From One To Many: Checking A Set Of Models

Rohit Dureja and Kristin Yvonne Rozier

Iowa State University

October 4, 2016
Complex systems’ design often requires analyzing several models of the system under development.
Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
Motivation

Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
- Check capabilities of systems with varying features, and
Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
- Check capabilities of systems with varying features, and
- Regression development to make a design robust.
Motivation

Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
- Check capabilities of systems with varying features, and
- Regression development to make a design robust.
Lift traditional model checking to model-set checking.

For every Model-Requirement pair

System Model $M$

Requirement $\varphi$

Traditional Model Checker

Model Set $M = \{M_1, \ldots, M_n\}$

Requirements Set $\mathcal{P} = \{\varphi_1, \ldots, \varphi_m\}$

Proof $M \models \varphi$

Error Trace $M \not\models \varphi$

Report

- Proof
- Trace