JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

Next-Generation
Digital Infrastructure
Research Area

Dependability in practice: How to do it?

Razvan Beuran

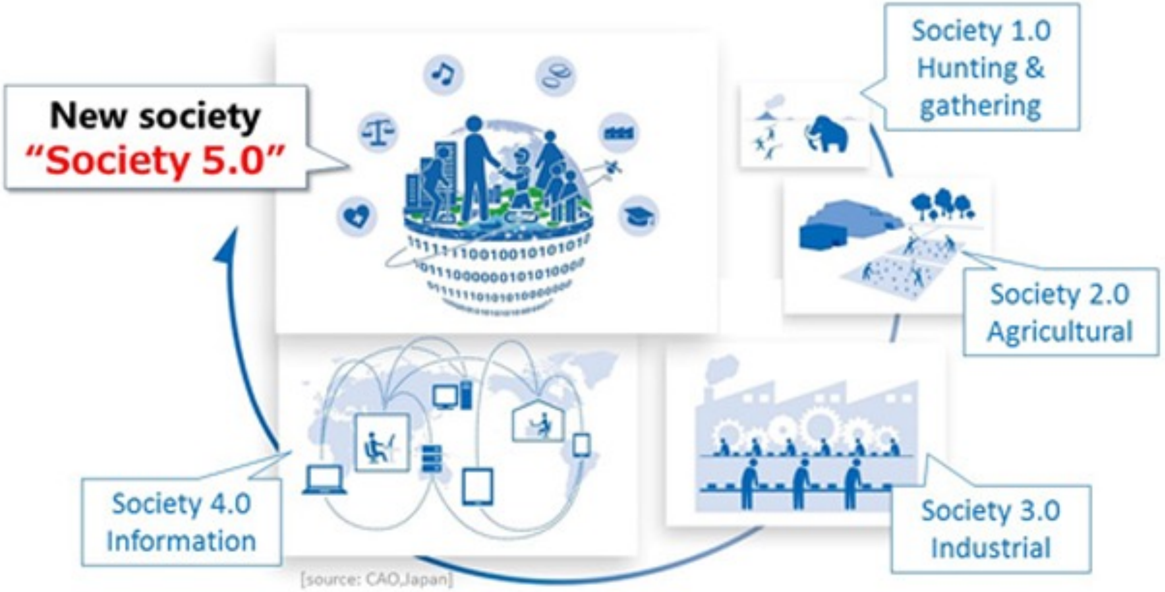
Dependability

- Theory
  - Well established (I guess, since my background is network security)
- Practice
  - Maybe not so clear?!
- Use case
  - Society 5.0 and smart buildings from the perspective of trustworthiness assurance

Society 5.0

- Vision put forward by the Japanese government

  “A human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspace and physical space.”



Source : https://www8.cao.go.jp/cstp/english/society5_0/index.html

Smart buildings

- Part of the **Smart City** vision, they are intelligent buildings that use a multitude of sensors and a central management system (Building OS) to make possible
  - Predictive maintenance
  - Operation efficiency
  - Comfort
  - High security
- Examples
  - Smart factories and warehouses
  - Smart offices and commercial buildings
  - Smart hospitals, etc.

Trustworthiness

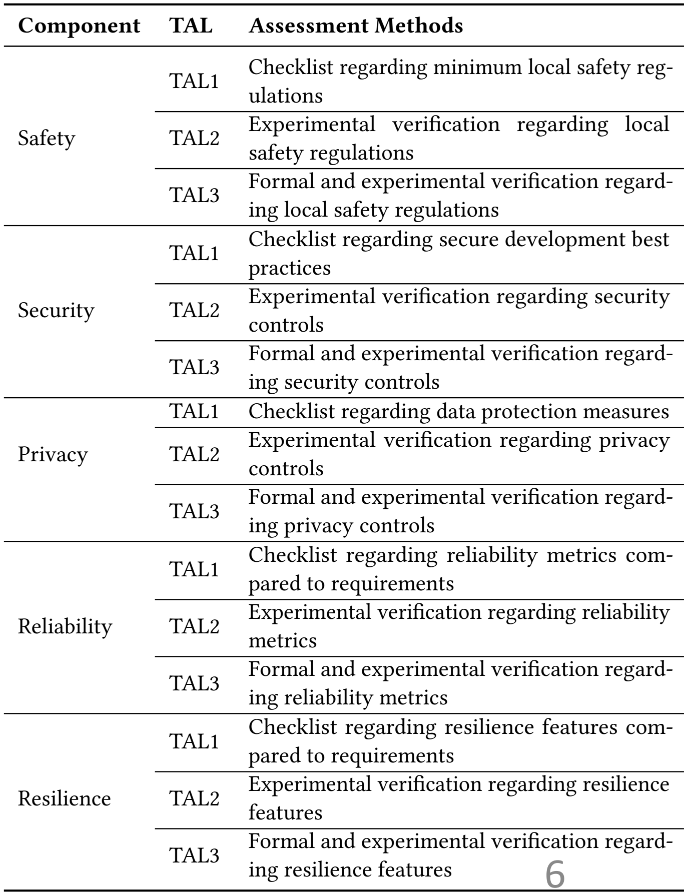
- **Definition**

  Degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks.

  ”The Industrial Internet of Things Vocabulary,” Industrial Internet Consortium (IIC), 2020

Trustworthiness Assurance

- Defined IoT trustworthiness assurance framework
  - Considered the five trustworthiness components
  - Used three assurance levels (TALs) to differentiate requirements and assessment methods
  - Current focus on smart buildings



Component	TAL	Assessment Methods
Safety	TAL1	Checklist regarding minimum local safety regulations
	TAL2	Experimental verification regarding local safety regulations
	TAL3	Formal and experimental verification regarding local safety regulations
Security	TAL1	Checklist regarding secure development best practices
	TAL2	Experimental verification regarding security controls
	TAL3	Formal and experimental verification regarding security controls
Privacy	TAL1	Checklist regarding data protection measures
	TAL2	Experimental verification regarding privacy controls
	TAL3	Formal and experimental verification regarding privacy controls
Reliability	TAL1	Checklist regarding reliability metrics compared to requirements
	TAL2	Experimental verification regarding reliability metrics
	TAL3	Formal and experimental verification regarding reliability metrics
Resilience	TAL1	Checklist regarding resilience features compared to requirements
	TAL2	Experimental verification regarding resilience features
	TAL3	Formal and experimental verification regarding resilience features

Reference: R. Beuran, S. E. Ooi, A. O. Barbir, Y. Tan, “IoT System Trustworthiness Assurance”, poster paper, 17th ACM Asia Conf. on Computer and Comm. Security (AsiaCCS 2022), Nagasaki, Japan, May 30-June 2, 2022, pp. 1222-1224.

My question to you

- While we are aware that dependability is hard to do for complex systems of systems, this is the particular type of scenario where it is most needed

How to address dependability/trustworthiness assurance for complex systems in practice?

- Maybe the future of dependable computing and fault tolerance is about its practical applications?!

Summary

- The theoretical aspects of dependability may have been well established, but perhaps the practical aspects are not so well defined
- Applicability to practical situations needs to be addressed (e.g., systems of systems)
- We have started working on a trustworthiness assurance framework to define the requirements in a top-down manner
- But how to achieve this in practice?!