Context

Something about using Sagar's or Dan's work on LLVM analysis

Context

Something about IKOS?

Comment

Each service corresponds to its specification

DaCosta

Code-Specification Corresponence

Code can statically be shown to

correspond to its specification

Also ties into AutoCorres

Backes

Formal reasoning tools exist for LLVM, something about CVMC, Clie, Boogie, Java Path Finder

Comment

Services in Lustre?

Kingston

Can either synthesize C/C++/etc. code from a formal specification (e.g., PVS/LEAN/Coq), extract a specification from an implementation, perform checks on the implementation, or if we're heretics, we could rely on testing

Comment

(see StatisAnalysisMitigation argument)