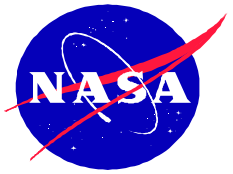


RIACS Workshop on the Verification and Validation of Autonomous and Adaptive Systems

5-7 December 2000

Asilomar

Willem Visser and Charles Pecheur ...

... with a little help from Johan Schumann ...

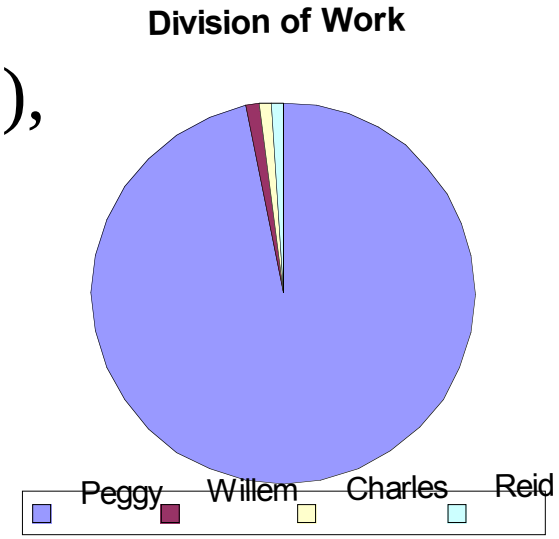
... as deputy for Reid Simmons (CMU)

Workshop…what workshop?

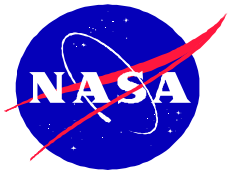
…oh that workshop

Organization

- Technical Content
  - Charles Pecheur (RIACS),
  - Reid Simmons (CMU),
  - Willem Visser (RIACS)
- Administration
  - Peggy Leising (RIACS)



Focus



- Combine
  - V&V Researchers
  - NASA Autonomous and Adaptive Systems
- Purpose
  - V&V people become aware of NASA Systems
  - NASA hear about state-of-the-art V&V
- Intermediate Goal
  - Foster collaborations
- Ultimate Goal
  - Improve reliability of NASA Autonomous and Adaptive systems

Participants
42

- Ames – 16
  - RIACS – 9
- Other NASA – 5
- Universities – 17
  - Europe – 3
- Research Labs – 4
- Focus area
  - V&V – 28
  - A&A – 14

Workshop Structure

- Day 1 (9am – 6pm)
  - Invited Presentations on Autonomous and Adaptive systems
    - Have V&V people hear about cutting edge systems
- Day 2 (9am – 3pm)
  - IS Program Description
  - Technical Break-out sessions
    - Discussing V&V issues
  - Wrap-up

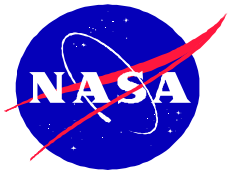
Day 1

- *Nicola Muscettola* – Ames
  - *Deploying Robust Autonomous Systems: Lessons from the Remote Agent Experiment*
- *Rodger Knaus* - Instant Recall, Inc
  - *First Steps Towards Neural Net V&V*
- *Don Soloway* – Ames
  - *Stability Issues with Reconfigurable Flight Control Using Neural Generalized Predictive Control*
- *Peter Engrand* – Kennedy
  - *V&V of an Autonomous Agent for Mars Duty at KSC*
- *David Kortenkamp* – Johnson
  - *Distributive, Adaptive Control of Advanced Life Support Systems*

Day 2

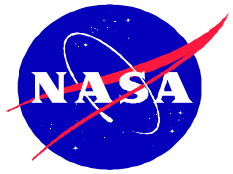
- Breakout Sessions
  - Complex Systems
    - Systems with different interacting parts
  - Adaptive Systems
    - Adaptive control – mostly neural nets
  - Intelligent Systems
    - Containing an AI component – model, rule or knowledge based
- Wrap-up
  - Breakout summaries (—> on-line report)
  - Violent (dis)agreement

Rest of the Talk



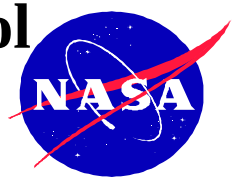
- Short summary of each presentation
- Summary of each breakout session
  - Discussion is encouraged
- Workshop output and future directions

First Steps Toward Neural Net V&V (Rodger Knaus)



- Traditional systems vs. Neural Nets
  - With NN there are no system to verify against specification – specifically true for online NN
- Turner Fairbank Highway Research
  - Example application: Detecting a sleepy driver
  - Some applications executed billions of times, exposing rare errors
- Focused on pre-trained neural nets
- Selecting and Validating an ANN
  - Once trained, how accurate is it?
  - Among candidate ANNs, which is best?

Stability Issues with Reconfigurable Flight Control Using Neural Generalized Predictive Control (Don Soloway)



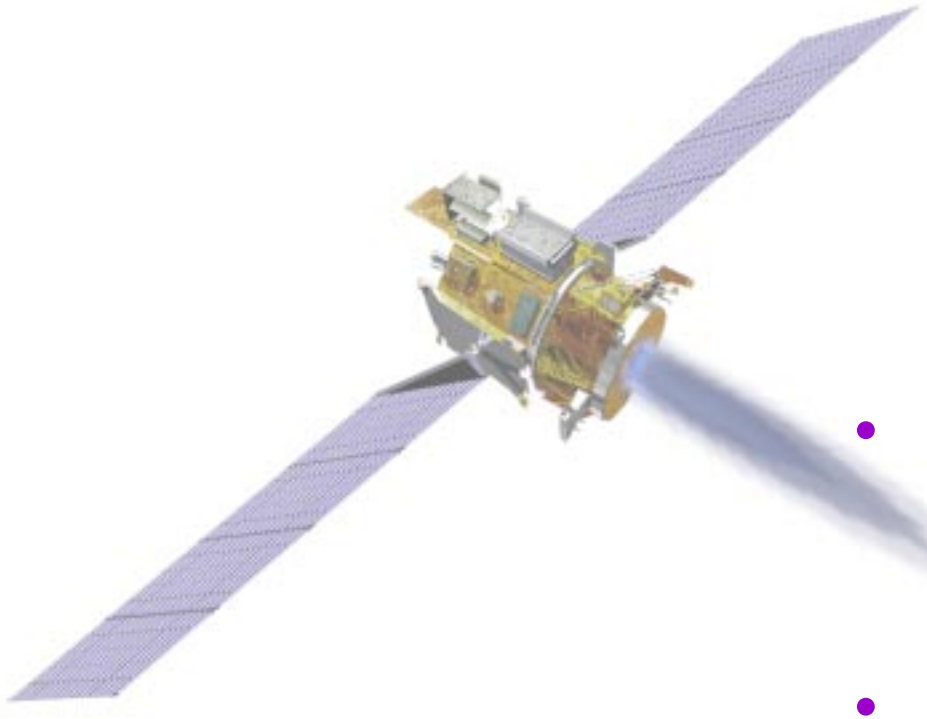
- Objective
  - Reduce Cost and Time
  - Improve Safety
- Generalized Predictive Control
  - Minimization of the Cost Function
- Cost function becomes more complex as more phenomena are observed during wind-tunnel testing that need to be accounted for, e.g.
  - Tracking + actuator damping
  - … + actuator constraints
  - … + frequency weighting
- Flight simulator example

Proofs of Stability are Lacking

"The mathematics for stability of handling increasingly complex control issues lags years behind demonstrated controllers"

- Neural Generalized Predictive Control
  - Neural network replaces model of plant
- Adds another layer of complexity

Deploying Robust Autonomous Systems: Lessons from the Remote Agent Experiment (Nicola Muscettola)



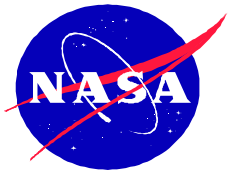
Remote Agent:

autonomous spacecraft controller

- from Ames and JPL
- planner+exec+diagnosis
- model-based

- Flew on DS-1, May 99
  - Lisp in space
    will never happen again
- Flexible time plans

Deploying Robust Autonomous Systems: Lessons from the Remote Agent Experiment (Nicola Muscettola)



- Testing the Remote Agent
  - 7 different testbeds (from UNIX sim to real DS1).
  - Hi-fi testbeds => more accurate but less available.
  - Test nominal cases + simple variations.
- The RAX Flight Experiment
  - Unexpected scenario: RAX performs OK.
  - Deadlock in executive: RAX is restarted.
    Due to a concurrency bug => model checking!
- Conclusions
  - AI software is still traditional software!
  - If engines are reliable, V&V of application = V&V of model.

Model Checking Autonomy Models For a Mars ISPP Facility (Peter Engrand)

In-Situ Propellant Production:

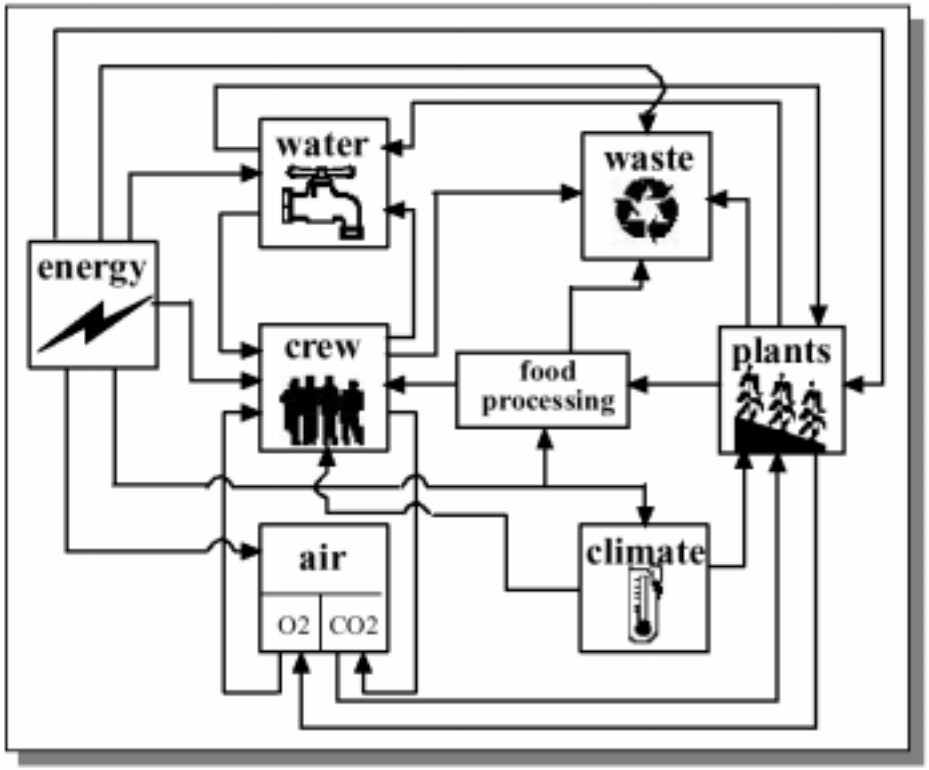
- Produces rocket fuel from Mars atmosphere
- Must work on its own for 500 days
- Prototype at KSC
- Controlled with Livingstone (=> model of ISPP)

=> V&V of the model!

Model Checking Autonomy Models For a Mars ISPP Facility (Peter Engrand, cont'd)

- Model checking of the Livingstone model of ISPP
  - Uses SMV symbolic model checker (CMU)
  - Translator from Livingstone to SMV (Ames & CMU)
  - Pilot study, develop tools and methodologies
  - Done at KSC, no V&V experts (but guidance from Ames)
- Focus on two known model faults
  - Non-trivial two-stage technique for functional dependency
- Conclusions:
  - Exhaustive results even for huge models (10^{55} states)
  - "Writing temporal logic is not for the faint of heart"

Distributed, Adaptive Control of Advanced Life Support Systems (David Kortenkamp)



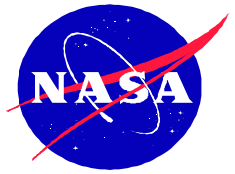
Advanced Life Support:
produce/recycle food, air and water in closed loop
- Complex (bio) processes
- Low margins
- Safety critical

- Experiments at JSC
- 3T control architecture
- Future: Bio-Plex testbed
  - 4 crew, 540 days
  - starts 2004

Distributed, Adaptive Control of Advanced Life Support Systems (David Kortenkamp, cont'd)

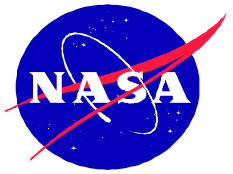
- V&V of ALSS? Very challenging!
  - Detect slow drifts vs. abrupt failures
  - Modelling of biological processes
  - Highly distributed and interconnected system and control
- Stand-alone/interface/integration/operational tests
- Three case studies:
  - ALSS prototype [*Schreckenghost*]
  - Air Revitalization System (3T + Livingstone) [*Malin*]
  - Water Recovery System (waste water!) [*Bonasso*]
- Conclusions:
  - sensitive to small changes => needs adaptive control - learning!
  - huge state and action space, hybrid => needs abstraction

V&V of Complex Systems



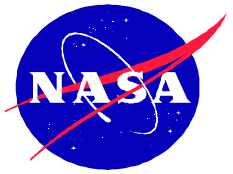
- 16 participants (14 V&V, 2 A&A)
- Defined 3 categories of systems
  - Traditional component-based systems
  - Agents with autonomous behavior
  - Systems with human or biological components
- Discussion was too lively to allow progression past the traditional systems
- Rather focused on general V&V issues

Some General Issues



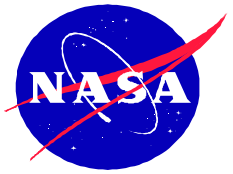
- Address V&V of computing systems not just software systems
  - How do we specify human and biological system behavior?
- System engineering problems are often addressed as software engineering
- Same points were also made in an HDCC case-study session (10-12 January 2001)

V&V Specific Issues



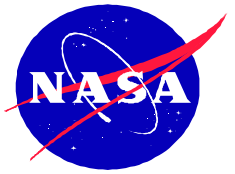
- Formal Specifications are required
- Must have provably correct design before implementation
  - Proof is hard, but it is a price worth paying
  - Focus formal proofs on critical areas
  - Develop domain-specific techniques
- Complex systems must be divided into sub-components that can be verified

Big Debates



- What is the size of system that can be verified by state-of-the-art V&V techniques?
  - Bad question?
  - Different techniques use different measures
- Challenge problems from NASA?

V&V of Adaptive Systems

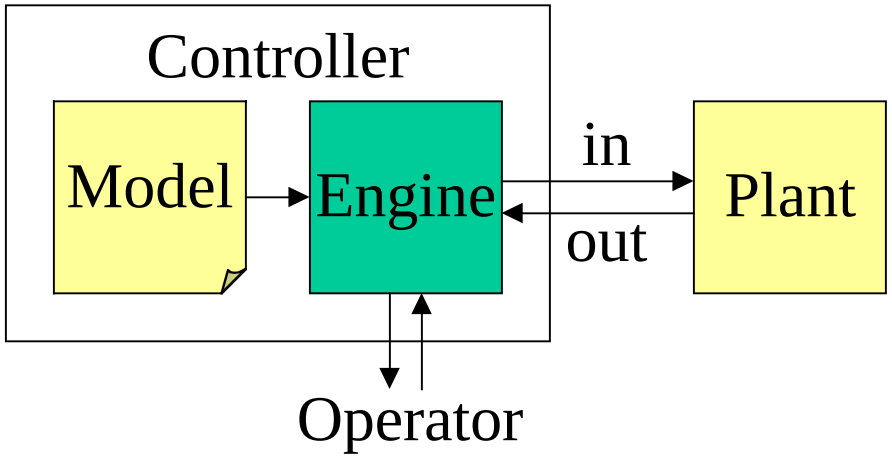


presented by

Johan Schumann

V&V of Intelligent Systems (1)

- Attendance: 13 (NASA: 6)
- Scope: AI
  - model-based, rule-based, knowledge-based, ...
  - Focus on model-based (because MB specialists).
- Model-based control:



V&V of Intelligent Systems (2)

- We need a software engineering process for model-based systems
  - What requirements?
  - Testing theory?
- Decompose the problem
  - (V&V of plant: out of scope)
  - (V&V of engine: hard but one-shot)
  - V&V of model:exploit abstraction!
  - V&V of complete controller

V&V of Intelligent Systems (3)

- Claim: Model-based control is "correct by design"

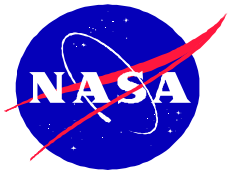
  Models directly capture the specification of the plant
  => controller is correct by construction!

  Yes, but:

  - Good specs => correct model ? (abstraction)
  - correct model => correct control ?
    (soundness and completeness of engine)

  => Still needs V&V of models and of controller

V&V of Intelligent Systems (4)

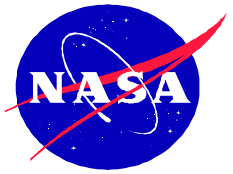


- Multiple models
  - plant (e.g. camera range)
  - constraints (e.g. avoid the Sun)
  - goals (e.g. shortest move)

  Different V&V roles

  Partial models => need reconciliation
- Model-based control theory?
  - Idea: extrapolate a test case to a whole area.
  - Needs formal theory (cf. linear feedback systems).
  - Is this feasible? Highly non-linear systems!

General Issues



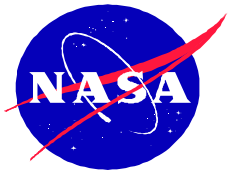
- Start with good S/W engineering principles
- Certification vs. debugging
  = proving correctness vs. finding faults
- Combine several techniques
- Scalability
- Metrics
- Design for V&V (monitoring, fault injection, ...)
- Run-time V&V

Report

- Goal: capture the contents of the discussions in day 2
- Process:
  - Moderators write initial draft
  - Sent to participants for comments
  - Moderators edit draft to incorporate comments
  - Final integration, formatting and web diffusion

http://ase.arc.nasa.gov/vv2000/asilomar-report.html

Outcome



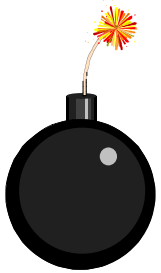
- Many positive opinions about the workshop
- A&A and V&V people know each other a little better
- "Lively" — few broad strategies but lots of good ideas
- Related: HDCC sees V&V of A&A as an important long-term goal

What's Next?

- Model-Based Validation of Intelligence
  - Part of AAAI Spring Symposium Series
  - Stanford, March 26-28, 2001
  - **Lina Khatib** and Charles Pecheur, co-chairs
- New collaborations
- Asilomar 2001?
  - Likely not the same format again
  - Your suggestions are welcome

Perspective

Formal V&V is now able to give real answers about real systems (e.g. Java programs)



Autonomous and adaptive systems are much, much more complex (e.g. adaptivity, biological processes, AI, ...)

There is room for a lot of future research (and workshops)