



\ ' hī - vī \

Automated Translation of Stateflow® Designs for Model Checking Verification

The HiVy Tool Set enables:

- Model checking of finite state machine designs (i.e., state-charts).
- This is achieved by translating state-chart specifications into the input language of the Spin model checker.
- The HiVy tool set transforms output of the commercial tool Stateflow® provided by The Mathworks, Inc.
- HiVy can also be used independently from Stateflow®. An abstract syntax of hierarchical sequential automata (HSA) is provided as an intermediate format for the tool set.

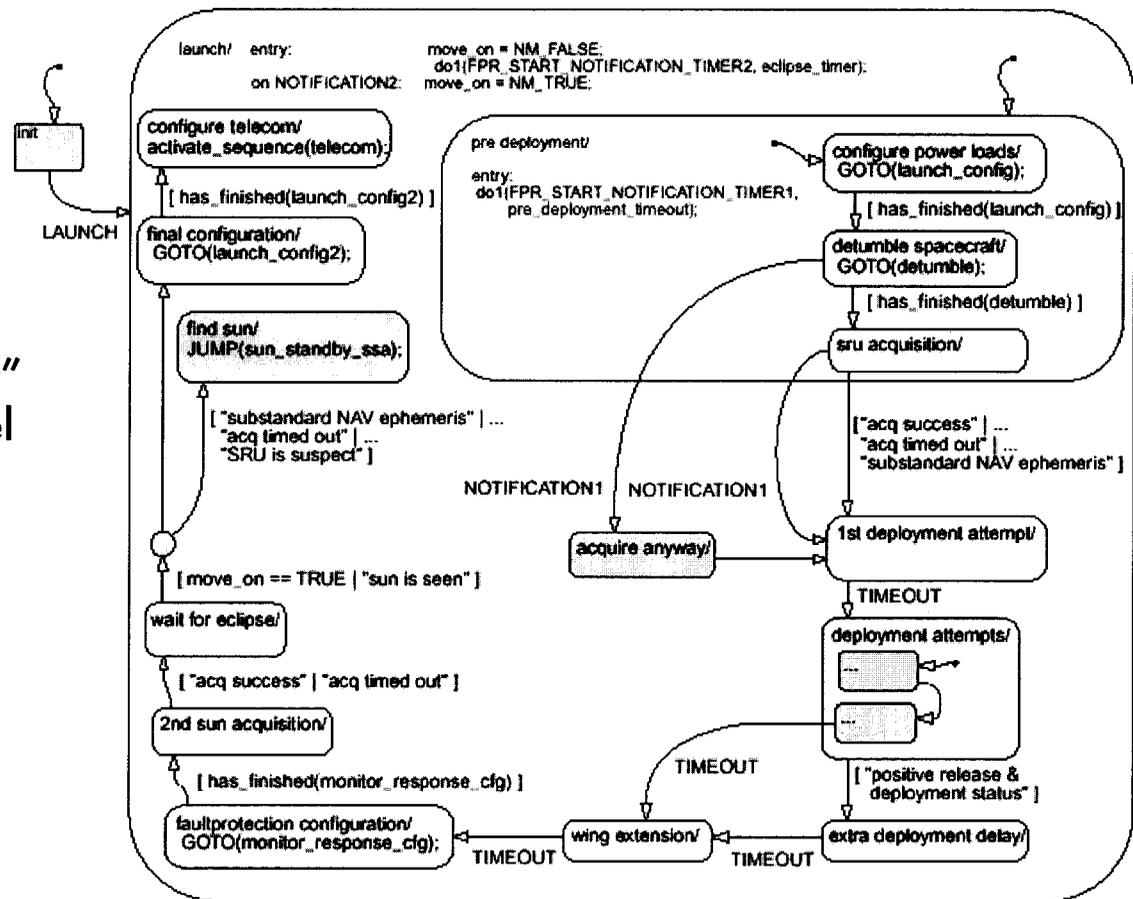
Why HiVy ?

Model-based code generation is used to develop Flight Software for JPL Missions

- DS1 Fault Protection (FP)
- Deep Impact FP

We asked...

1. Can we apply "lightweight" formal methods and model checking to mission flight software verification at JPL?
2. Can we automate the process?
3. Can we quantify the benefits compared to traditional verification approaches?



A section of the launch statechart, showing sun acquisition and pre-deployment of the DS1 solar array panels.

Why Enable the Use of Model Checking ?

NASA and JPL Relevance

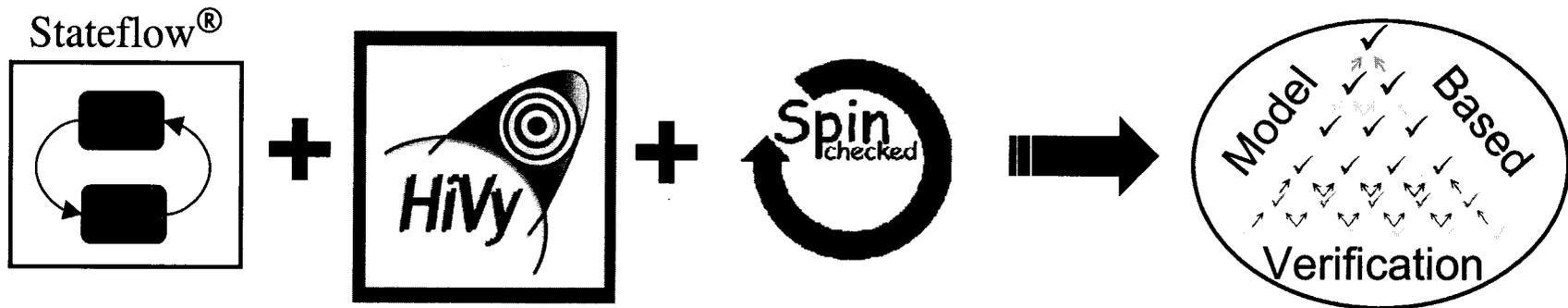
- Increasingly complex and critical aspects of NASA/JPL projects rely on robust software. Advanced software verification methods are needed to meet mission goals.

	Traditional	State-charts	Model Checking
Requirements	<i>Informal</i>	<i>Informal</i>	➔ <i>Formal (LTL)</i>
Design	<i>Informal</i>	<i>Semi-formal</i>	➔ <i>Formal (Promela)</i>
Code	<i>Formal</i>	<i>Formal</i>	

*Notable bonus: Gerard Holzmann, the creator of the Spin model checker, is now at JPL

Industry Applications

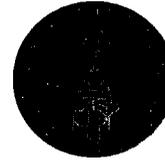
- 1) Aerospace Industry
- 2) Automotive Industry
- 3) Any Industry specifying their designs with Stateflow[®]



Key Benefits

- Enables exhaustive exploration techniques of model checking
- Design verification can occur earlier in the software development cycle
- The state-chart as the design source provides synergy between auto-generated verification model (via HiVy) and auto-generated code (via Stateflow Coder)

Technology Status



- The **HiVy** Tool Set (beta version) is available under CalTech/JPL license agreement
- However, **HiVy** is currently under *optimization* development to reduce the number of processes created in the translation of models
 - To minimize state-space explosion in model checking
 - New optimized version available by October 1, 2003
- **HiVy** Wish List (partners/sponsors sought)
 - Evaluation/incorporation of expanded semantic set
 - XML representation for Stateflow; tool set modification for XML-based parsing of models
 - Customer systems to model check using **HiVy** tool set translation

Publications

- K. Barltrop, P. Pingree, *Model Checking Investigations for Fault Protection System Validation*. 2003 International Conference on Space Mission Challenges for Information Technology, July 2003
- P. Pingree, E. Benowitz, *Experiences in Integrating Auto-Translated State-Chart Designs for Model-Checking*. 2003 Workshop on Model-Checking for Dependable Software-Intensive Systems, June 2003
- P. Pingree, E. Mikk, G. Holzmann, M. Smith, D. Dams, *Validation of Mission Critical Software Design and Implementation Using Model Checking*. The 21st Digital Avionics Systems Conference, October 2002.
- P. Pingree, E. Mikk, *The HiVy Tool Set*. Pending NASA Tech Brief Publication.