



The HiVy⁺ Tool Set



Paula J. Pingree

Jet Propulsion Laboratory

Erich Mikk

Erlangen, Germany

Presented by Gordy Cucullu, Jet Propulsion Laboratory

July 2004





HiVy: Enables State-Chart Model Checking

- Motivation:
 - Validate software designs specified in StateFlow[®] state-charts (*.mdl model files)
 - The final mission code can be auto-generated from these model files
 - Developed a tool to auto-generate Promela, the input language of SPIN, from the same set of model files used to generate the final mission code.
 - Thereby we can follow the JPL testing philosophy, “Test what you fly, fly what you test”
 - Direct specification and validation of mission-critical software is possible using exhaustive model checking techniques
- Applications Flight Spacecraft:
 - Stateflow[®] auto-coding implemented on NASA’s Deep Space-1 & Deep Impact (DI) Projects
 - JPL R&TD used limited SPIN testing on DS-1, DI Fault Protection & Mars Exploration Rover Arbiter using HiVy
- About the Authors
 - Paula J. Pingree, senior JPL engineer in the System Engineering Technology Infusion Group. [paula.j.pingree@jpl.nasa.gov](mailto:Paula.j.pingree@jpl.nasa.gov)
 - Erich Mikk, PhD; personal collaboration effort; Erich.Mikk@epost.de

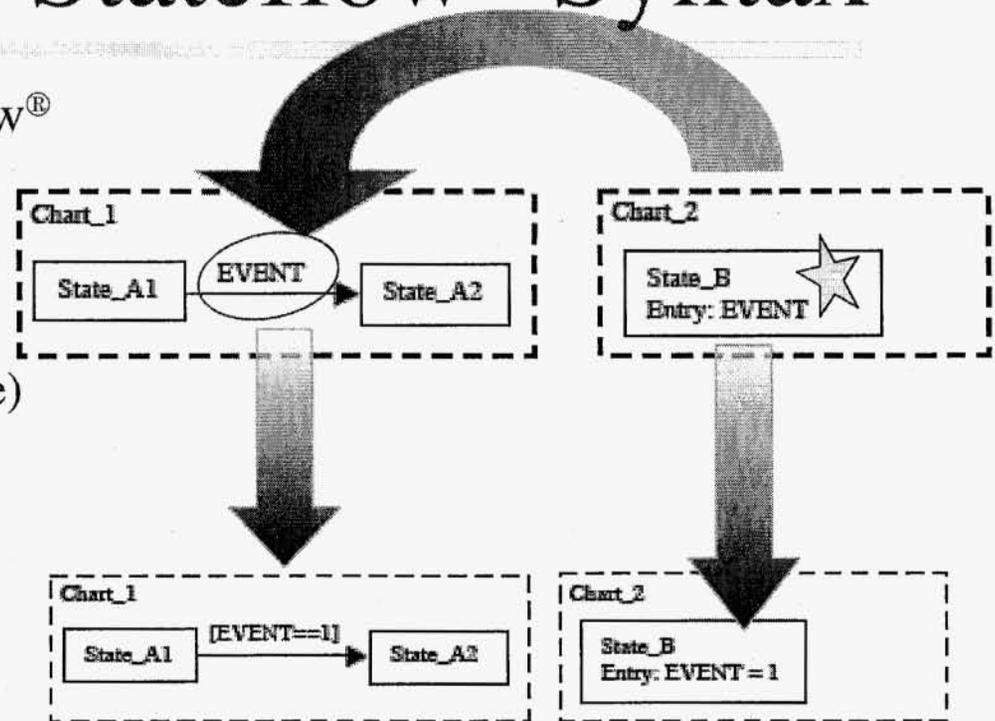
July 2004





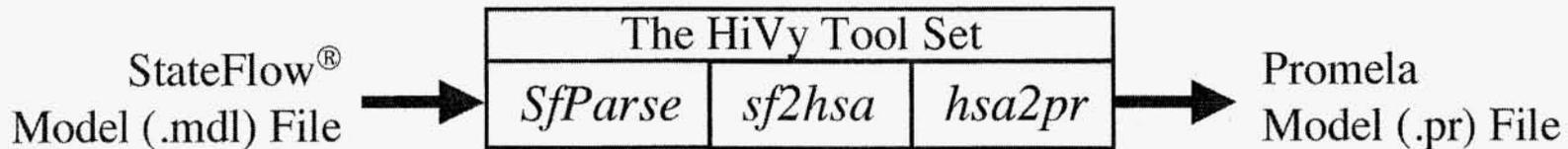
HiVy Supported Stateflow[®] Syntax

- HiVy features a sub-set of Stateflow[®]
- Alternate implementations
 - Inner transitions with same source and destination
 - Implicit event generation (example)
- Supports externally (Stateflow[®]) generated events
 - allows for non-determinism
- Converts events and states into a proposition list for LTL generation
- Additional simple model development strategies to support successful translation include
 - Scoping, embedded state-charts, sub charts & closed system verification





HiVy Tool Set Files



- SFParse (Perl) -- parses Stateflow[®] model files for tokens of interest
- sf2hsa (C): formats parsed data into Hierarchical Sequential Automata (HSA) intermediate format
- hsa Merge (C): allows multiple models to be merged at HSA-level prior to final translation
- hsa2pr (C): translates HSA to Promela
 - Dependent on VDM (Vienna Development Model) compiler
- HiVy mimics MOCES translator that E. Mikk developed for Statemate.

July 2004





HiVy Optimizations

- “Efficient HiVy” -- Gerard Holzmann
 - directly modified HiVy codegen.c module to increase Promela translation efficiency.
- Created Post Processor* procol.pl -- knocked down the state space in POTS model by 6%, and memory savings of 47%

- Procol.pl

Parameter	Original HiVy	HiVy Optimization	Reduction
Real/user time	3.5 seconds	1.5 seconds	57%
Total actual memory use	8.87 Mb	4.67 Mb	47%

- Automated** in Perl
- The basic architecture of the post processor
 - Uses Promela “atomic” and “labels” to make non-deterministic state & transition jumps
 - combined all processes into one “super” proc type
 - Removed unused variable declarations
 - POTS model reduced from 1285 -> 1170 lines of code

* Algorithm developed by John Powell, JPL **Script developed by Don Gibbs, JPL

July 2004



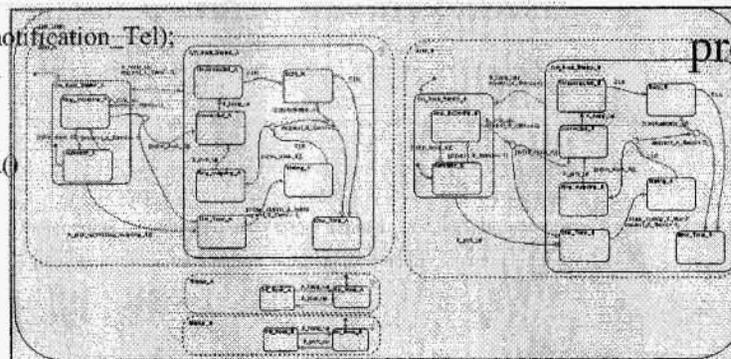


HiVy Example:

A Plain Old Telephone System (POTS)

```
/****** INTEGER VARIABLES *****/
byte request_A_Event;
byte request_B_Event;
/*-----*/
/****** PROPOSITIONS *****/
#include "propositions"
/****** PROCESSES *****/
active proctype function_Top_Level()
{
  loop: atomic{
    WAIT_ACTIVATION(activation_Top_Level) ->
    if
    :: current_state_Top_Level==state_Top_Level_frame ->
    {
      skip;
      RESET_NOTICE(notification_Top_Level);
      ACTIVATE(activation_Top_Level_frame);
      WAIT_NOTICE(notification_Top_Level) ->
    }
    fi;
    INC_NOTICE(notification_Tel);
  }
  goto loop;
}
active proctype function_Status_A()
{
  loop: atomic{
```

- Reach-ability
- Verification (dead-locks)
- Linear Temporal Logic verification
- Lines of code:
 - Stateflow *.mdl file, 2328 LOC
 - HiVy *.pr file, 1285 LOC
 - versus identical hand-model, ~ 180 LOC
- Used this model to develop post processor



July 2004





HiVy: Improvements & Current Availability

- Areas for Improvement
 - State-space issues limit the model size -> Efficiency
 - Inclusion of C code in verifications using HiVy models is not the strength of this tool
 - Increase the Stateflow[®] semantics supported by HiVy
 - Trail file assistance
- Beta version available, but by the end of the fiscal year, the updated version and post processor will be available.

July 2004



End of File

