The Formal Verification of a Reintegration Protocol

Lee Pike\textsuperscript{1}  Steven D. Johnson\textsuperscript{2}

\textsuperscript{1}Galois Connections, Inc.
leepike@galois.com

This work was completed while a member of the Formal Methods Group at the NASA Langley Research Center.

\textsuperscript{2}Indiana University
sjohnson@cs.indiana.edu

September 20, 2005
The reintegration protocol was developed by Wilfredo Torres-Pomales, Mahyar Malekpour, and Paul Miner (NASA Langley Research Center).

Bruno Dutertre and Leonardo de Moura (SRI, International) provided many helpful suggestions concerning SAL.
SPIDER (Scalable Processor-Independent Design for Enhanced Reliability) is an ultra-reliable safety-critical fly-by-wire distributed architecture being designed in-house at NASA Langley.¹

The SPIDER Reintegration Protocol allows a node that has suffered a transient fault to regain consistent state with the operational nodes in the system in the presence of faults.

The verification is carried out using SRI International’s Symbolic Analysis Laboratory (SAL). SAL includes a bounded model checker and combined decision procedures for automated verification of infinite-state systems via $k$-induction.

This is the first verification of a reintegration protocol, but it should be extensible to the verification of reintegration in systems similar to SPIDER, e.g., the Time-Triggered Architecture (TTA).

Industrial case-study in using brand-new verification technology combining induction via bounded model-checking and Satisfiability Modulo Theories (SMT) decision procedures for easy parameterized proof of correctness.

Builds on the “Timeout Automata” modeling approach developed by Bruno Dutertre and Maria Sorea (SRI).²

Techniques for modeling faults, time-triggered behavior, and time-progress that reduce the number of transitions required to prove a property by $k$-induction are presented in the paper.

Now What?

- This technique is particularly well-suited for parameterized verification of real-time partially-synchronous systems.
- SMT is attracting significant interest in academia and industry.
- More nontrivial case-studies are needed to direct the development of this technology (this case-study was a principal source of benchmarks in the recent SMT competition held at CAV, 2005).
Pointers

Full technical report & source files
http://www.cs.indiana.edu/~lepike/
Google: lee pike

SPIDER
http://shemesh.larc.nasa.gov/fm/spider/
Google: formal methods spider

SAL
http://sal.csl.sri.com/
Google: SRI symbolic analysis