Verification and Validation of
Model-Based Autonomous Systems

Charles Pecheur, RIACS (ARC)
Project Profile

- 3-year project, FY99 to FY01
- Performed by ARC,
  With grant to CMU (Reid Simmons),
  Delivered to KSC.
- Goal: support V&V of Livingstone-based applications by the application developers (not by V&V experts)
- Two complementary approaches:
  - Symbolic model checking of models
  - Closed-loop verification of applications
Model-Based Autonomy

- Based on AI technology
- General reasoning engine + application-specific model
- Use model to respond to unanticipated situations
The Livingstone MIR

Remote Agent's model-based fault recovery sub-system

---

Courtesy Autonomous Systems Group, NASA Ames

© Charles Pecheur
Autonomy

Livingstone

Livingstone Model

Livingstone Requirement

Livingstone Trace

Verification

SMV

MPL

2

SMV Model

© Charles Pecheur
Livingstone to SMV Translation

Livingstone Model
(defcomponent valve ()
  (:inputs (cmd :type valve-cmd))
  ...
  (Closed :type ok-mode
    :transitions
    ((do-open :when (open cmd)
      :next Open) ...))
  (StuckC :type :fault-mode ...)
  ...
)

SMV Model
MODULE valve
VAR mode: {Open,Closed,
    StuckO,StuckC};
    cmd: {open,close};
DEFINE faults:=[StuckO,StuckC];
TRANS
(mode=Closed & cmd=open) ->
  (next(mode)=Open | next(mode) in faults)
Symbolic Model Checking

- Manipulates sets of states,
  Represented as boolean formulas,
  Encoded as binary decision diagrams.
- Can handle larger state spaces ($10^{50}$ and up).
- BDD computations:
  - Good in average but exponential in worst case.
  - Computation time depends on BDD size
    => number of variables, complexity of formulas,
    but not directly state space size.
- Example: SMV (Carnegie Mellon U.)
From Livingstone Models to SMV Models

• Co-developed with CMU
• Based on Livingstone 1 (Lisp)
• 4K lines of Lisp
• Similar nature => translation is easy
• Properties in temporal logic + pre-defined patterns
• Temporal queries
  – e.g. "what faults imply eventual recovery"
  – Proof-of-concept prototype (done at CMU)
  – deceptive results so far
• Migration to Livingstone 2 (in progress)
Application
In-Situ Propellant Production

- Use atmosphere from Mars to make fuel for return flight.
- Livingstone controller developed at NASA KSC.
- Components are tanks, reactors, valves, sensors...
- Exposed several (known and unknown) modelling errors.
- Latest model is $10^{55}$ states.
- Live experience of V&V methods used by non-specialists.

\[ \text{Mars atmosphere} \quad \text{on-board} \]
\[ \text{CO}_2 + 2\text{H}_2 \rightarrow \text{CH}_4 + \text{O}_2 \]

**NASA**
Closed-Loop Verification Principle

- Start from conventional testing (the real program).
- Instrument the code to be able to do full model checking (or as close as possible).
Livingstone PathFinder (LPF)

- Closed-loop verification for Livingstone.
- In Java, using Livingstone 2 (C++ via Java JNI).
  - Uses Livingstone 2 checkpointing.
- Scenario:
  (sequence of commands) \times (choice of faults)
- Livingstone-based simulator.
  - Supports under-constrained models.
- Open API between testbed and model checker
  - Re-use parts of Java model checker.
Publications and Presentations

Ames Research Center

• 3 Papers on Livingstone-to-SMV translator
  – Simmons & Pecheur, AAAI Spring Symposium (03/00)
  – Pecheur & Simmons, Goddard FAABS Workshop (04/00, book chapter in preparation)
  – Simmons & Pecheur, IROS Conference (11/00)

• 3 Presentations on V&V of ISPP
  – Engrand & Pecheur, Goddard FAABS workshop (poster, 04/00)
  – Engrand, RIACS V&V of A&A workshop (invited, 12/00)
  – Engrand, AAAI Spring Symposium MVI (03/01)

• 1 Survey paper on V&V of MBAS (to be submitted)
  – Pecheur, NASA/TM-2000-209602

• 2 Papers on ISPP including V&V
  – Gross et al., IAC 1999 (09/99)
  – Clancy et al., Technology 2009 (11/99)

• 2 Workshops on V&V of MBAS
  – RIACS V&V of Autonomous and Adaptive Systems (Pecheur, Simmons, Visser, 12/00)
  – AAAI Model-based Validation of Intelligence (Khatib, Pecheur, 03/01)

• 2 Tutorials on V&V including V&V of MBAS
  – Pecheur, Simmons, Visser & Havelund, Langley FM 2000 (06/00)
  – Pecheur & Visser, ASE 2000 (09/00)
Future Directions

- **MPL2SMV:**
  - FMEA analysis from Livingstone models.
  - Use SAT-solving and bounded model checking.
  - More user guidance (patterns, verification process tool).

- **Temporal Queries:**
  - Can it be made useful? More experiments, improve tool.

- **Livingstone PathFinder:**
  - Explore different exploration strategies, case studies.

- **Publications**
  - Survey paper, temporal queries, closed-loop verification, ...