2022 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

High-Assurance Design of Learning-Enabled Cyber-Physical Systems with Deep Contracts

Pierluigi Nuzzo, University of Southern California

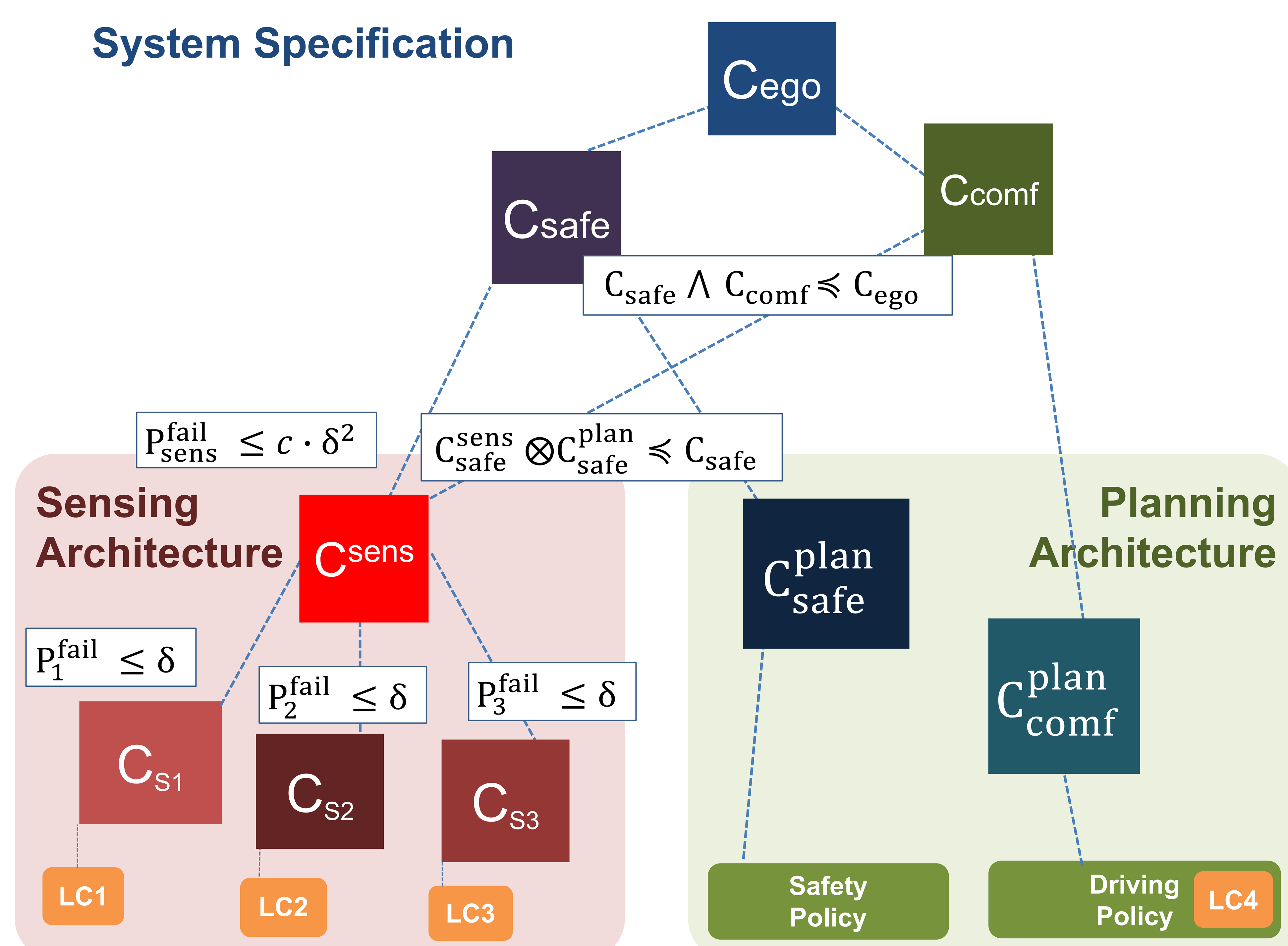
Challenge: Modern AI techniques enable system adaptiveness and resilience but also bring more complexity, uncertainty, and approximations in the design

Objective: *A* ***holistic, modular framework*** *(modeling techniques, specification formalisms, and scalable algorithms) for the* ***design and analysis of AI-enabled cyber-physical systems*** *with* ***strong guarantees of correctness***

Approach: Reasoning with ***contracts*** (assume-guarantee pairs):

- ***Context-aware:*** Describe components conditioned to their environment
- ***Compositional:*** Enable modular verification, hierarchical refinement, and design reuse based on a rigorous calculus
- ***Stochastic:*** Effectively express and propagate ***uncertainty*** at different abstraction layers

Award #1846524, 07/2019-06/2024



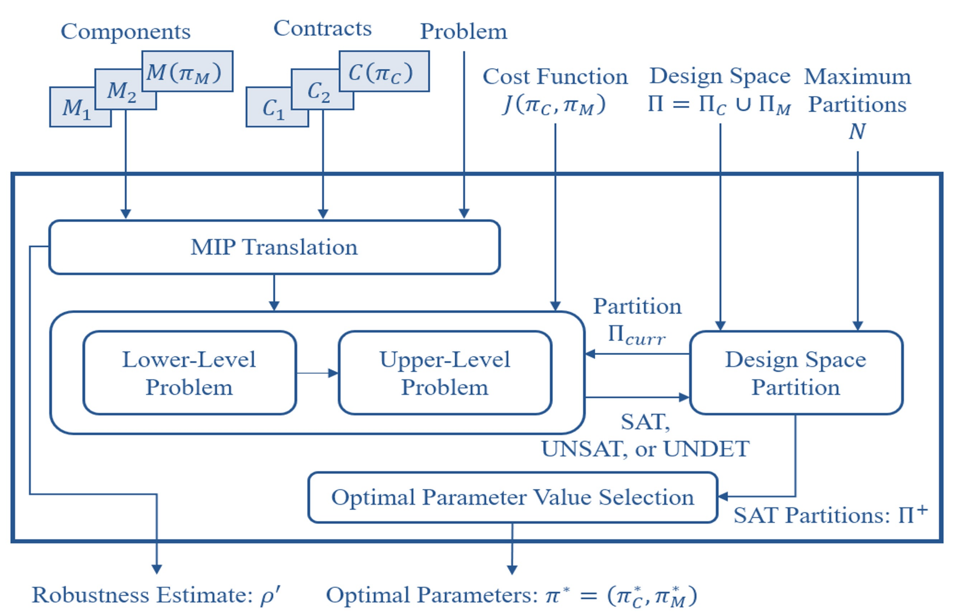
Impact: Provide the foundations for **rapid, compositional, certified design and operation** of **adaptive and resilient AI-enabled cyber-physical systems** for many applications: autonomous vehicles, robotics, industrial automation, medical devices, ...

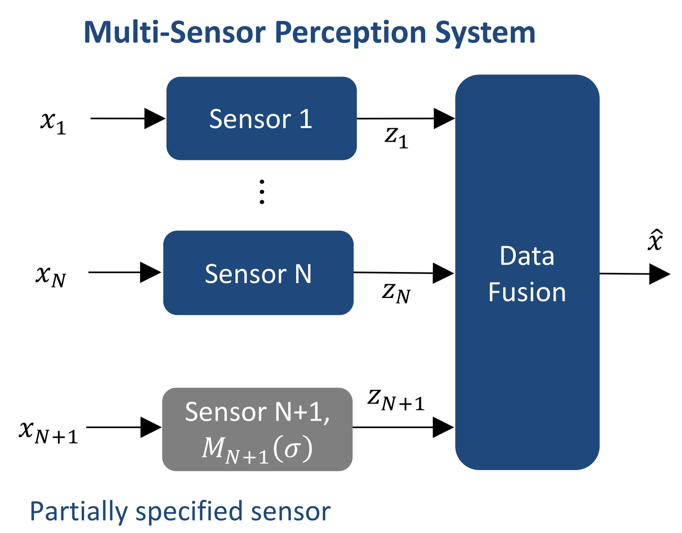
Educational program: Focus on systems engineering concepts and multidisciplinary methods to realize safe and cost-effective intelligent systems

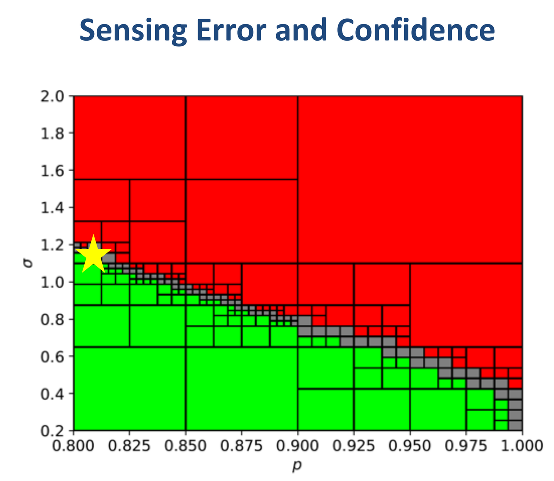
- **Pre-college:** via summer programs
- **Undergraduate and graduate:** via laboratory activities (**USC AutoDRIVE Lab**) and associated initiatives such as the **USC Autonomous Vehicles Club**, and the USC autonomous driving **RaceOn!** competition

High-Assurance Design of Learning-Enabled Cyber-Physical Systems with Contracts: Accomplishments

Stochastic Contracts: Quantitative Requirement Analysis



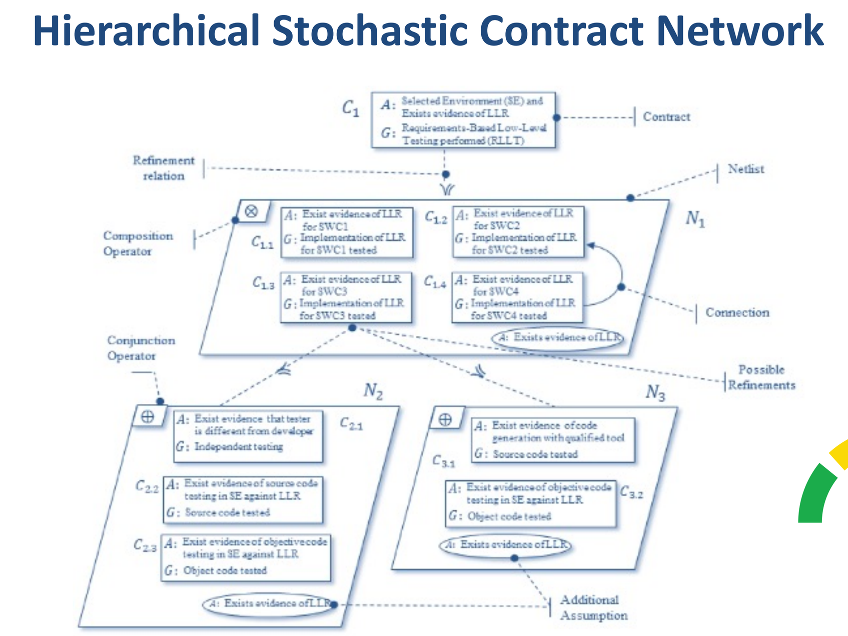


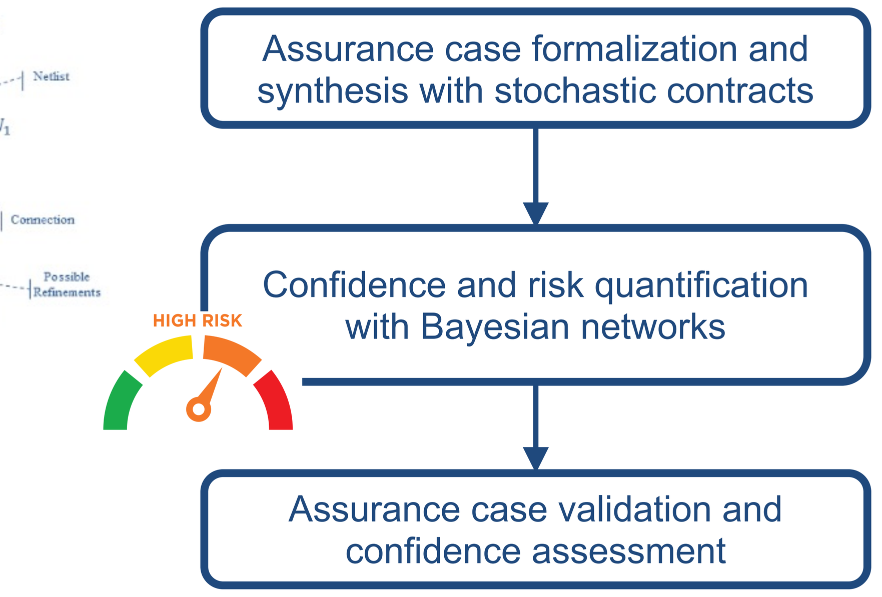


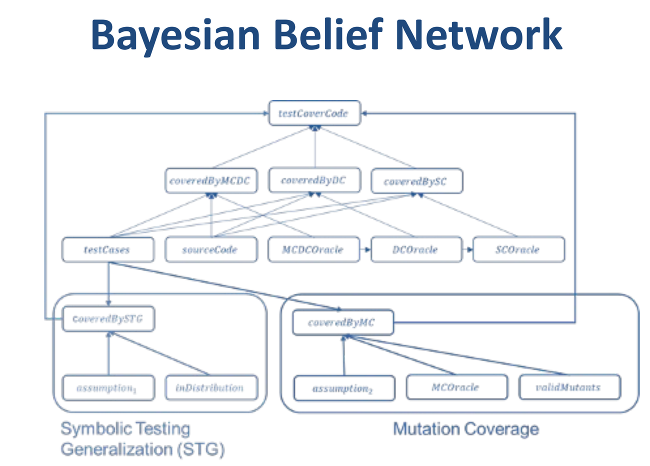
The **quantitative semantics of StSTL** enables quantifying the degree of satisfaction of an StSTL formula and formulate **robust verification, parameter synthesis** and **design space exploration problems**

TECS'19, DATE'19, ICCAD'22

Automated Construction of Assurance Cases



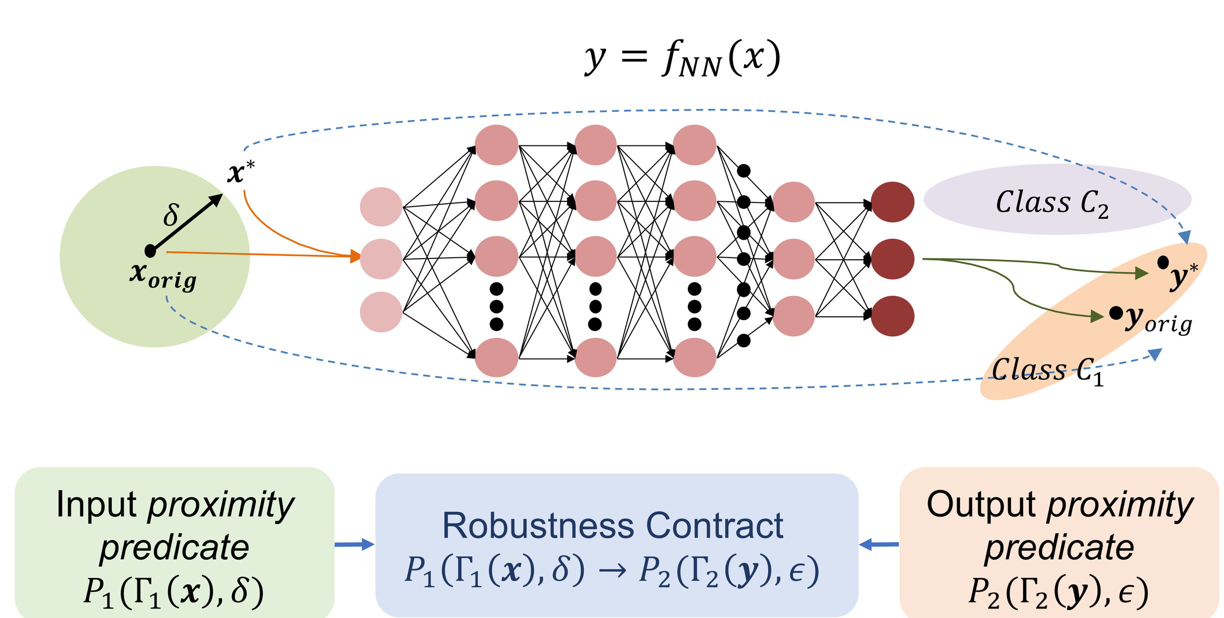


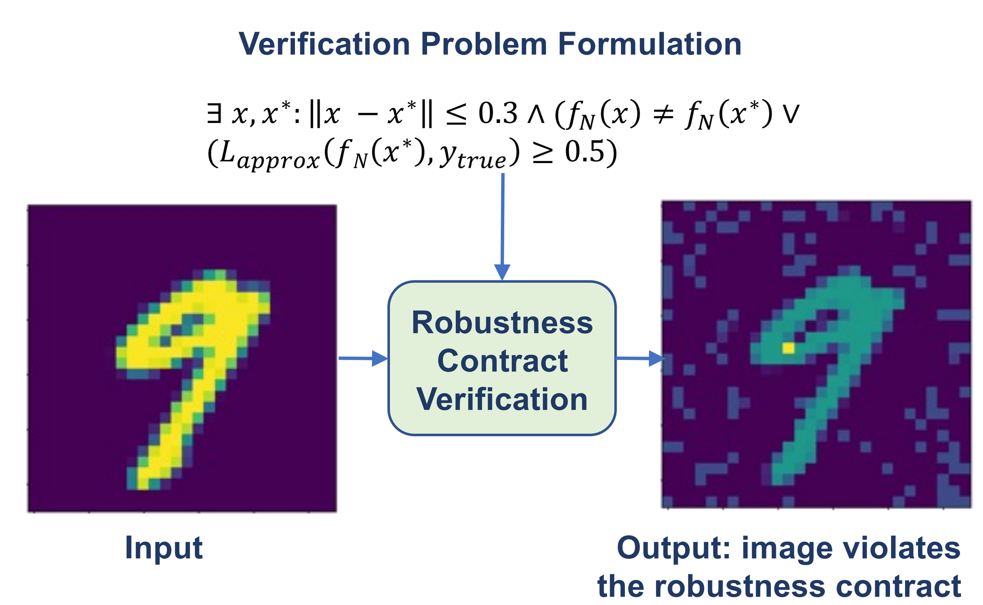


Stochastic contracts provide the **semantic foundation** for the **automated construction of assurance cases**, structured arguments about system dependability, which can accelerate **system certification** and help transition from a process-driven to a **property-driven certification** approach

NFM' 22, SAFECOMP' 22

Robustness Contracts for AI-Enabled Components





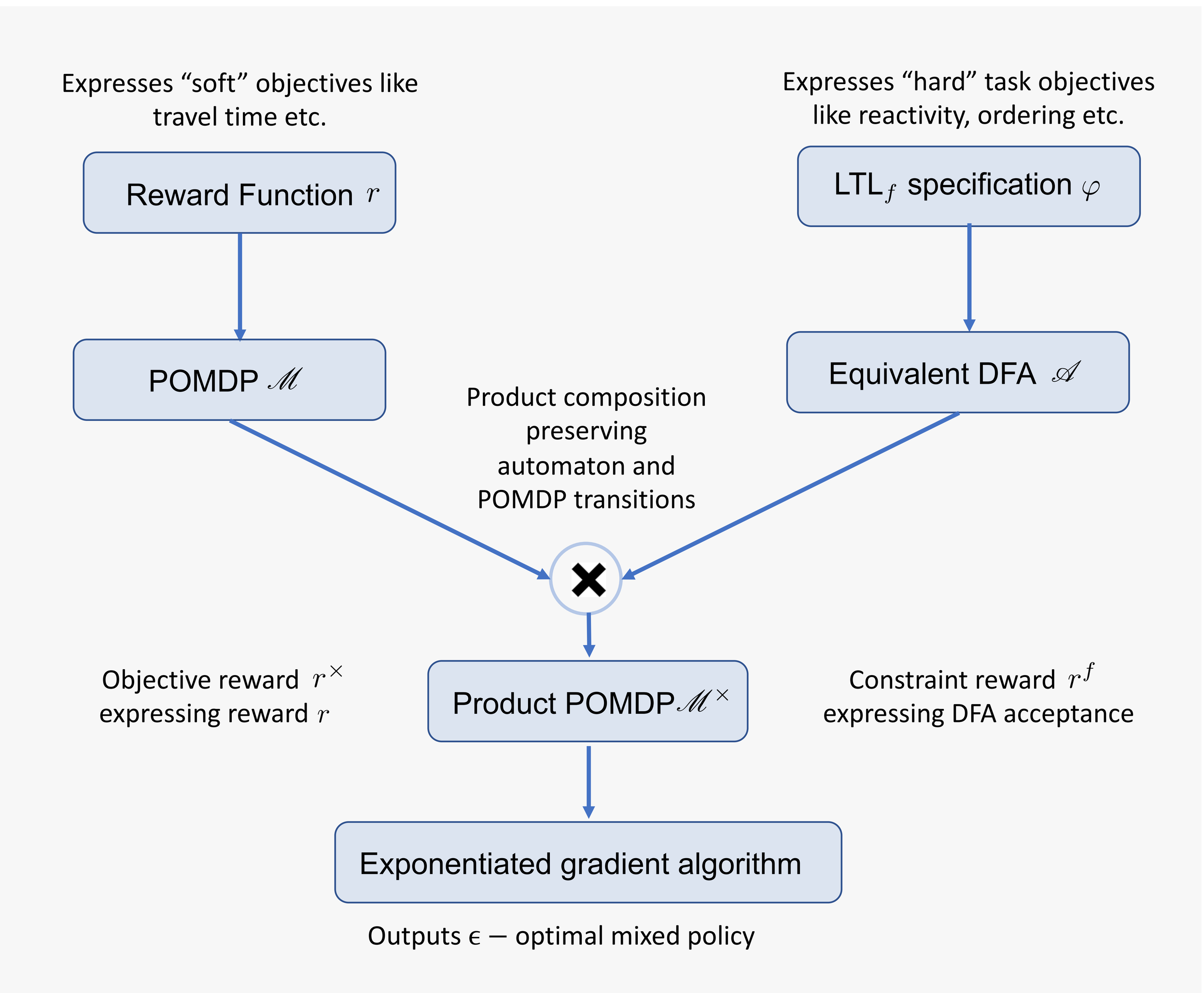
Enable **verification of neural network-based components** against multiple robustness criteria and **compositional verification of closed-loop systems** with deep reinforcement learning controllers against perception errors

MEMOCODE'20,
Best Paper Award

Synthesis of Optimal Control and Reinforcement Learning Policies Under Mission-Critical Constraints

Optimal planning via **reinforcement learning** for Markov decision processes under **signal temporal logic** specifications

Optimal planning for **partially observable Markov decision processes** under **finite linear temporal logic** specifications



AAAI'21, ACC'21, CDC'21, UAI'22