

Trusted AI at TU Graz

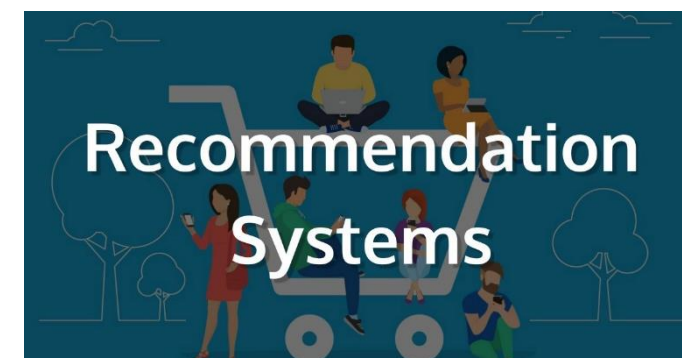
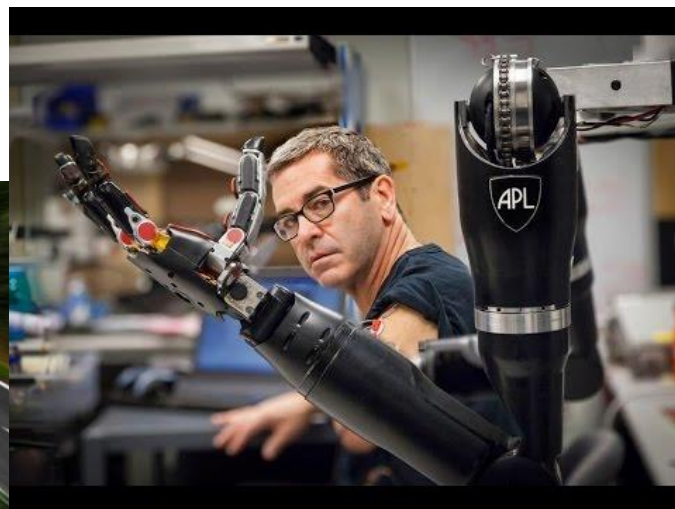
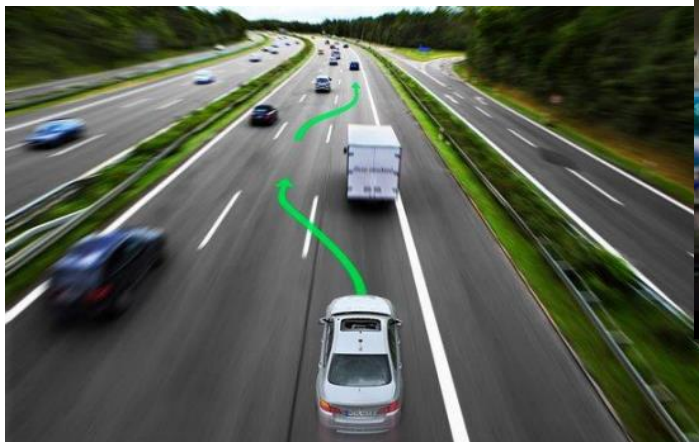


Bettina Könighofer

bettina.koenighofer@tugraz.at

July 23, 2024

Design Trustworthy AI-based Systems



Design Trustworthy AI-based Systems

Safety

Explainability

Accountability

Fairness

Robustness

Sustainability

Security

Privacy

Bernhard
Aichernig



Franz
Wotawa



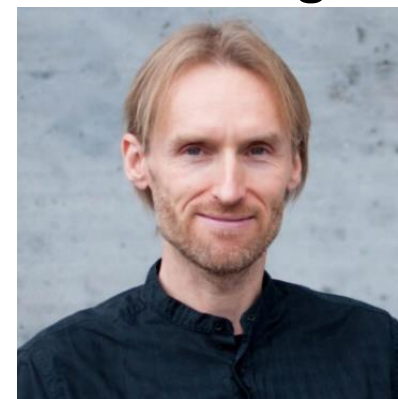
Roman Kern



Roderick Bloem



Christian
Rechberger



Elisabeth Lex



Bettina
Könighofer



Martin
Tappler



Institute for Security (IAIK)



**STEFAN
MANGARD**



**RODERICK
BLOEM**



**MARIA
EICHLSEDER**



**DANIEL
GRUSS**



**BETTINA
KÖNIGHOFER**



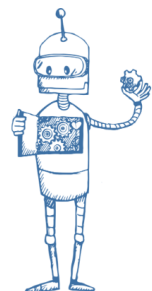
**CHRISTIAN
RECHBERGER**



**SUJOY
SINHA ROY**

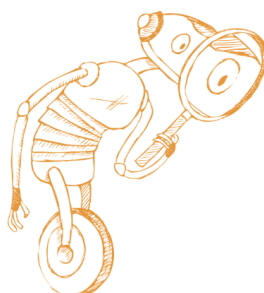
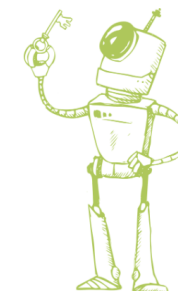


**REINHARD
POSCH**



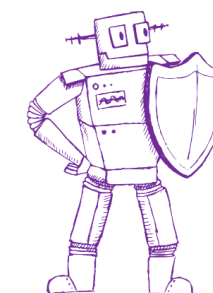
**SECURE
SYSTEMS**

**CRYPTOLOGY &
PRIVACY**



**FORMAL
METHODS**

**SECURE
APPLICATIONS**



Trusted AI Group at IAIK

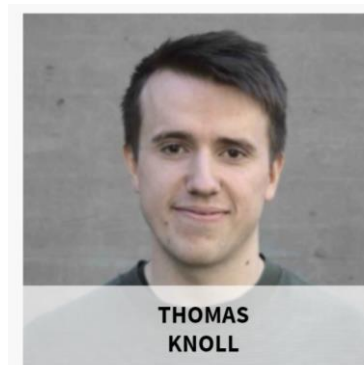
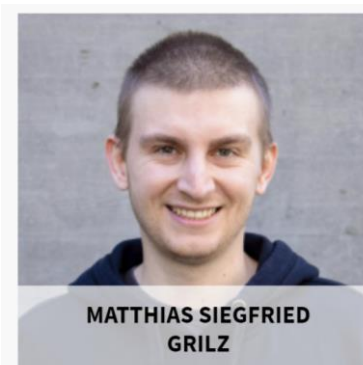
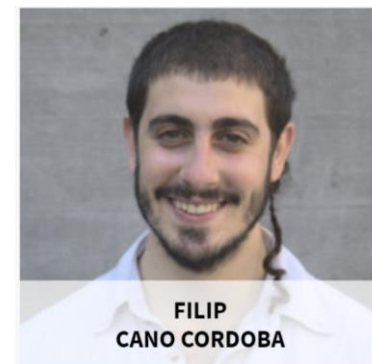
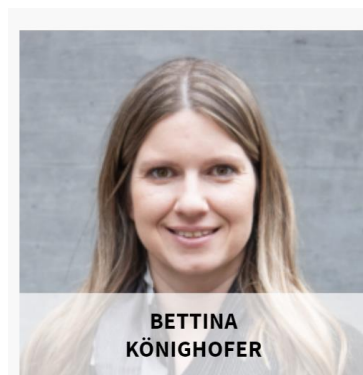
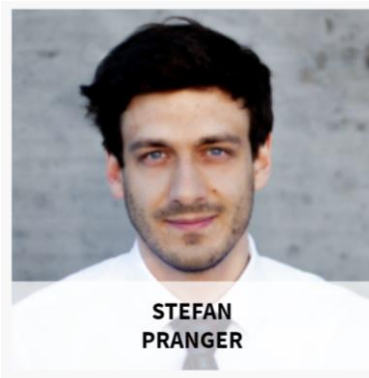
Safety

Explainability

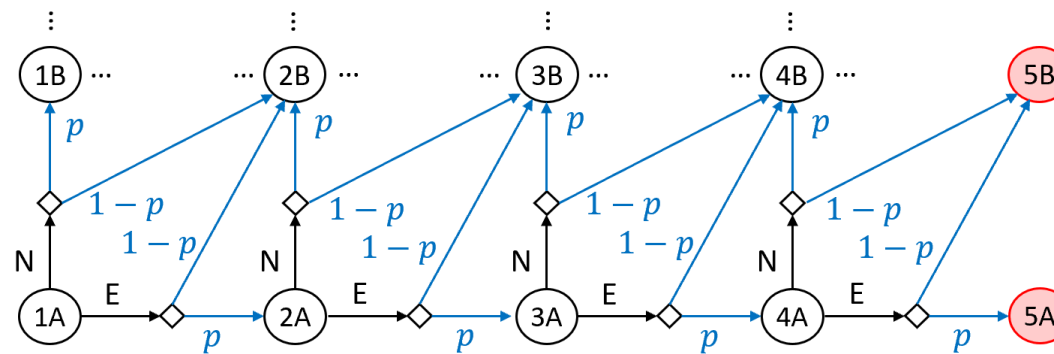
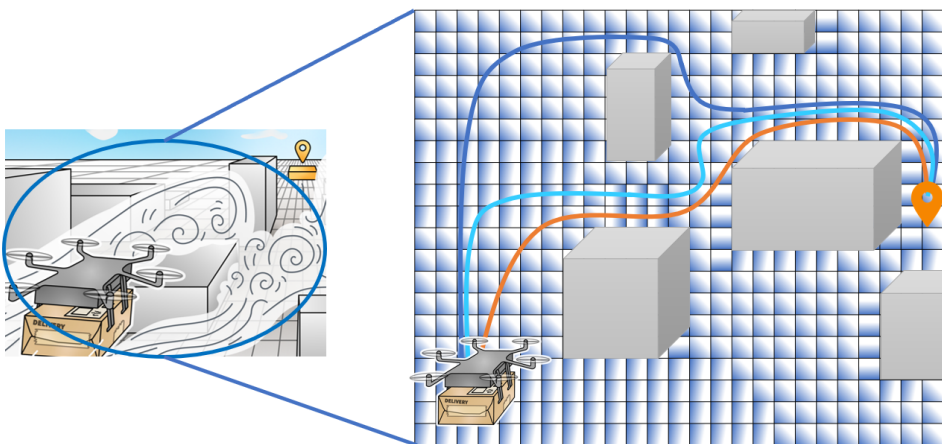
Accountability

Fairness

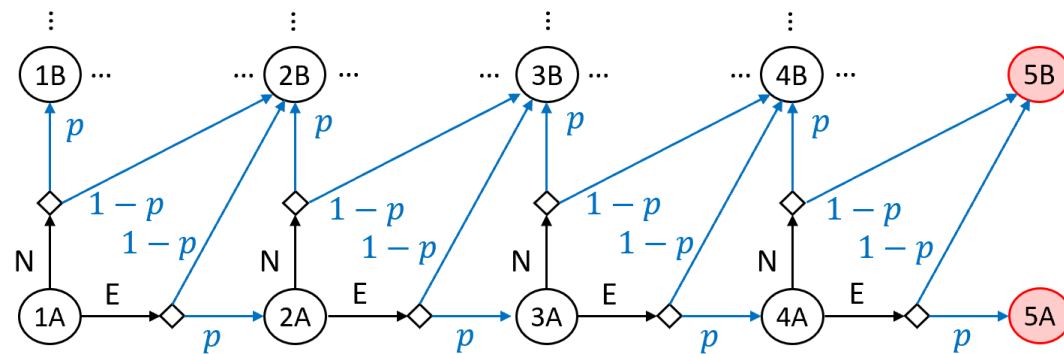
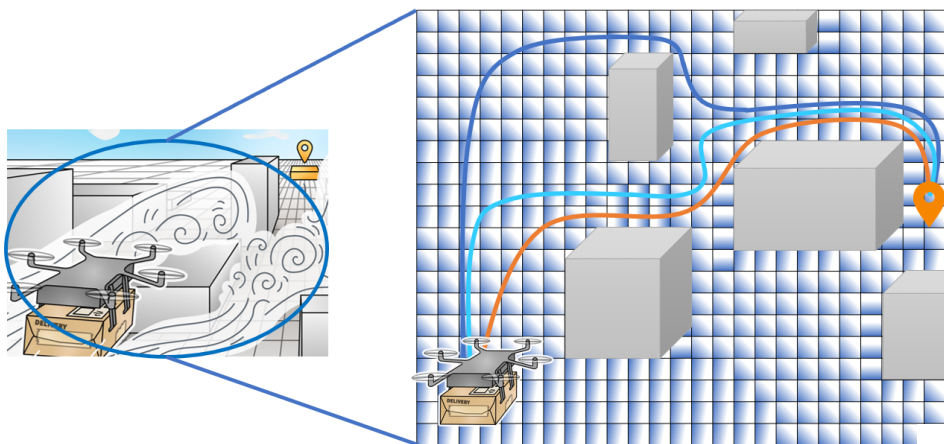
Robustness



Model system behaviour

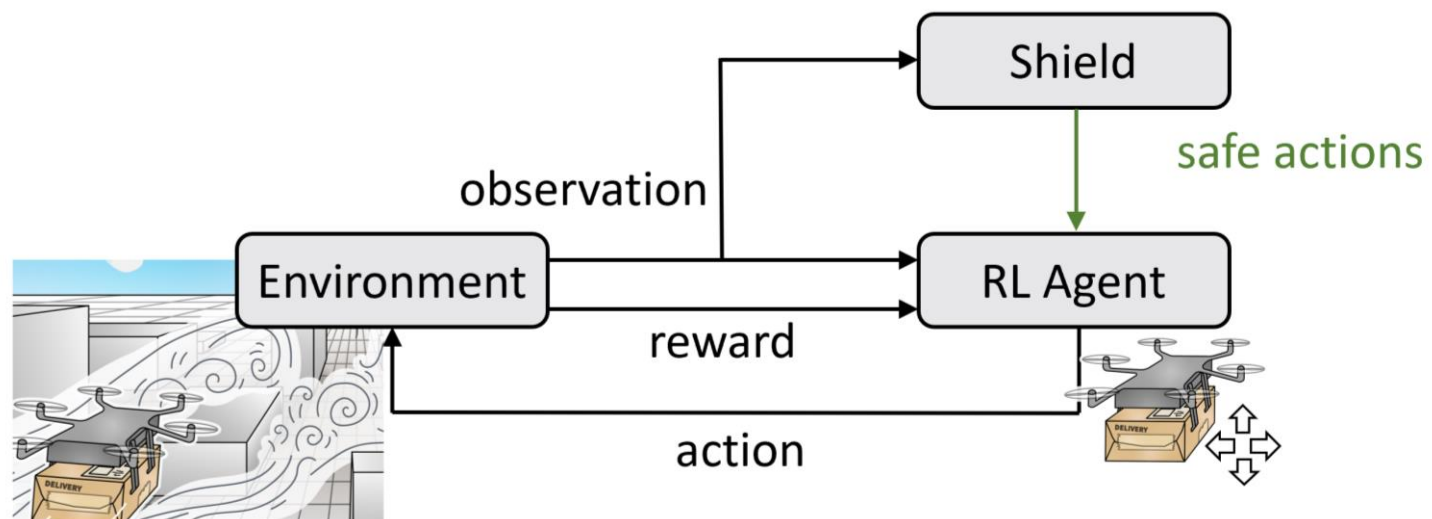


Model system behaviour



Use model

- Testing, Verification
- Enforcing Safety
- Monitoring Fairness
- Explainability
- Risk Analysis...



Thank you!

Contact me for collaborations

- Joint project proposals
- Fair and correct decision making
- Fundamental research / industrial applications

Bettina Könighofer

bettina.koenighofer@tugraz.at

