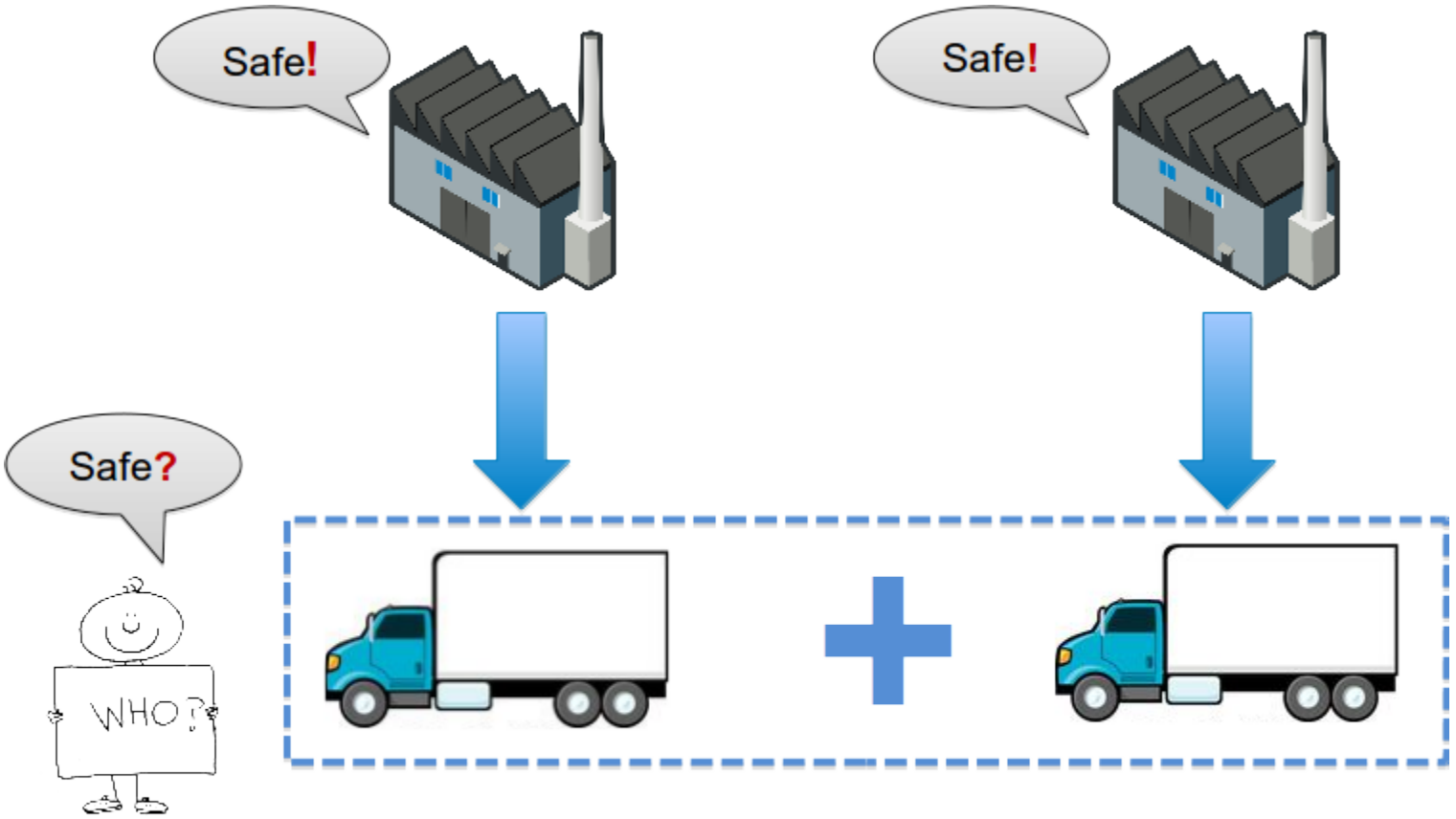
SYSTEM-BASED SAFETY ANALYSIS OF AUTOMOTIVE SoS APPLICATIONS

VOLVO

PART OF RI.SE

SWEDISH ICT

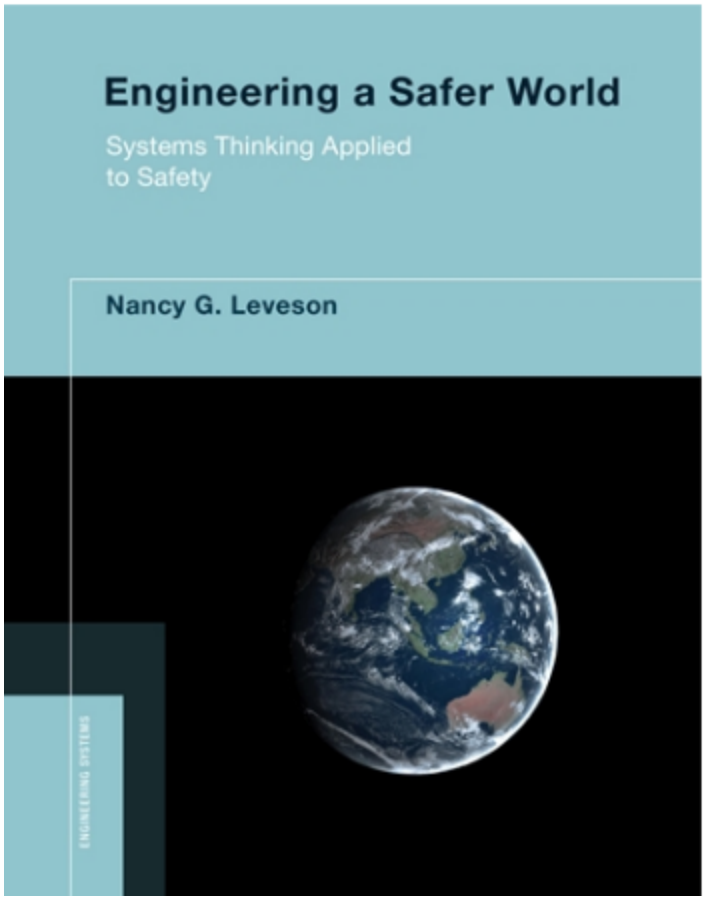
THE WHO (AND HOW)?

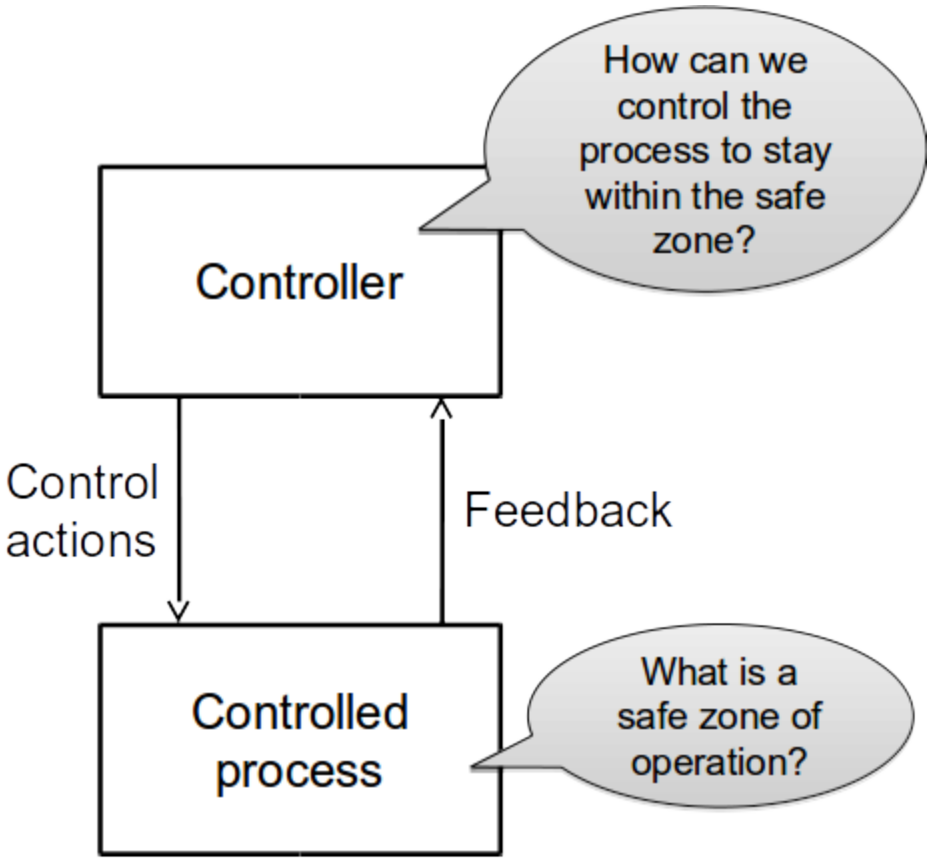


RQ: *How to conduct safety analysis of SoS, with application to C-ITS?*

SoS AND SAFETY

SYSTEMS ORIENTED SAFETY ANALYSIS – STAMP



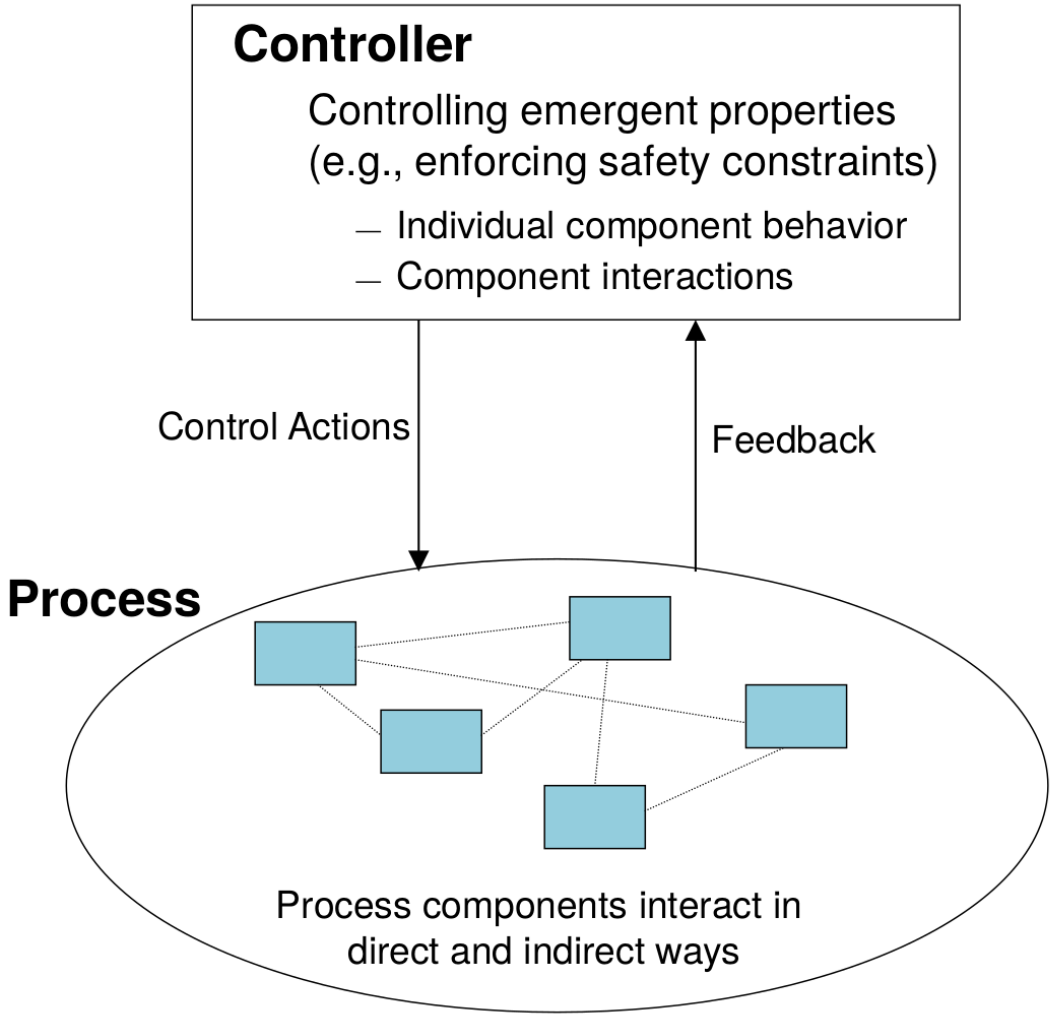


STANDARD APPROACHES DO NOT HANDLE

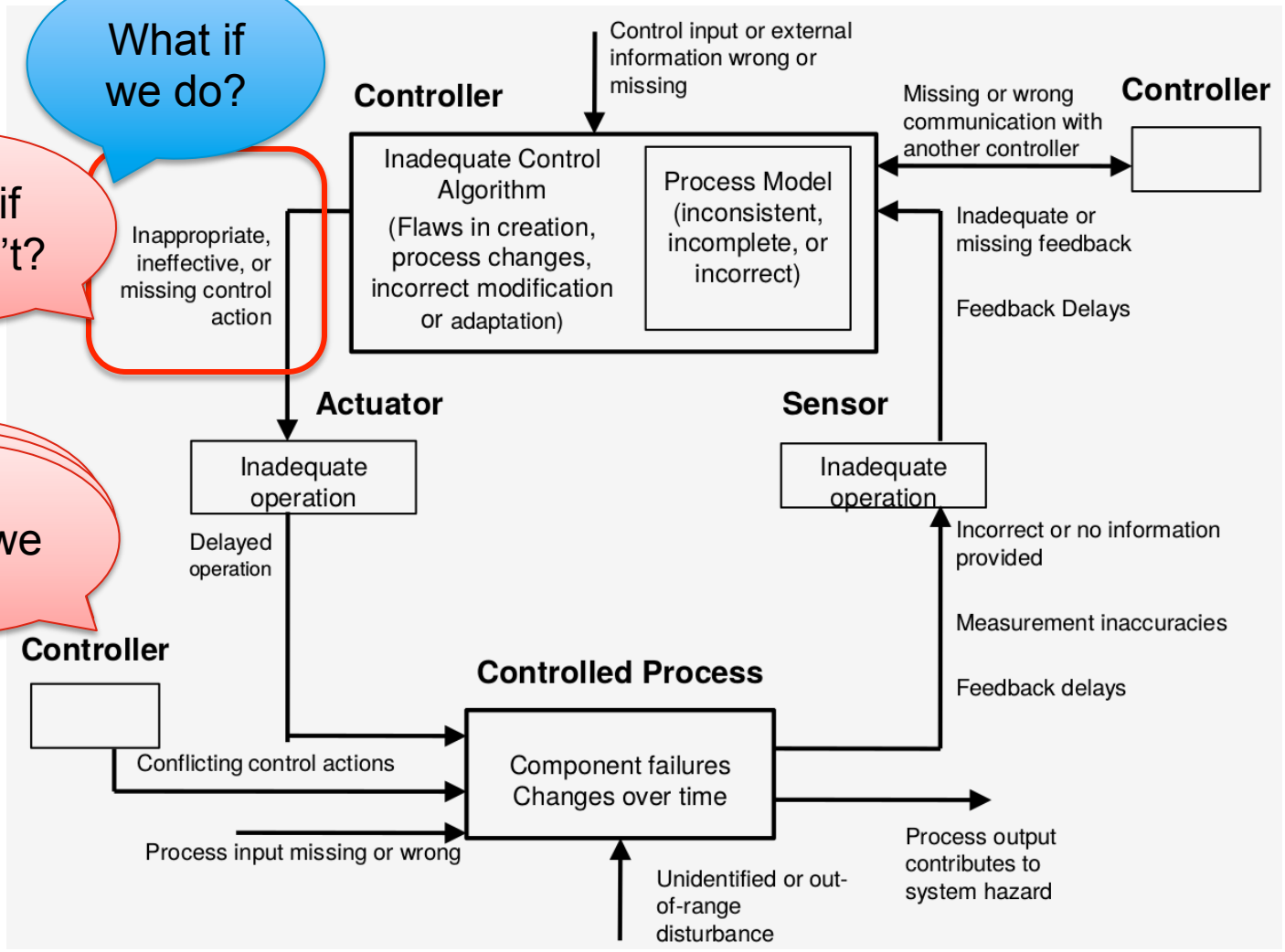
- Software and SW requirements errors
- Component interaction accidents
- Human behavior (in a non-superficial way)
- Systemic factors (affecting all components), e.g.
  - System design errors
  - Migration of systems towards greater risk
  - High complexity

SWEDISH ICT

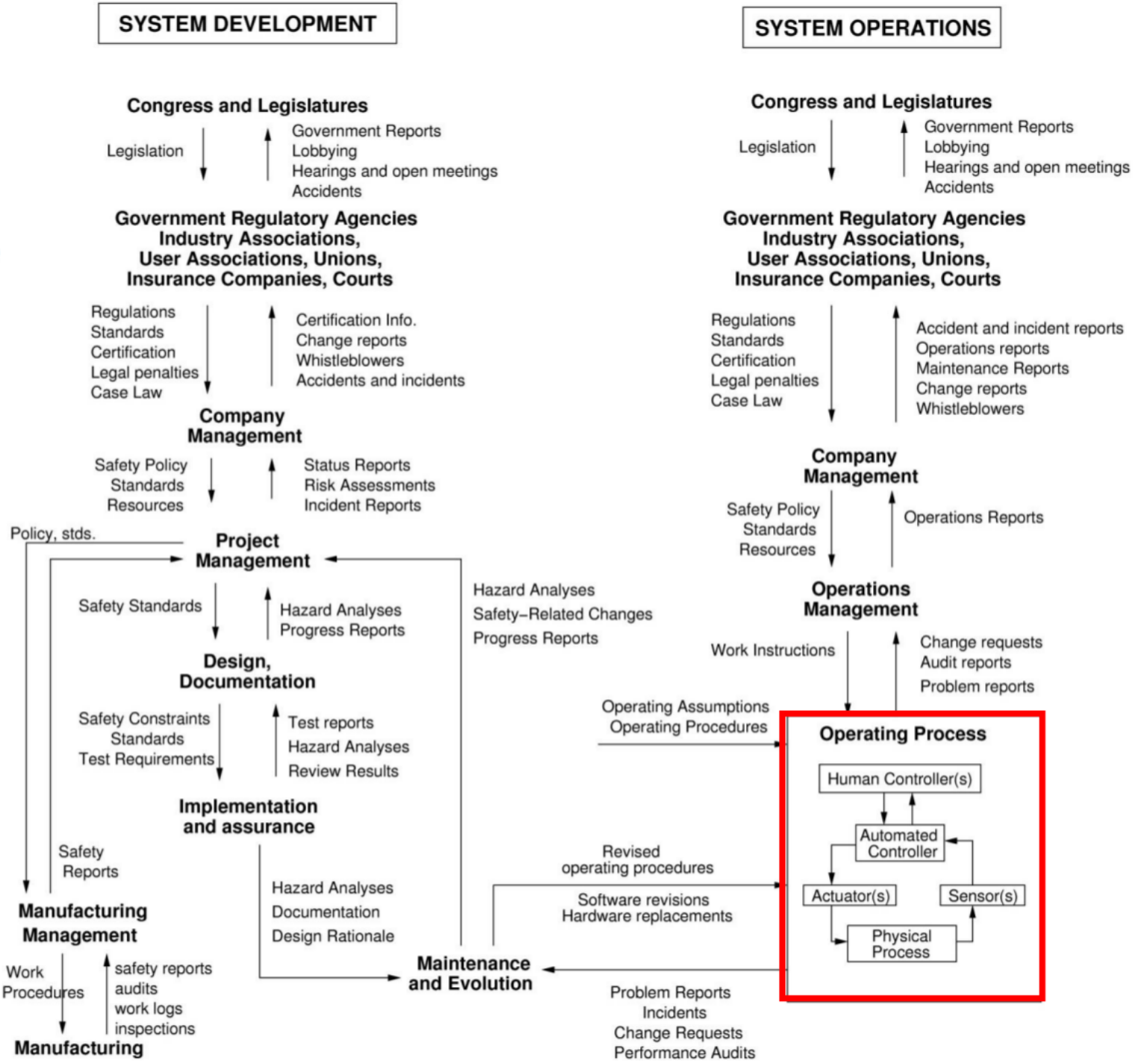
WHAT IS STAMP?



STAMP ANALYSIS



Example Safety Control Structure (SMS)



CONCLUSIONS

- A certain threshold in learning STAMP
- Lack of comparative studies
- System-based view on safety
- Growing momentum (yet some more remains to be done)
- Initial results seem encouraging
- SoS-specific challenges:
  - Allocation of safety functionality
  - Undocumented requirements
  - Risk monitoring (and update of earlier safety analysis)
  - Complexity
  - Trade-offs between different goals (SoS/S, SoS/S-safety)
  - Responsibility ownership
  - …

SWEDISH ICT

WWW.SWEDISHICT.SE

PART OF RI.SE

SWEDISH ICT