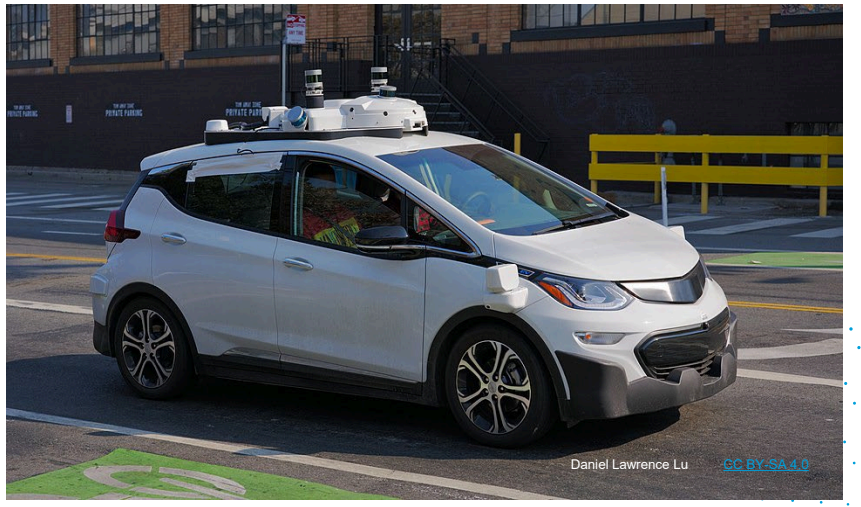


A modular risk concept

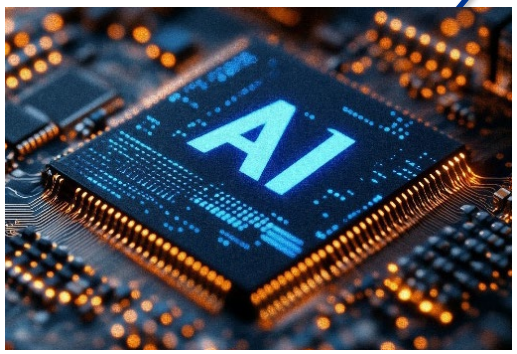
for complex systems

Dag McGeorge

29 August 2025

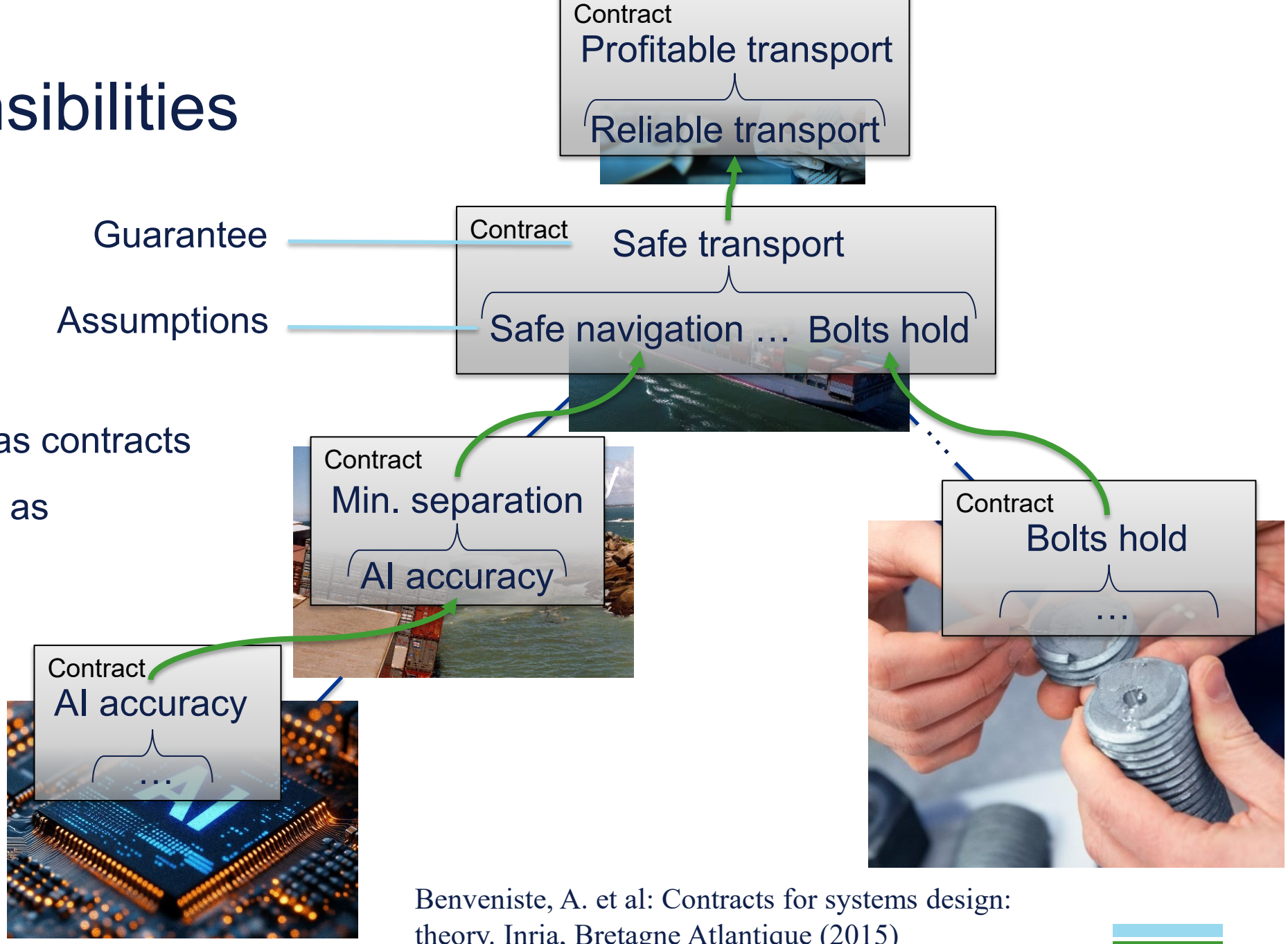
Autonomous ship example

- Different parties responsible for different system parts
- We want them to manage their risks while not messing with each other



Share responsibilities

- Allocate responsibility as contracts
- Express dependencies as refinements



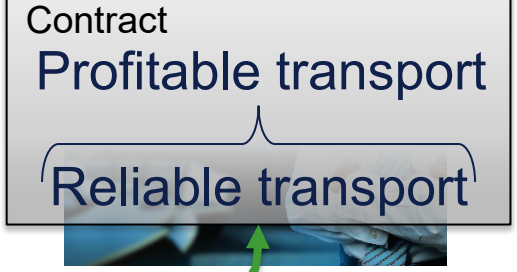
Benveniste, A. et al: Contracts for systems design: theory. Inria, Bretagne Atlantique (2015) https://hal.inria.fr/hal-01178467

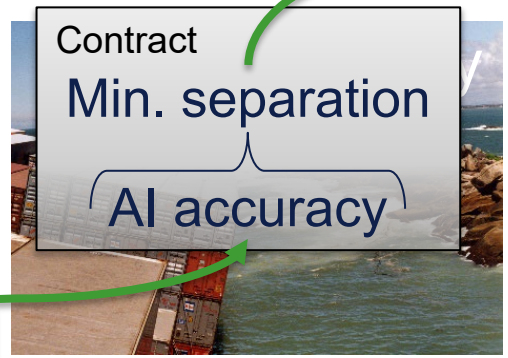
Modular risk:
CBD = risk constraints

- Risk-assess the Contracts:
  - Could a guarantee ***not*** hold even if all assumptions hold?
- Risk-assess the Refinements:
  - Could a dependency ***not*** hold?
- Risk-assess the Parts:
  - Any ***hazards*** while fulfilling a guarantee?

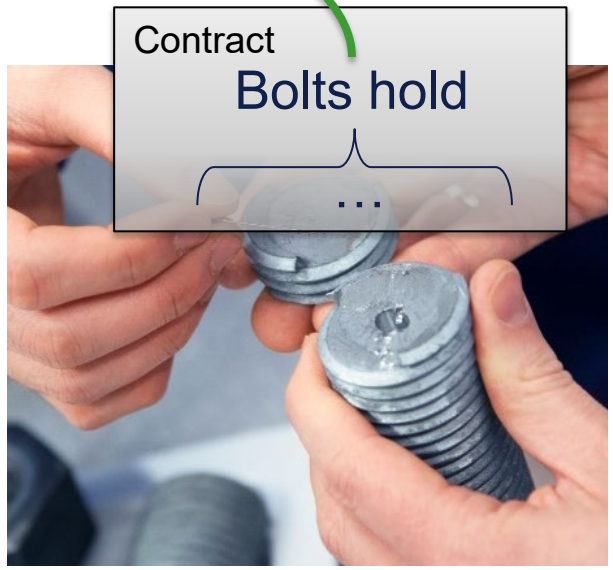
Risk constraints

Koopman, P., Widen, W.: Redefining safety for autonomous vehicles. SAFECOMP 2024:
"*The system must not only mitigate hazards, but also meet externally imposed constraints*"



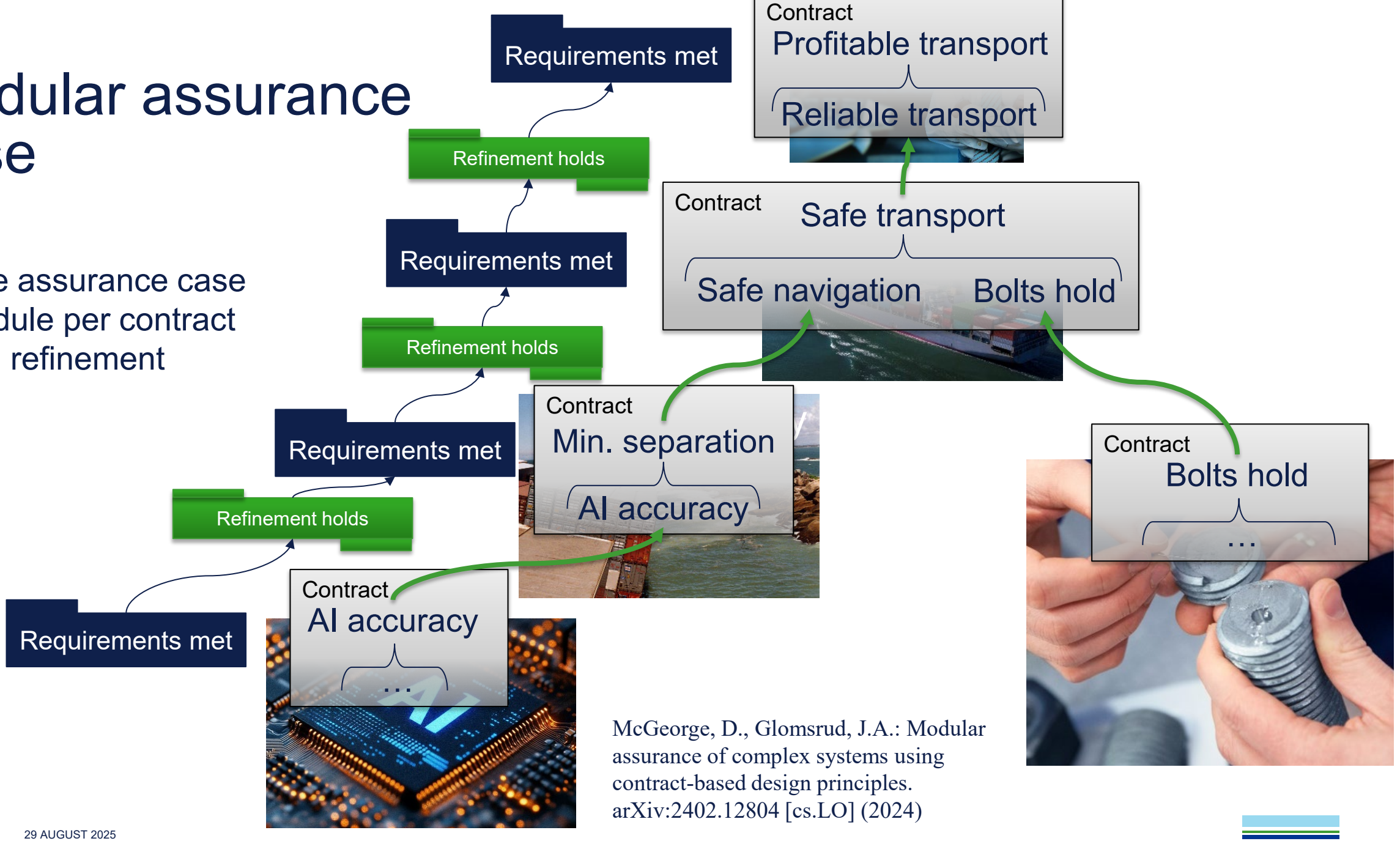



Privacy protected?



Modular assurance case

One assurance case module per contract and refinement



McGeorge, D., Glomsrud, J.A.: Modular assurance of complex systems using contract-based design principles. arXiv:2402.12804 [cs.LO] (2024)

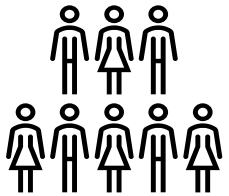
Summary

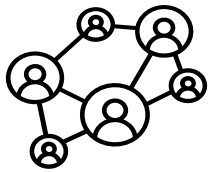
Traverse system

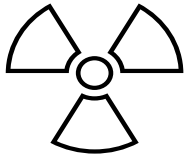
1 Stakeholder analysis

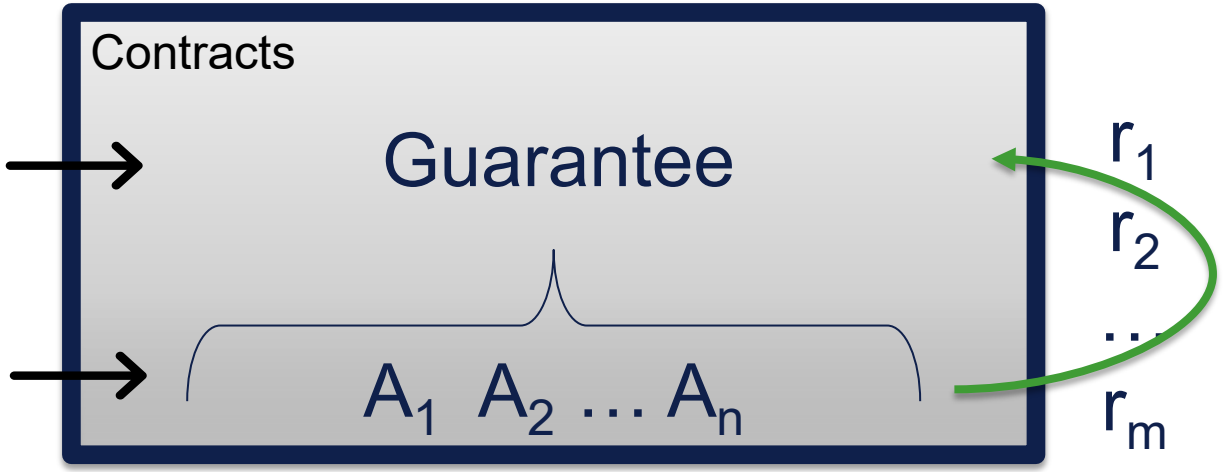
2 System dependencies

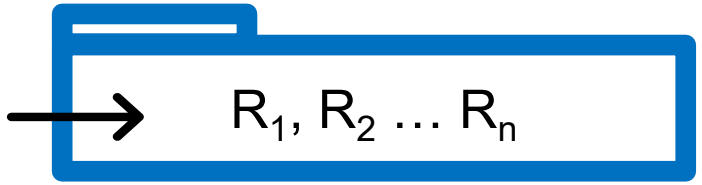
3 Risk analysis



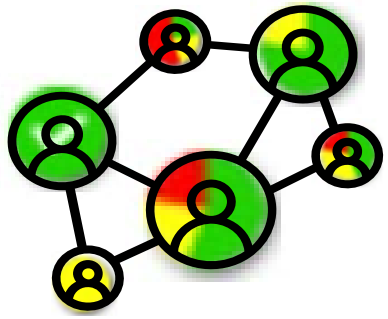








Modular assurance case



McGeorge, D., Glomsrud, J.A.: Modular assurance of complex systems using contract-based design principles. arXiv:2402.12804 [cs.LO] (2024)

Thank you for your attention!

dag.mcgeorge@dnv.com
+47 994 80 076

www.dnv.com