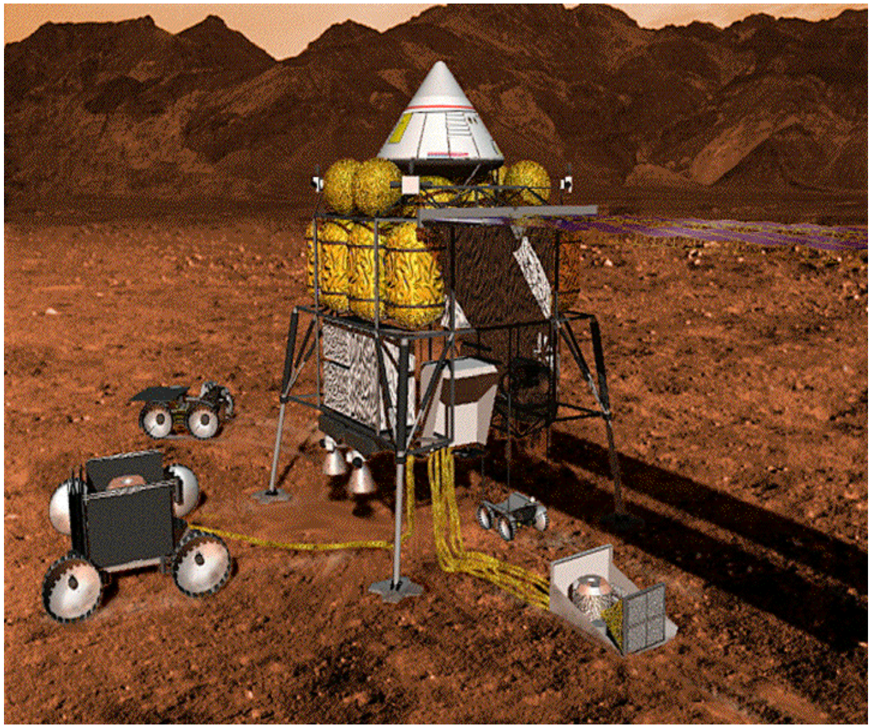
Verification of Autonomy Software

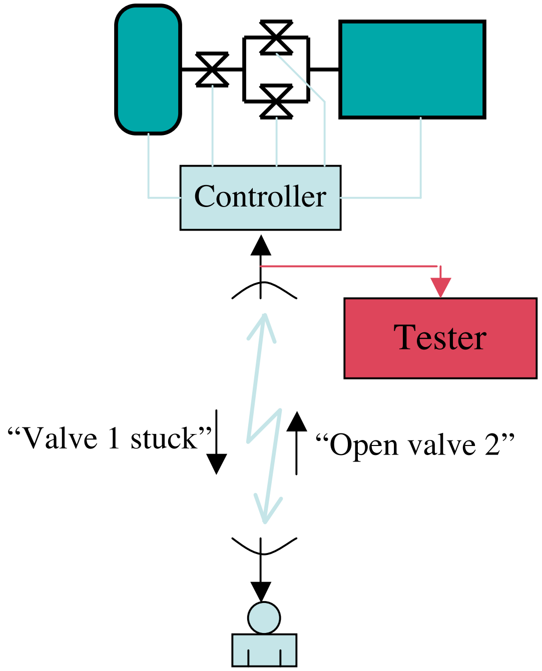


Contact: Charles Pecheur (RIACS)

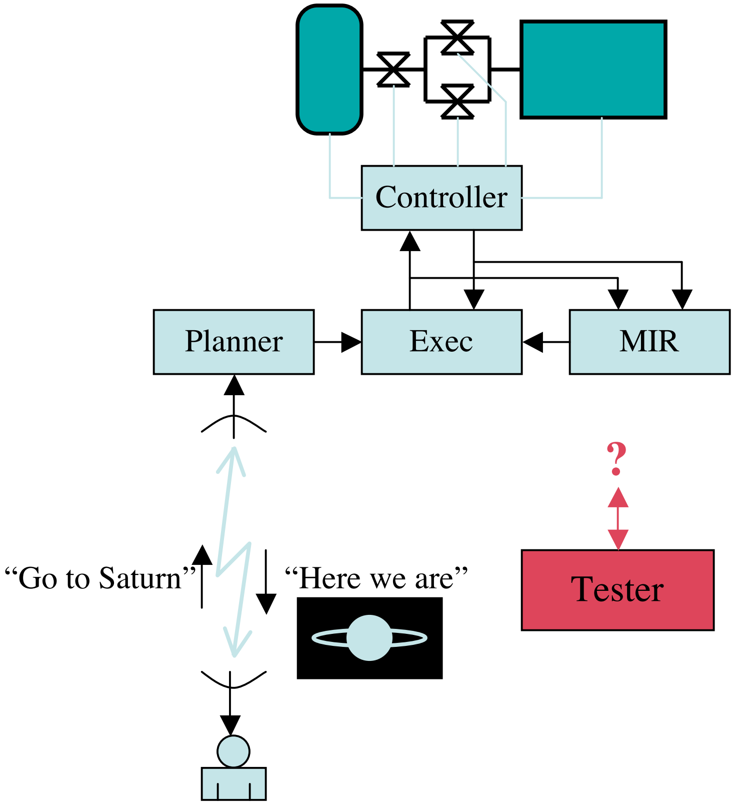
`pecheur@email.arc.nasa.gov`

with Tony Lindsey (QSS)
Stacy Nelson (NelsonConsult)
Reid Simmons (Carnegie Mellon)
Alessandro Cimatti (IRST, Italy)

Controlled vs. Autonomous



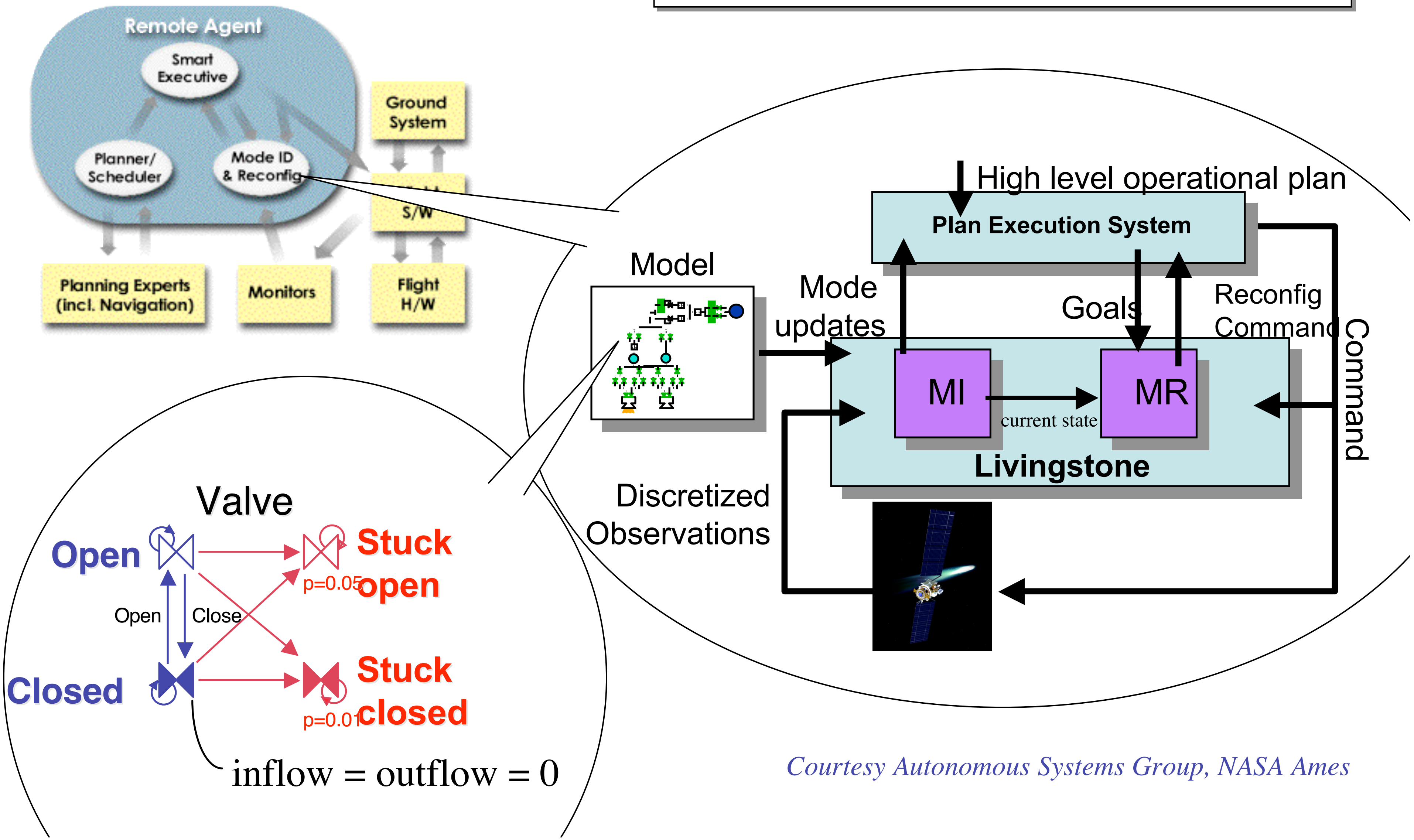
- Short time cycle (sec..min)
- Human deals with unexpected
- Open-loop, easy to test
- Tractable state space, testing is appropriate



- Long time cycle (day..year)
- Machine deals with unexpected
- Closed-loop, hard to test
- Huge state space, testing is insufficient

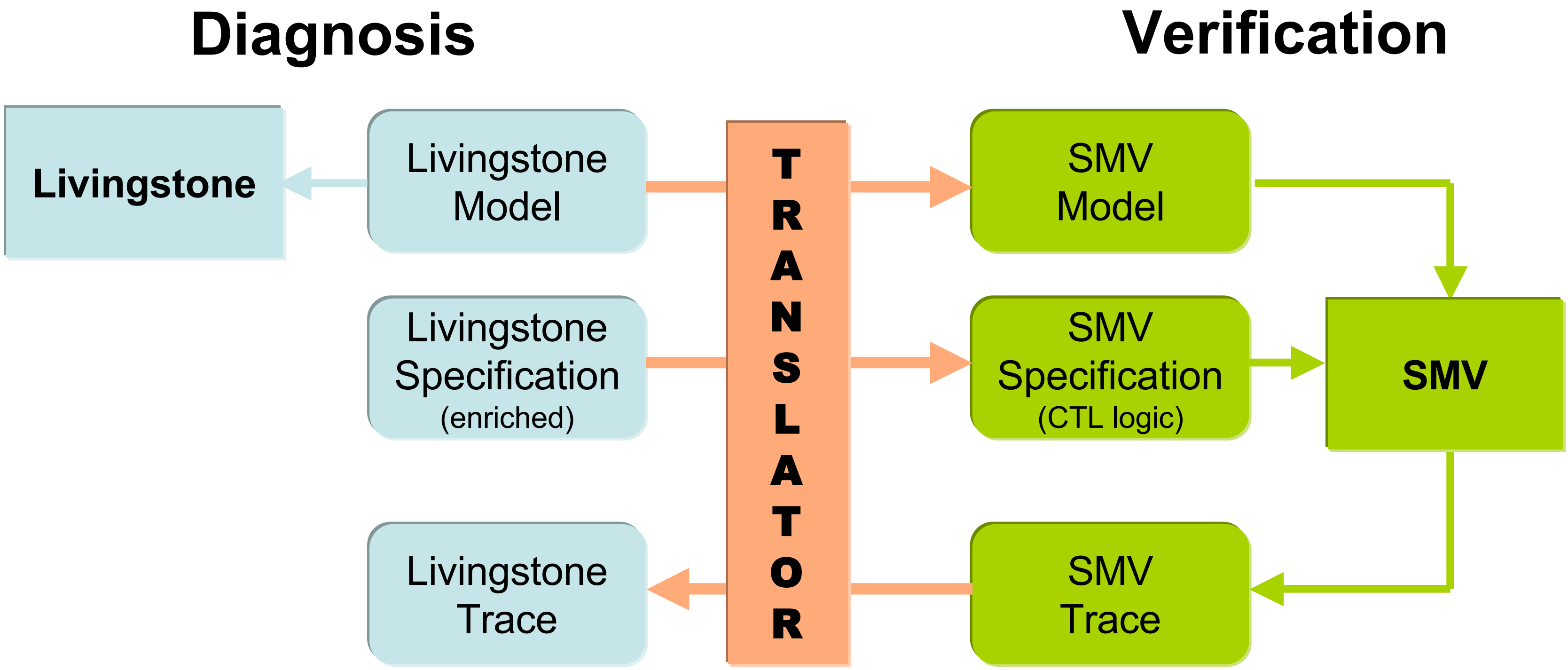
Livingstone

A model-based diagnosis system, uses a discrete, qualitative model to detect and diagnose faults.



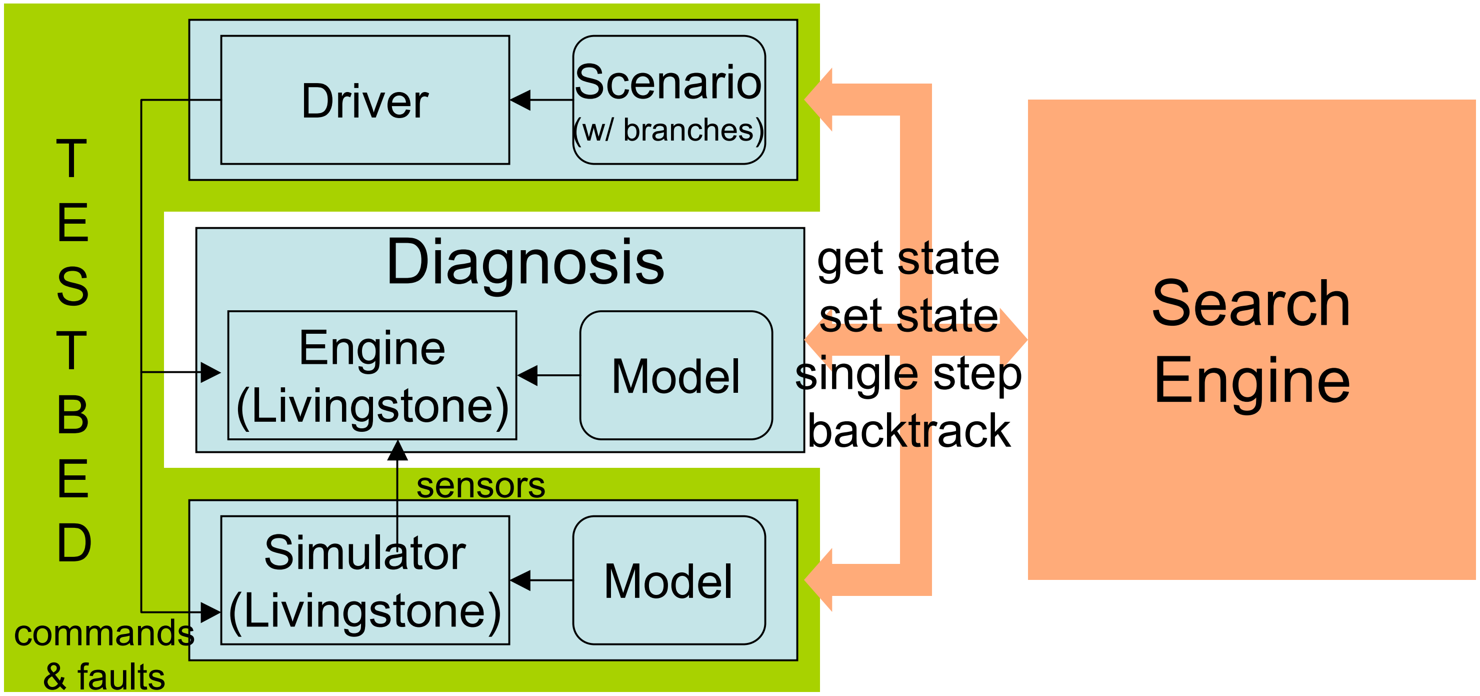
Courtesy Autonomous Systems Group, NASA Ames

Livingstone-to-SMV Translator



- Allows exhaustive analysis of Livingstone models (10^{50+} states)
- Uses SMV: symbolic model checker (BDD and SAT)
- Enriched spec syntax (vs. SMV's core temporal logic)
- Hide away SMV, offer a model checker for Livingstone
- Graphical interface, trace display

Livingstone PathFinder (LPF)

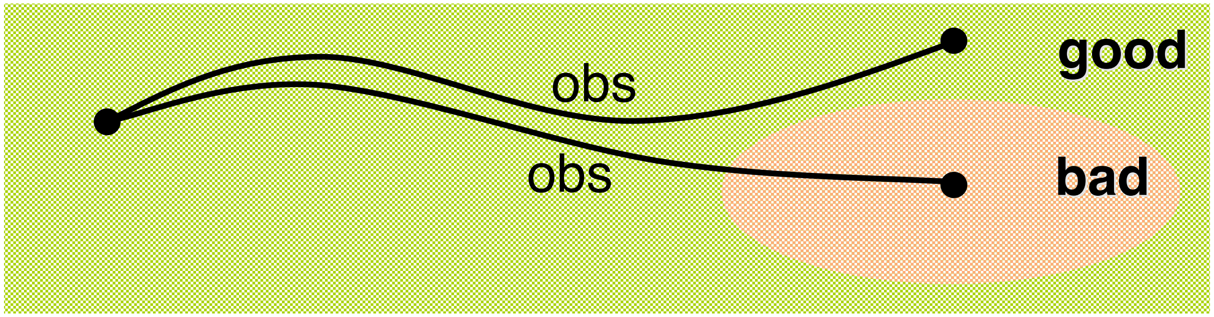


- Execute the Real Program in a simulated environment (testbed)
- Instrument the Code to be able to backtrack between alternate paths
- Modular architecture, allows different diagnosis, simulators, search algorithms
    - e.g. depth-first / breadth-first / random / guided / interactive / ...

Verification of Diagnosability

Q: From observations (input/output), can diagnosis always tell when plant comes to a bad state?

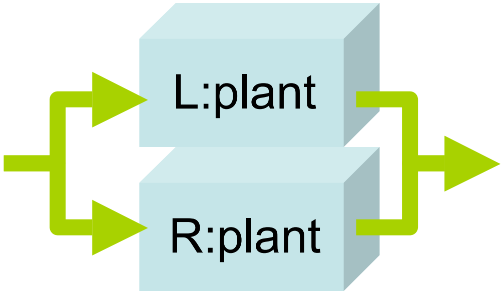
A: **YES unless** plant can go good or bad with the same observations (and therefore diagnosis cannot tell)



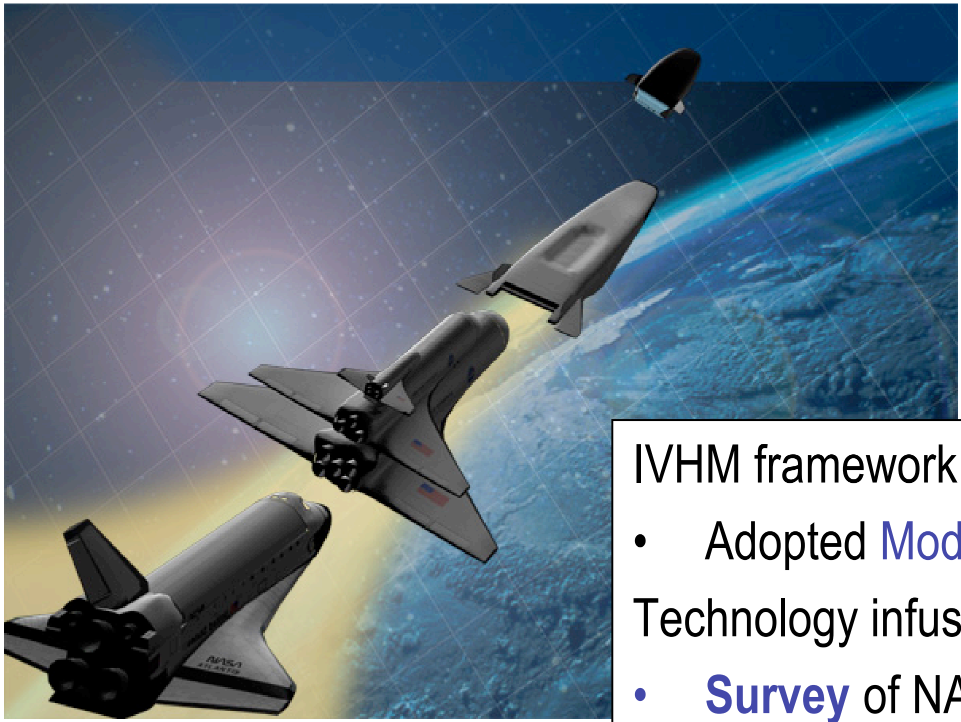
Verification using model checking (SMV)

- Two "siamese twin" copies of the plant (L/R), with coupled observations
- verify that one cannot reach:

  (L **in** good) **and** (R **in** bad)



Verification of IVHM* for Next-Gen Space Vehicle



***IVHM** = Integrated Vehicle Health Management
= Integrated prognosis/diagnosis

IVHM framework developed by Northrop Grumman Corp.

- Adopted Model-Based Diagnosis, including Livingstone

Technology infusion project:

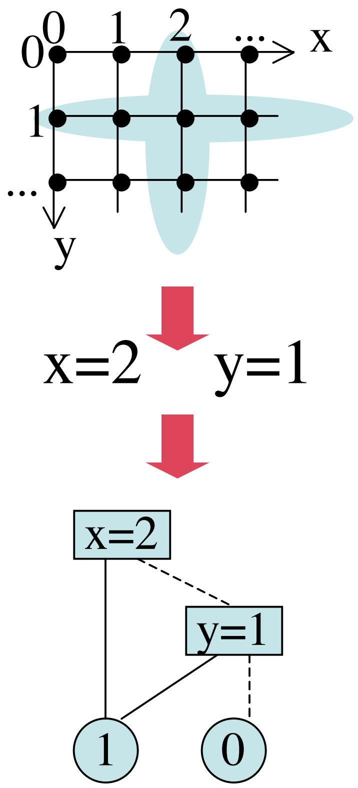
- **Survey** of NASA current V&V practice, applicable formal methods, our verification tools
  See **ase.arc.nasa.gov/vvivhm**
- **Maturation** of Livingstone verification tools (translator and LPF): tool extensions, GUI, improved documentation and packaging, integration with other IVHM tools

Symbolic Model Checking

Model Checking = verification by exhaustive exploration

- + Full coverage (incl. non-determinism)
- – Limited by state space explosion

- **Symbolic** Model Checking =
  Processes **sets of states**,
  Represented as **boolean formulas**,
  Encoded as **binary decision diagrams** (**BDDs**).
- Can handle larger state spaces (10^{50} and up)
  - – but BDD size can explode too
- Works very well for Livingstone models
- Most widely used: SMV (Carnegie Mellon / Cadence / IRST)
- Variant: **Bounded Model Checking** using **SAT** solvers



To Probe Further

On-Line

- **Livingstone to SMV Translator:** ase.arc.nasa.gov/mpl2smv
- **Livingstone PathFinder:** ase.arc.nasa.gov/lpf
- **Verification of IVHM:** ase.arc.nasa.gov/vvivhm

Publications

- Stacy Nelson, Charles Pecheur. **Formal Verification of a Next-Generation Space Shuttle.** FAABS II, Greenbelt, MD, October 2002. To be published in LNCS.
- Charles Pecheur, Alessandro Cimatti. **Formal Verification of Diagnosability via Symbolic Model Checking**. MoChArt-2002, Lyon, France, July 2002.
- Steven Brown, Charles Pecheur. **Model-Based Verification of Diagnostic Systems.** Proceedings of JANNAF Joint Meeting, Destin, FL, April 8-12, 2002.
- Charles Pecheur, Reid Simmons. **From Livingstone to SMV: Formal Verification for Autonomous Spacecrafts.** FAABS I, April 2000. LNCS 1871, Springer Verlag.

Reports

- Stacy Nelson, Charles Pecheur. **NASA processes/methods applicable to IVHM V&V**. NASA/CR-2002-211401, April 2002.
- Stacy Nelson, Charles Pecheur. **Methods for V&V of IVHM intelligent systems**. NASA/CR-2002-211402, April 2002.
- Stacy Nelson, Charles Pecheur. **Diagnostic Model V&V Plan/Methods for DME.** NASA/CR-2002-211403, April 2002.
- Charles Pecheur. **Verification and Validation of Autonomy Software at NASA**. NASA/TM 2000-209602, August 2000.

Publications and Reports available on-line at:

http://ase.arc.nasa.gov/pecheur/publi.html