

Compositional Model Checking Analysis: Suggestions and Explanations

Daniel Larraz

University of Iowa

1 Rules

Format: suggestion (conclusion), list of explanations (premises).

- *Suggestion 1*: No action required.
 - All components of the system satisfy their contract.
 - No component of the system was refined.
- *Suggestion 2*: Fix M 's contract.
 - Component N is correct after refinement.
 - M is a subcomponent of N .
 - M 's contract is too weak to prove N 's contract, but M 's definition is strong enough.
- *Suggestion 3*: Either complete specification of N 's contract, or remove component M .
 - Component N satisfies its current contract.
 - M is a direct subcomponent of N .
 - One or more assumptions of subcomponent M are not satisfied by N .
- *Suggestion 4*: Either make A weaker, or fix N 's definition to satisfy A .
 - Component N doesn't satisfy its contract after refinement.
 - Assumption A of subcomponent M is not satisfied by N .
- *Suggestion 5*: Either make N 's assumptions stronger, or fix N 's definition to satisfy N 's guarantees.
 - Component N doesn't satisfy its contract after refinement.
 - Either N has no subcomponents, or all its subcomponents satisfy their contract.
- *Suggestion 6*: Fix reported issues for N 's subcomponents.
 - Component N doesn't satisfy its contract after refinement.
 - One or more subcomponents of N don't satisfy their contract.