Abstract for 1999 Rational Software User Conference

(July 25-29, 1999, Washington State Convention Center, Seattle, WA)

Julia Dunphy, Nicolas Rouquette, Martin Feather and Yu-Wen Tung
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109, USA

Background: we develop spacecraft fault-protection software at NASA/JPL.
Challenges exemplified by our task:

- high-quality systems - need for extensive validation & verification
- multi-disciplinary context – involves experts from diverse areas
- embedded systems - must adapt to external practices, notations, etc.
- development pressures – NASA's mandate of "better, faster, cheaper"

Response:

- Utilize Rational Rose UML models (notably statecharts):
  - generate code and verification from the same model
  - use model as common currency of expression and understanding
  - quickly customize semantics of the models on an as-needed basis
- Utilize Rational Rose extensibility and API:
  - prototype generator components using Rose Extensibility Interface
  - realize the generator as decoupled collection of modules communicating via COM
  - create generator components in programming language of choice
- Architect the generator employing Rose round-trip engineering:
  - model in Rose the data objects and processing objects that comprise generators
  - cost-effectively compose generators as mix-and-match of reusable components
  - maximize validation confidence by sharing code generation and validation generation processing objects and organization
  - hierarchically structure components into collections, grouped as COM libraries
  - GUI to allow drag-and-drop creation and customization of generators

Case study: fault-protection subsystem of a deep-space probe:

Statechart models of spacecraft components under fault-protection control

- Statechart model of fault-protection itself
- Fault-protection code generated from model
- Validation by generating input to model checker (an automated exhaustive analysis technique)
- Status monitoring and reporting code generated from same model