# Bridging the Gap Between Protocol Design and Implementation through Automated Mapping

Daniel Jackson (MIT), Eunsuk Kang (CMU), Stéphane Lafortune (University of Michigan), Rômulo Meira-Góes (CMU), Cristina Nita-Rotaru (Northeastern University), and Stavros Tripakis [PD] (Northeastern University)

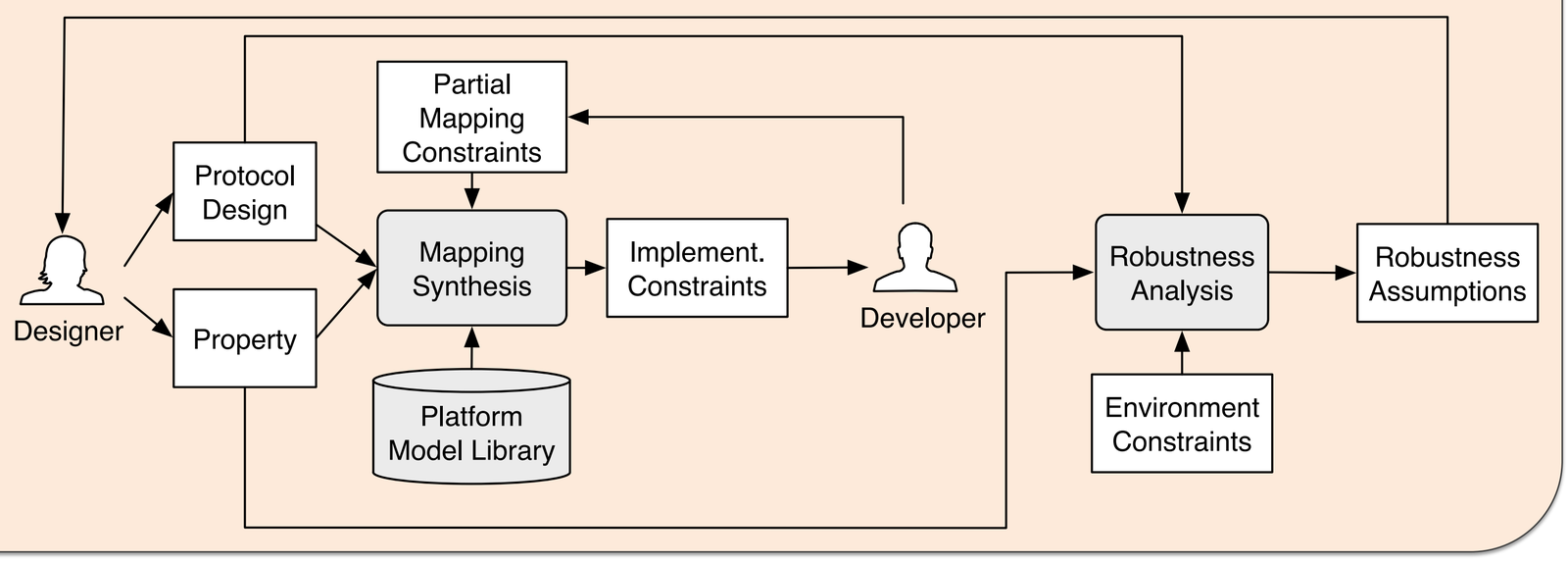
Award numbers: CNS-1801546 (Northeastern-Lead), CNS-1801342 (Michigan), CNS-1801399 (MIT)

Project Website

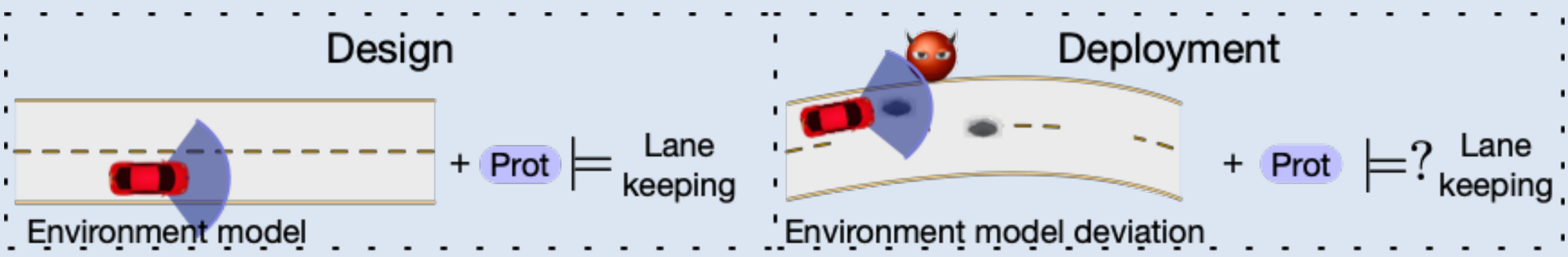
**Project Objective**: *Develop formal methodologies for building protocols that provably obey rigorous security guarantees.*

Impact:

- Increase trustworthiness in security protocols
- Novel ways of finding vulnerabilities and attacks
- Novel ways of analyzing robustness for security of protocols




**Robustness Challenge:** *Which environmental deviations can a protocol tolerate?*




**Objective**:

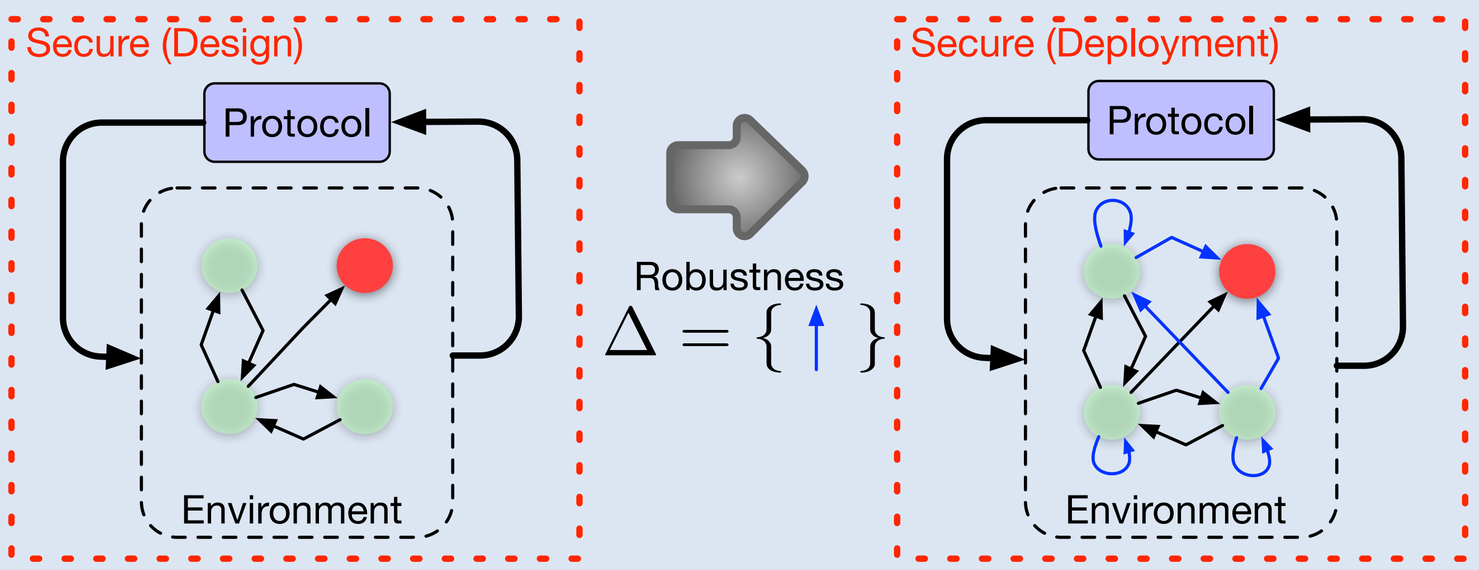
- Analyze protocol robustness against model deviations
- Model deviations due to security threats
- Compare protocols with respect to their security robustness
- Design protocols with desired security robustness levels

**Approach**:

- Discrete-transition models
- Linear-time properties
- Deviations modeled as additional transitions
- Robustness = all robust deviations
- Identify structural properties of protocols with respect to security robustness

**Solution:**

- Protocol is secure even under certain deviations
- General solution via model checking
- Maximum deviation with respect to invariance properties




As security protocols form a backbone in today's web infrastructure, understanding their security properties and improving their robustness is crucial

This project:

- Bridged the gap between the formal methods and security communities
- Trained a body of undergrad. and grad. students and research fellows
- Is applicable to cyber-systems and to abstracted models of cyber-physical systems