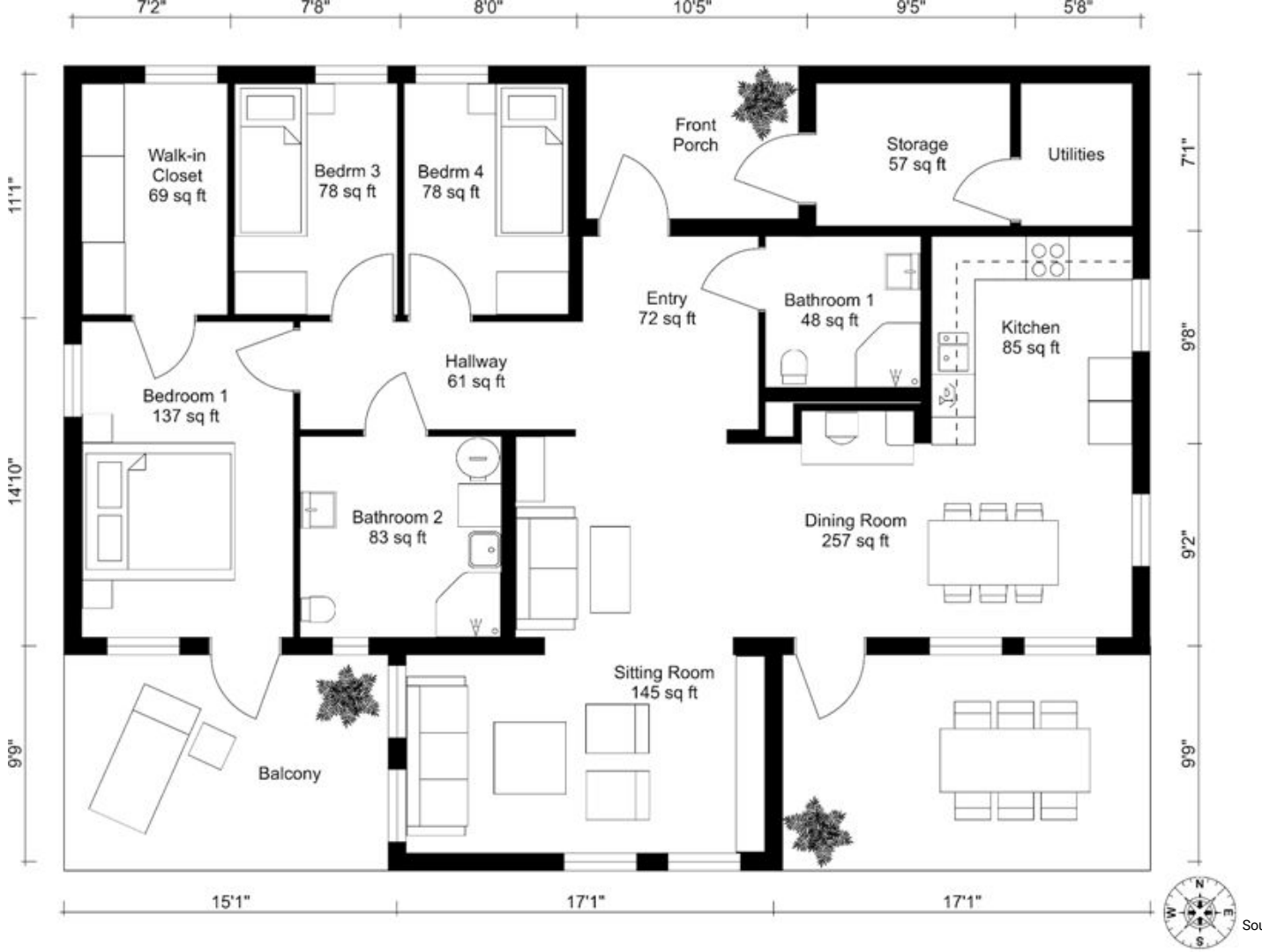
Adaptive Safety in Autonomous Ecosystems

Dávid Halász
halasz@mail.muni.cz

What are (software) ecosystems?

- An evolutionary step towards more advanced software systems
- Systems of Systems
- Higher complexity
- Higher uncertainty



Source: roomsketcher.com

Source: shutterstock.com

Autonomous Ecosystems

- Higher degree of autonomy
- Member systems can join or leave at any time
- Increased dynamicity of context changes
- Lower amount of predictable situations
- Harder to achieve safe and secure behavior
- Traditional safety mechanisms are not enough

Problems with safety

- Intentional vs unintentional behavior
- False positive and false negative situations
- Supervision awareness
- Feedback loops

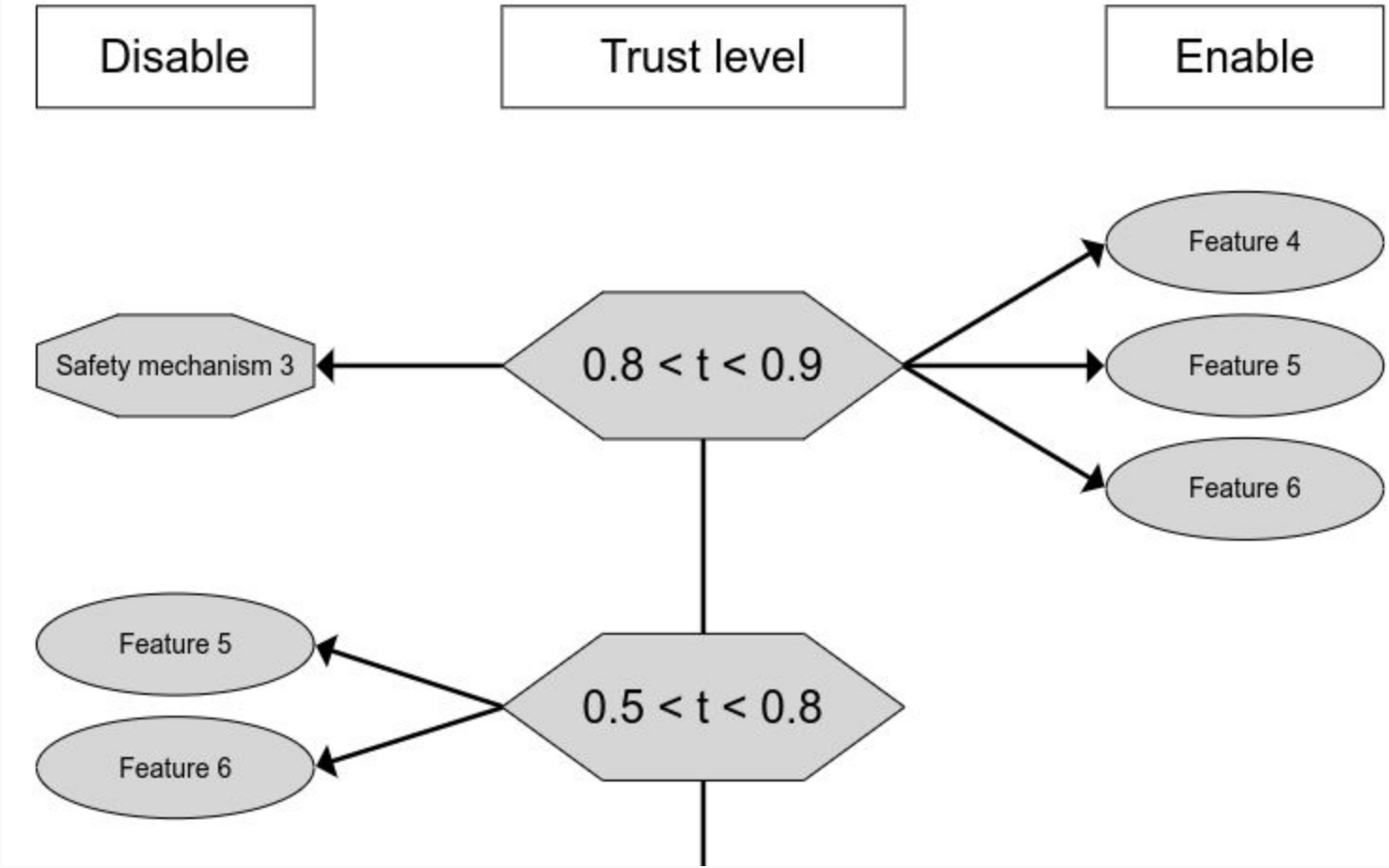
Related work

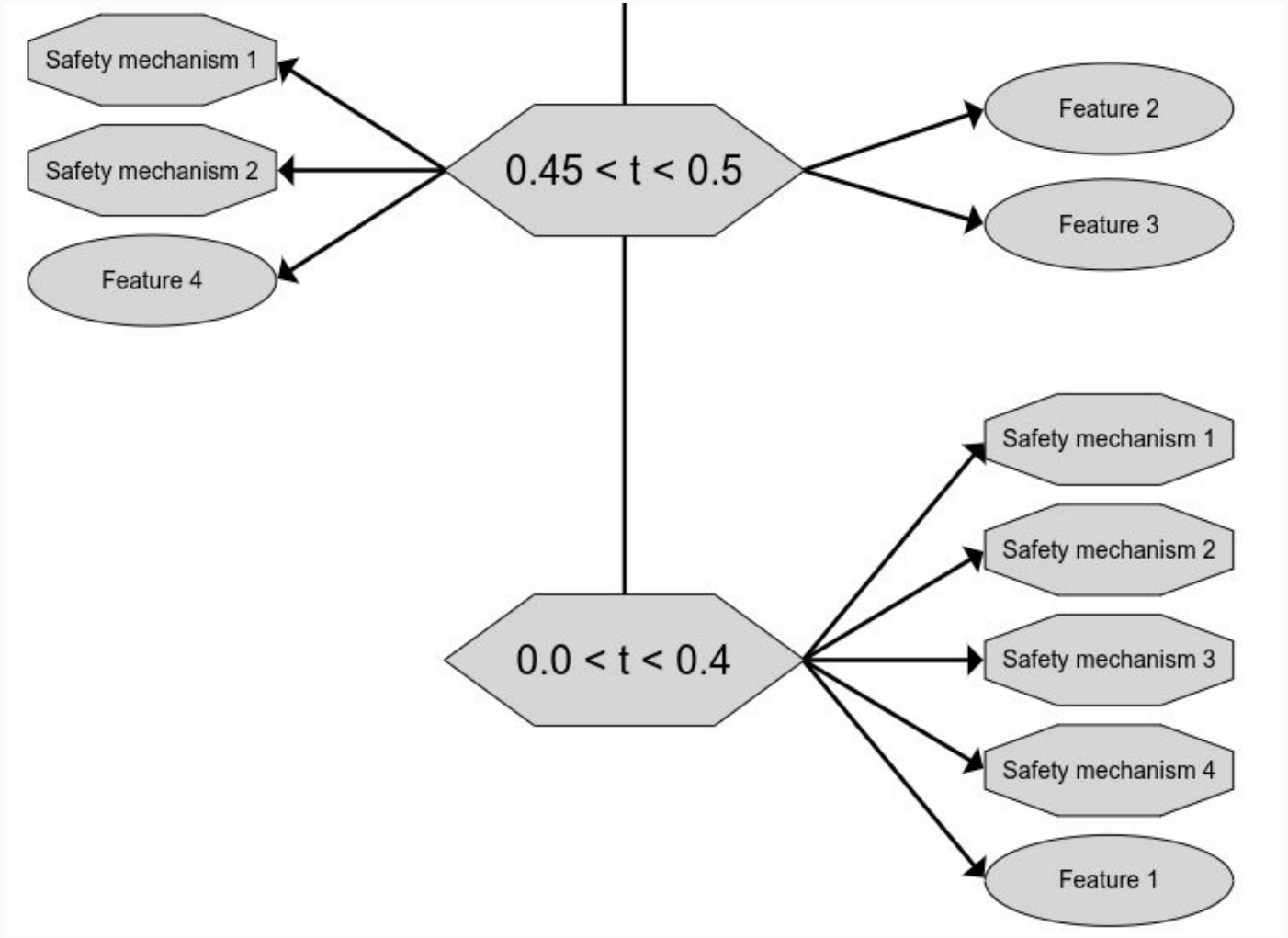
- Simplex Architecture
- Isolated Environments
- Autonomous Vehicles (Danish)
- Wireless Networks (Bacem)
- MAPE-K
- Runtime models

Proposed solution

Trust-based Adaptive Safety

- Trust quantification method
  - Trust Team is working on it
  - Overlap with Danish's research
  - Needs to have a more granular (non binary) output
- Real-time trust evaluated among member systems
  - Each against each
  - Direct and indirect trust
- Dynamic toggling of features and safety mechanisms
  - This is where it is adaptive


Disable
Trust level
Enable
Feature 4
Safety mechanism 3
0.8 < t < 0.9
Feature 5
Feature 6
Feature 5
0.5 < t < 0.8
Feature 6


Safety mechanism 1
Safety mechanism 2
Feature 4
0.45 < t < 0.5
Feature 2
Feature 3
0.0 < t < 0.4
Safety mechanism 1
Safety mechanism 2
Safety mechanism 3
Safety mechanism 4
Feature 1

Expected output

- A method for adaptive safety
- A software architecture
- Validation using simulations
- Reaching out to automotive companies
- Focus is on AVs, but can be generalized

Thank you for your attention!

Dávid Halász
halasz@mail.muni.cz