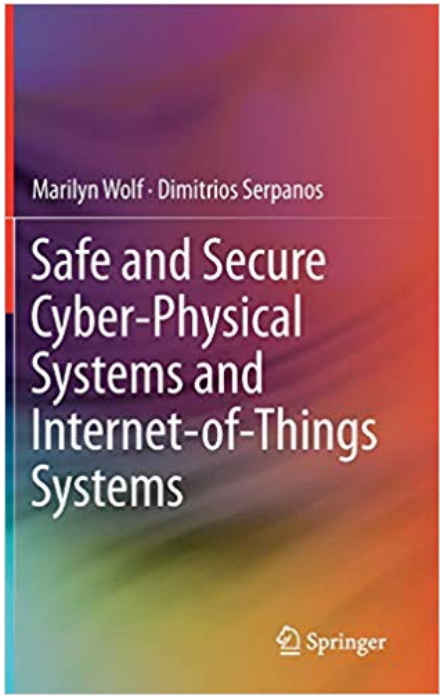






Books


Dimitrios Serpanos
Marilyn Wolf
Internet-of-Things (IoT) Systems
Architectures, Algorithms, Methodologies
Springer


Marilyn Wolf · Dimitrios Serpanos
Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems
Springer

Thank you!