Trustworthiness in Cyber-Physical Systems-of-Systems (SoS)

Jakob Axelsson

RISE Research Institutes of Sweden and Mälardalen University

Sweden

jakob.axelsson@mdh.se

December 13, 2019

RI.SE
Research Institutes of Sweden

MÄLARDALEN UNIVERSITY
SWEDEN

Introduction

- SoS = collaboration between independent systems.
- Uncertainties can lead to losses of value during operation.
- Approach: Use control models of SoS to deal with uncertainties and complexity.

Overview of presentation:

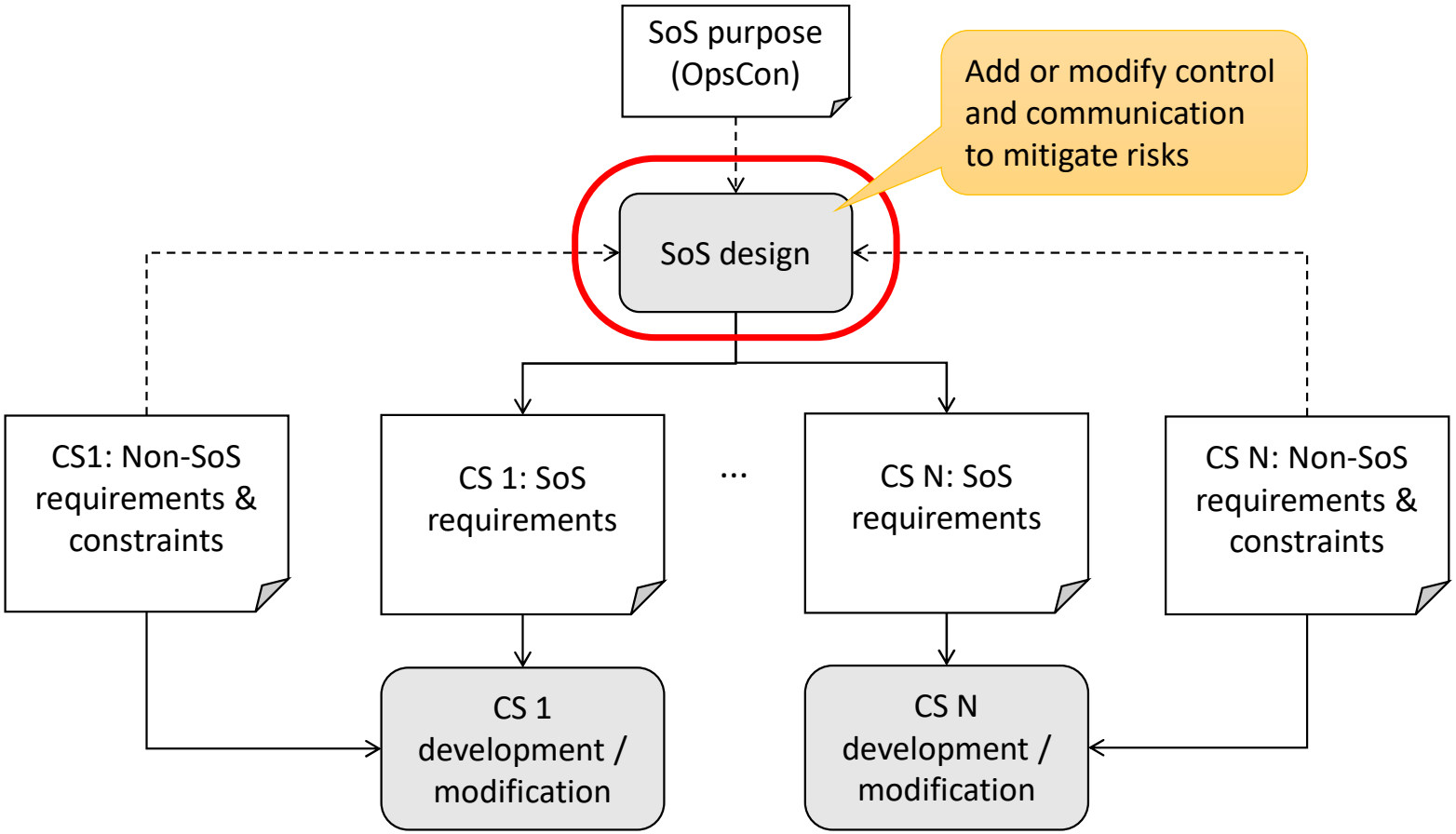
- Risk management in SoSE
- Operational risks:
  - Safety
  - Security
  - Privacy
- Managerial risk control

Motivating example: Truck platooning SoS

- Objective: Lower fuel consumption through reduced aerodynamic drag, by driving trucks closer to each other.
- Requires automatic distance control using wireless communication.
- SoS: trucks are operationally and managerially independent.

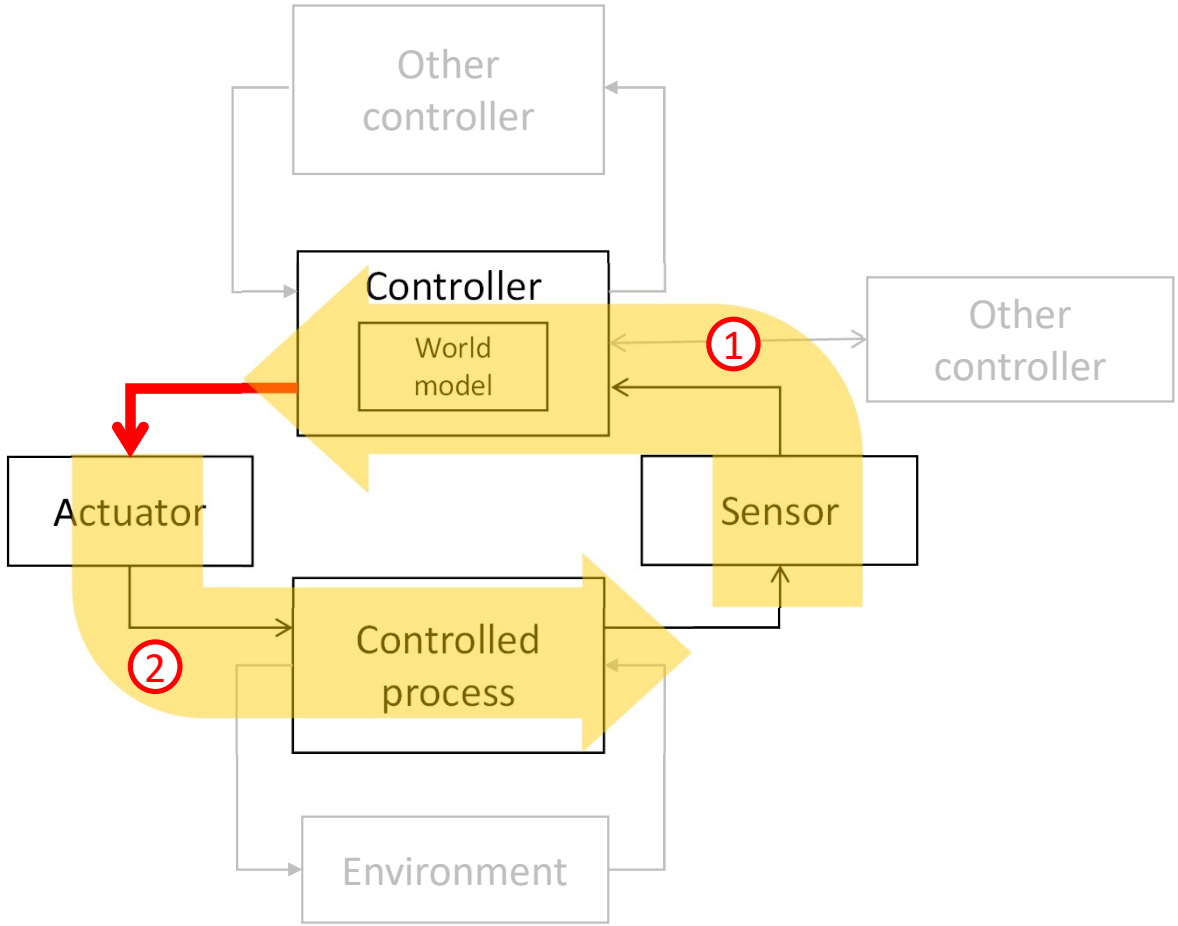
Image from ”Sweden 4 Platooning” project involving Scania, Volvo, DB Schenker, Swedish Road Administration, KTH, and RISE.

SoS engineering and risk mitigation

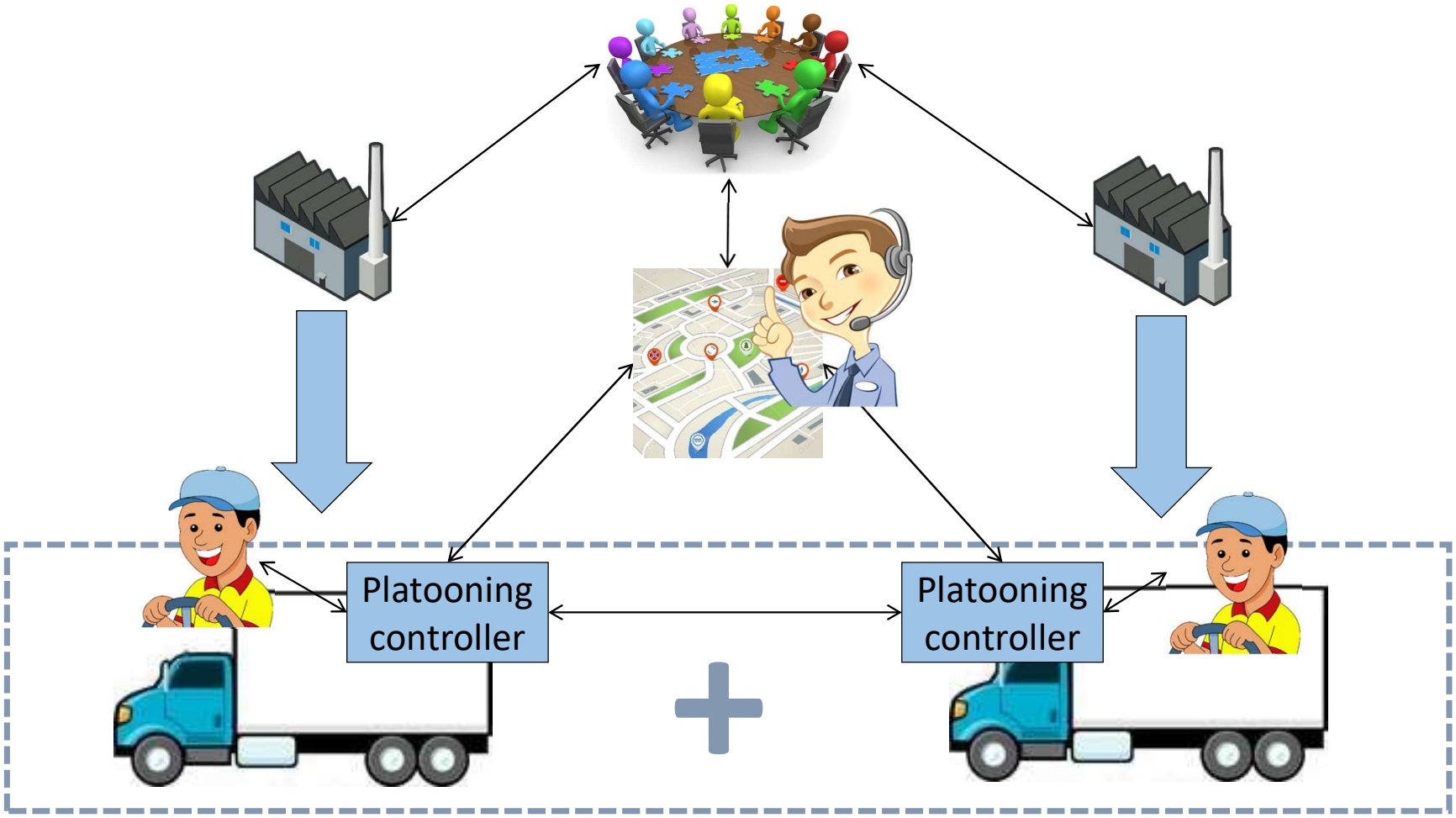


SoS risk analysis based on control models

- SoS risks can stem from hardware, software, people, organizations.
- Functional models can handle all these.
- System consists of controllers, processes (with sensors, and actuators).
- Hazards result from inadequate control:
    1. What causes a controller to perform an inadequate action?
    2. How could an adequate action not be followed?

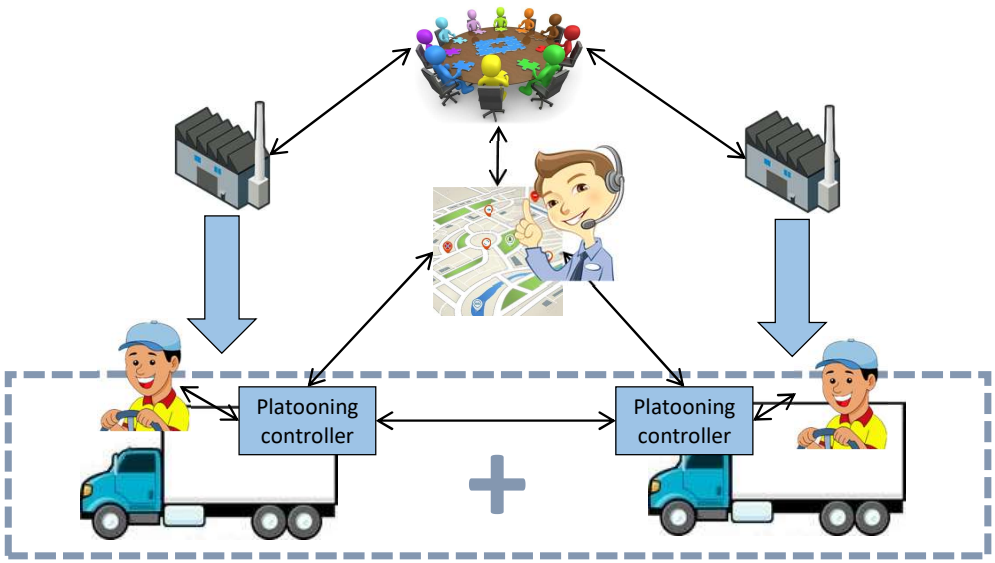


Platooning SoS control model

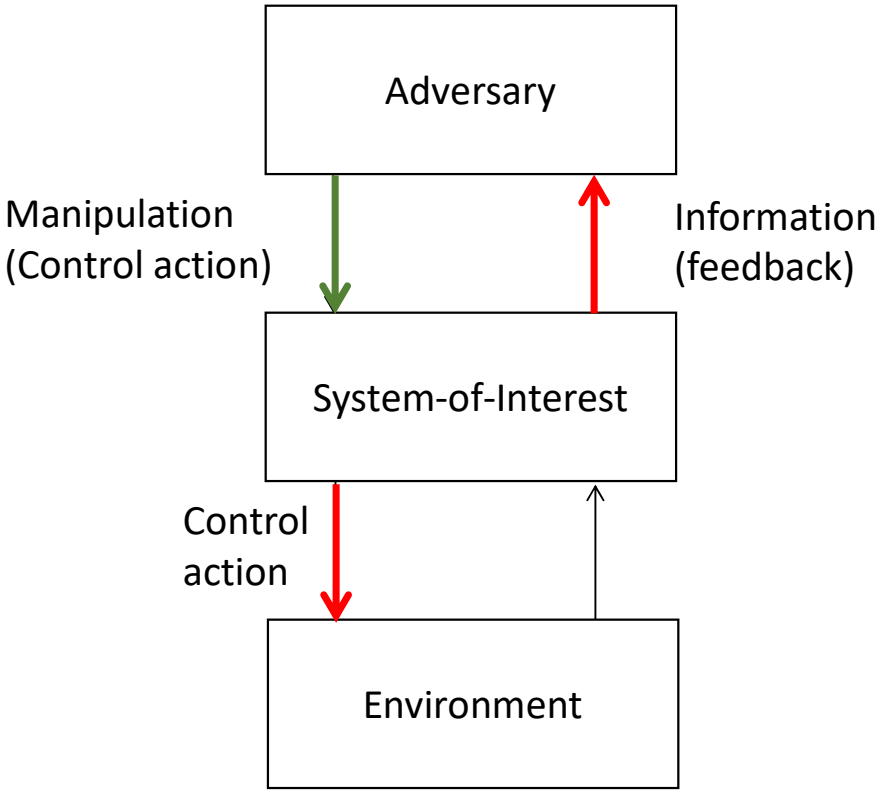


Example of safety analysis in platooning

1. **SoS loss:** ”Platoon occupant injured.”
2. **Hazard:** ”Too short separation distance between trucks.”
3. **Inadequate control action:** ”Follower vehicle accelerates when separation distance is too short...”
4. **Causal scenario:** ”... because the distance sensor did not provide a correct measurement, while the leading vehicle is braking.”
5. **CS requirement:** ”Each vehicle shall always validate its primary distance measurements against a secondary information source, and resume manual control if they are different.”

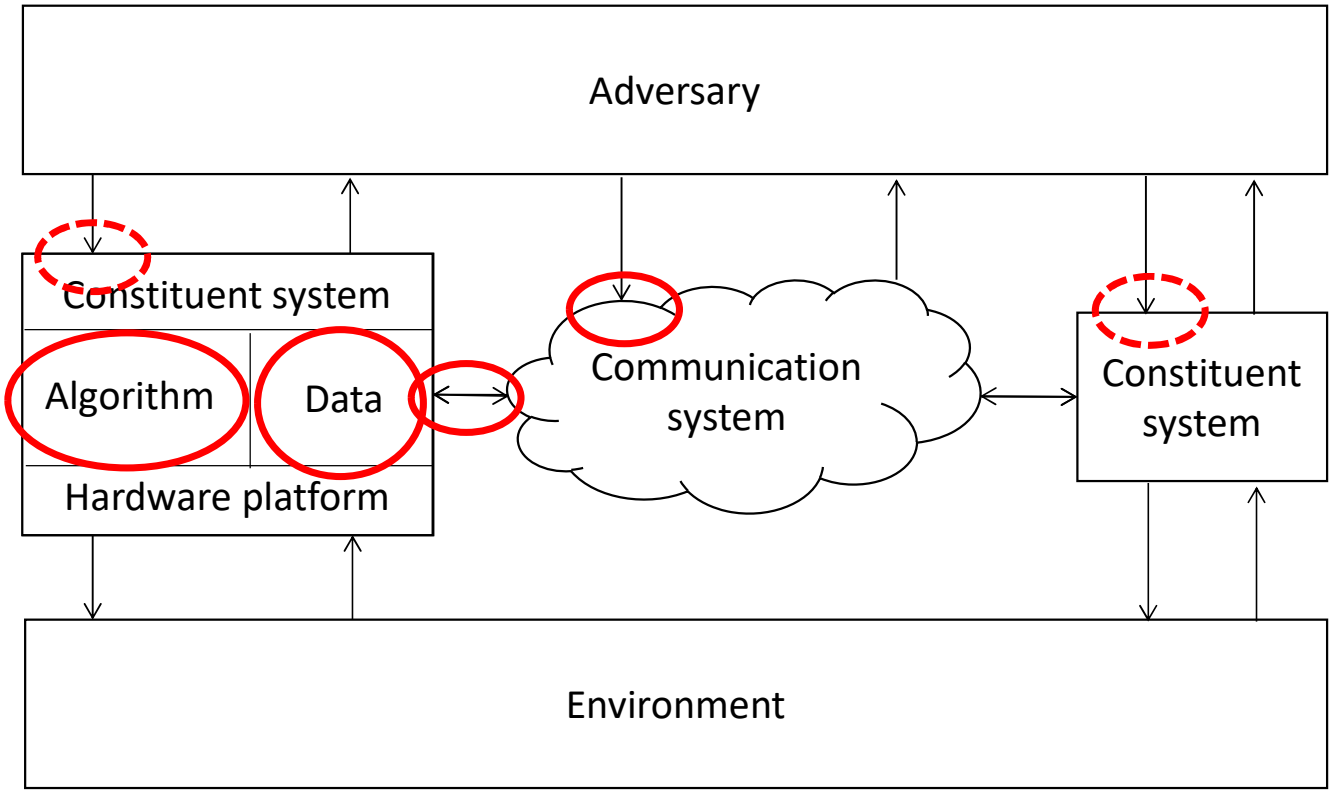


Security as a control problem

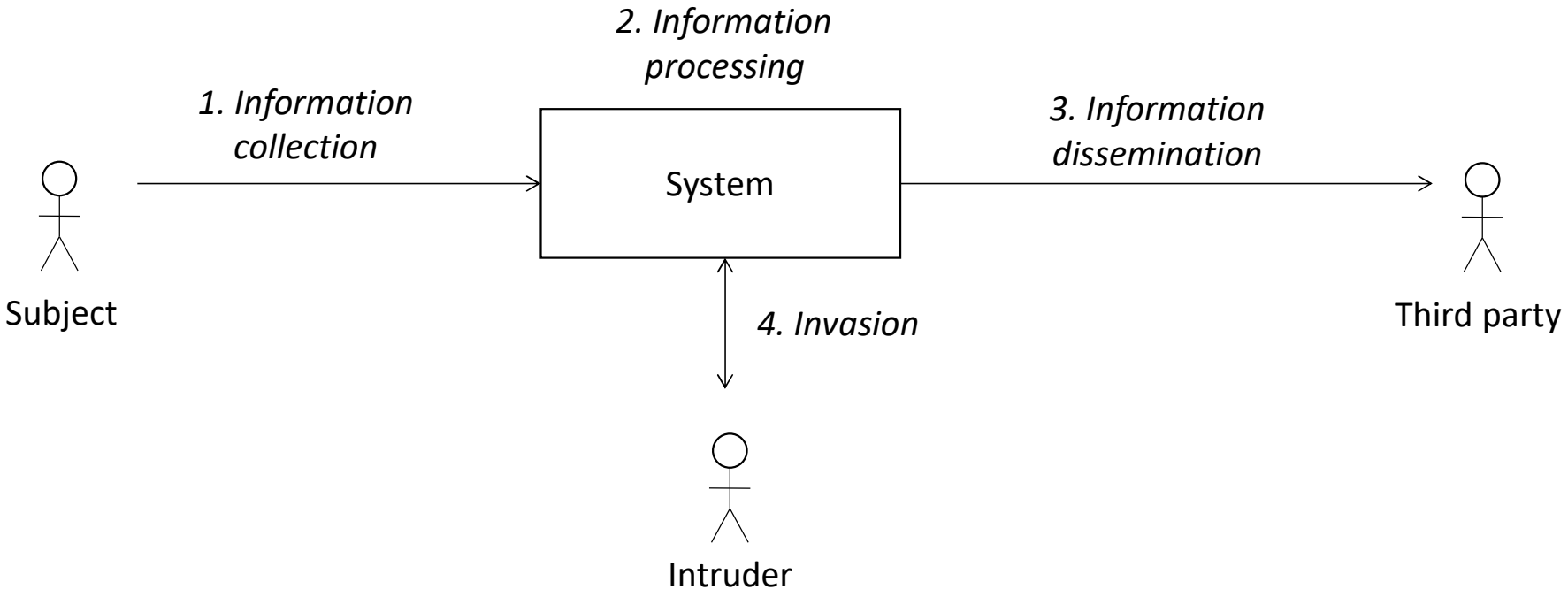


- Adversary manipulates SoI by injecting information:
  - Objective: attain some value by making the SoI change its outputs (an unintended control action).
  - Value examples: financial gain, interest of nation state, support for ideology.
- Result of manipulation:
  - Returning valuable information to the adversary; or
  - Changing how SoI influences the environment.
- If the manipulation leads to a loss for the SoI owner, defense should be put in place.
- Security losses may relate to other risk types, e.g. safety or loss of mission.

SoS attack surfaces



A taxonomy of privacy in information systems

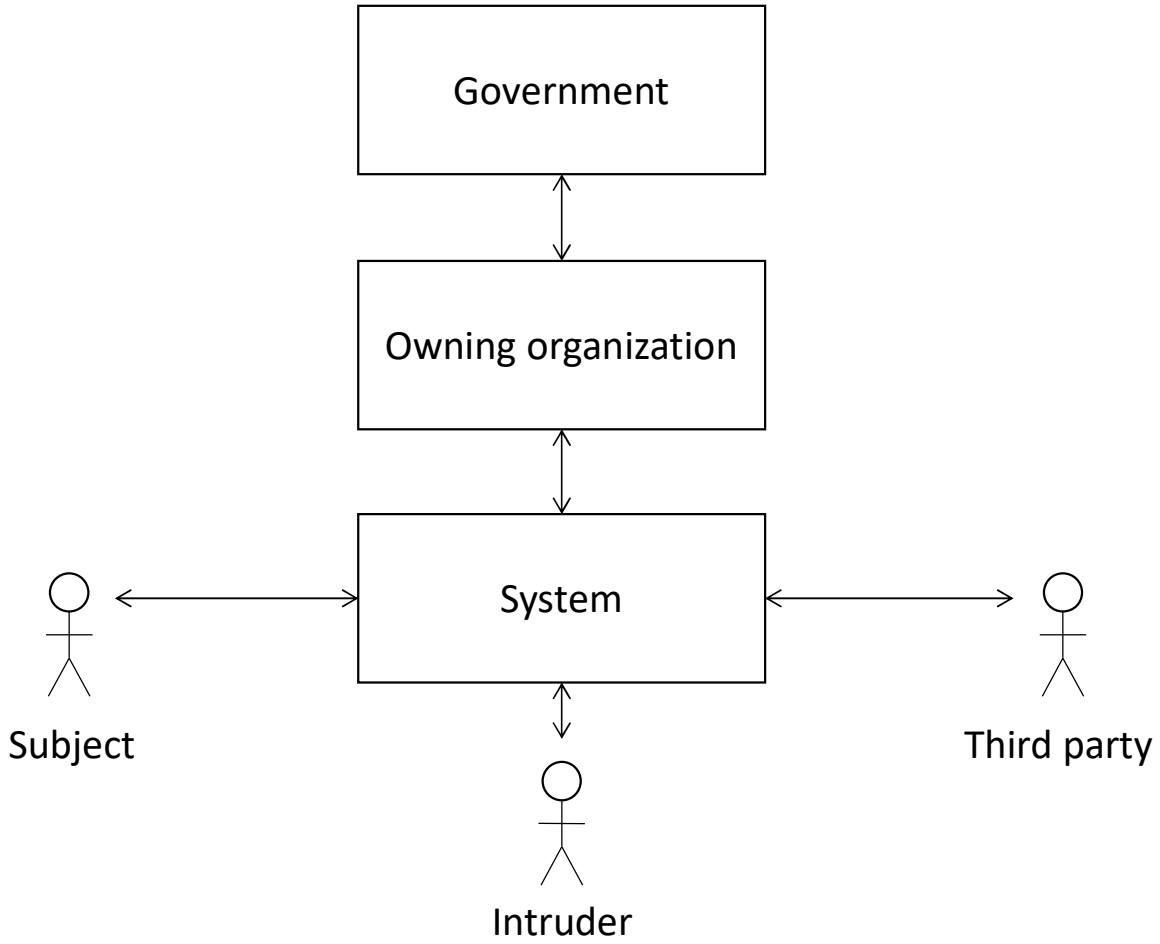


(Source: Solove, 2006)

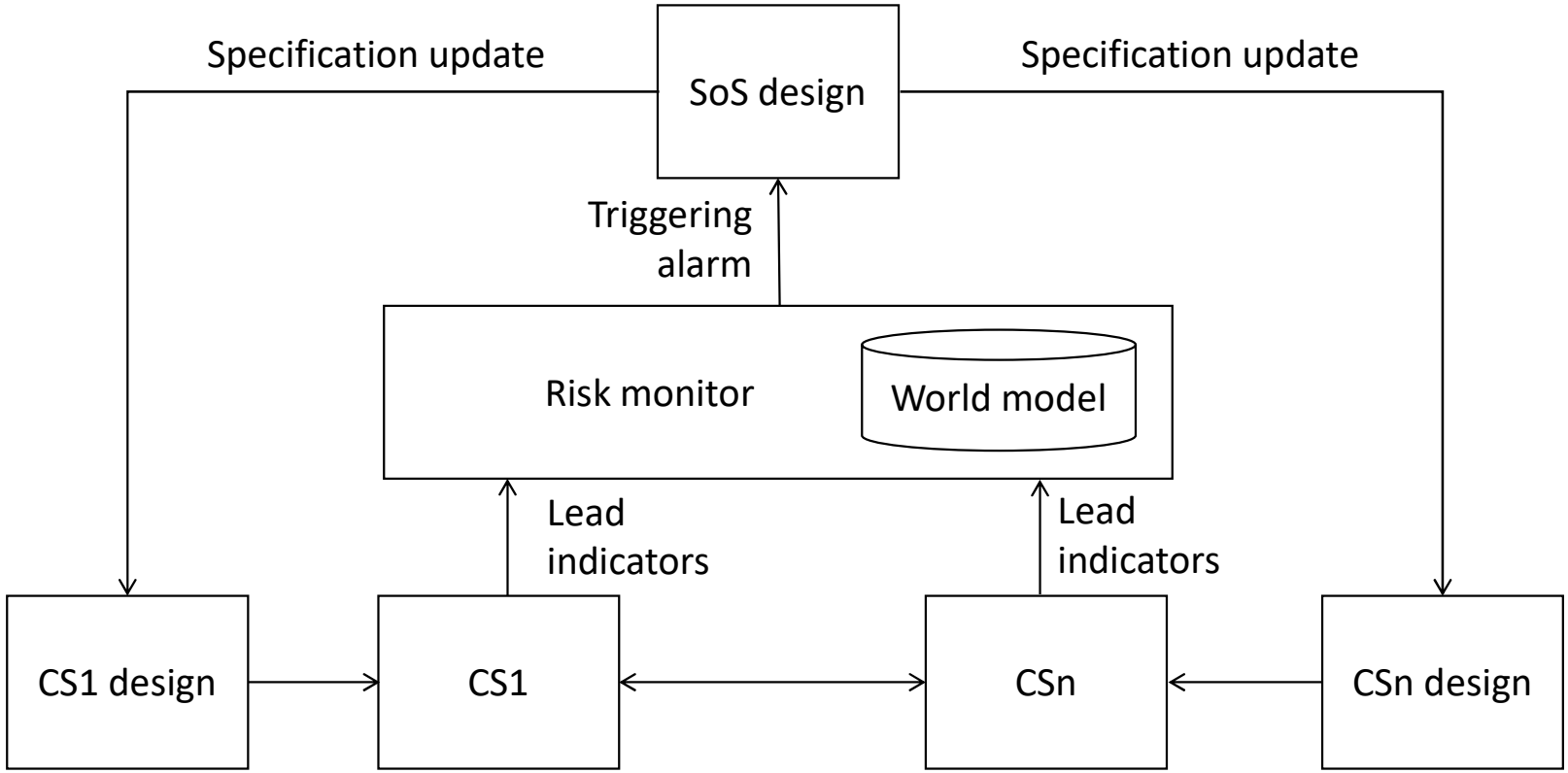
Privacy in SoS

- Aggregation (information processing):
  - Harmless data items in two different CS may become sensitive when combined in an SoS.
  - Anonymous information may become traceable.
- Disclosure (information dissemination):
  - A subject interacting with a CS would consider another CS a third party.
  - A CS may require to get consent for such data sharing.

Privacy legislation



Managerial risk control by DevOps



Summary and conclusions

- Trustworthiness is a key SoS concern, incl. safety, security, privacy.
- Analysis based on functional control models.
- Common analysis: e.g. security risks that lead to safety risks.
- Static analysis will not suffice due to complexity and evolution.
- DevOps: dynamic, managerial feedback loops.
- Important to separate responsibilities between SoS and CS levels.