Adjustable Autonomy Testbed

Jane T. Malin and Debra K. Schreckenghost

The Adjustable Autonomy Testbed (AAT) is a simulation-based testbed located in the Intelligent Systems Laboratory in the Automation, Robotics and Simulation Division at NASA Johnson Space Center. The purpose of the testbed is to support evaluation and validation of prototypes of adjustable autonomous agent software for control and fault management for complex systems. The AAT project has developed prototype adjustable autonomous agent software and human interfaces for cooperative fault management. This software builds on current autonomous agent technology by altering the architecture, components and interfaces for effective teamwork between autonomous systems and human experts. Autonomous agents include a planner, flexible executive, low level control and deductive model-based fault isolation. Adjustable autonomy is intended to increase the flexibility and effectiveness of fault management with an autonomous system. The test domain for this work is control of advanced life support systems for habitats for planetary exploration. The CONFIG hybrid discrete event simulation environment provides flexible and dynamically reconfigurable models of the behavior of components and fluids in the life support systems. Both discrete event and continuous (discrete time) simulation are supported, and flows and pressures are computed globally. This provides fast dynamic simulations of interacting hardware systems in closed loops that can be reconfigured during operations scenarios, producing complex cascading effects of operations and failures. Current object-oriented model libraries support modeling of fluid systems, and models have been developed of physico-chemical and biological subsystems for processing advanced life support gases. In FY01, water recovery system models will be developed.
Adjustable Autonomy Testbed

Jane T. Malin and Debra K. Schreckenghost

Mission Systems 2001
January 31, 2001
Operations Concepts for Life Support

- Autonomous control systems should operate safely without eyes-on, vigilance monitoring
  - Implement safe operations with well-defined protocols at boundary conditions
  - Provide strategies for notifying humans when interesting or unusual events occur or a need for manual action arises
  - Support remote monitoring of systems
  - Generate activity histories and event summaries
- Human support is performed by exception – during critical operations, anomalies, or unusual situations
  - Support novel manual operations in response to anomaly or opportunity
  - Permit human override of automation
  - Operate autonomous system continuously, even when human is in control
- Operations results from LMLSTP Phase III Test (Fall, 97)
  - Engineer workload with automated control system
    - 6-8 hrs per week on console, plus 6 hrs every 4 days for incineration and 3 hours every 20 days for planting/harvesting
  - Tasks with human-in-the-loop: incineration, plant/harvest, calibration
Adjustable Autonomy Testbed

- **Purpose**
  - Develop automated control software that supports human-in-the-loop operations
  - Provide a simulated life support environment to develop and test this control software

- **Approach**
  - Add improved capability for user to monitor and command control processes in 3T
    - Displays that provide an overview of system operations (e.g., ARS) and summarize control activity history
    - Notification of faults and automated actions in response to them
    - Electronic procedures for manual commands
  - Provide new fault detection capability that complements anomaly handling in 3T
    - Integrate with model-based fault diagnosis software from Ames (Livingstone)
Three Tier (3T) Control Architecture

- **Planner (AP):** predicts activities to achieve control objectives
  - Represents and assigns tasks to multiple agents
  - Monitors plan execution, detects plan execution failure, and replans at failure.
- **Sequencer (RAPs):** selects and orders procedures to implement planned activities
  - Chooses procedures reactively, based on current state of environment.
  - Allocates procedure steps to specific skill managers
- **Skill Manager:** implements procedure steps as closed loop control
  - Skills are activated to issue commands to control instrumentation
  - Events are activated to monitor sensor readings in response to control
# 3T Example: Prepare for Incineration

<table>
<thead>
<tr>
<th>PLANNER</th>
<th>SEQUENCER</th>
<th>SKILL MANAGER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accumulate O2 for incineration</strong></td>
<td><strong>Task: Prep for Incineration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Method: prep-started</strong>&lt;br&gt;Context: not prep-for-incineration&lt;br&gt;Actions&lt;br&gt;1. Empty O2 buffer tank&lt;br&gt;2. Stop O2 transfer&lt;br&gt;3. Issue message</td>
<td></td>
<td><strong>Skill: Turn on pump</strong>&lt;br&gt;<strong>Skill: Close O2 isolation valve</strong>&lt;br&gt;<strong>Skill: Turn off pump</strong></td>
</tr>
<tr>
<td><strong>Method: monitor-o2-pressure</strong>&lt;br&gt;Context: prep-for-incineration&lt;br&gt;O2 reservoir not full&lt;br&gt;Actions&lt;br&gt;1. Measure reservoir pressure</td>
<td></td>
<td><strong>Event: measure o2 pressure</strong></td>
</tr>
<tr>
<td><strong>Method: prep-complete</strong>&lt;br&gt;Context: prep-for-incineration&lt;br&gt;O2 reservoir full&lt;br&gt;Actions&lt;br&gt;1. Mark O2 reservoir full&lt;br&gt;2. Issue message</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enhancing 3T for Improved User Interaction

• Monitoring system operation
  – Displays providing an operational overview
  – Histories of control activities and their consequences
  – Notification of faults and automated actions in response to them

• Commanding 3T control system
  – Electronic procedures for manual commands

• Potential for reuse
  – Electronic procedures and displays for new subsystem with creation of new configuration files
  – Remote access to new displays with 3T modification to export raps data
  – Centralized data logs with modification to jForwarder
Monitoring ARS Operation

Operating Mode
- VCCR: half-cycle-1 air_save
- CRS: standby
- OGS: operational

Active Failures
- HX1: unexpectedly-off

Control Action Log
- CRS_TO_OPERATE initiated

Device View
- CO2 inletOffice: 55 psia
- CO2 Accum
Reviewing Histories of Control Activities

**Summary**

- **000:00:37.01** half-cycle-1 accum
- **000:00:00.00** PU01: on to on_flow_blocked
- **000:00:58:48** HANDLE-MIR-FAULTS is complete with status GOAL-SUCCEEDED
- **000:00:18.18** PU01: on_flow_blocked to on_flow_blocked
- **000:00:18.18** PU01: on_flow_blocked to on

**Task Agenda**

<table>
<thead>
<tr>
<th>Time</th>
<th>Active Command</th>
<th>Monitor-VCCR</th>
</tr>
</thead>
<tbody>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>HANDLE-VCCR-ALERTS</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>put-out-warning vccrskm (even low even low even low even low even low)</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>handle-mir-faults #resource: nil</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>turn-pump-p vccrskm blower off 120</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>no-op mir-blower - problem</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>turn-pump-p vccrskm blower on 120</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>RESTORE-CONFIGURATIONS</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>no-op nothing-to-restore</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>CHECK-VCCR-CONFIG</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>configure-vccr hc1 air_save</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>configure-hc-adsorb hc1</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>configure-hc-adsorb-p vccrskm hc1 120</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>turn-heater-p vccrskm hc2 off 120</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>turn-heater-p vccrskm hc1 off 120</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>configure-desorb-state-p vccrskm hc1 air_save 120</td>
</tr>
<tr>
<td>000:08:31:24</td>
<td>SUCCEEDED</td>
<td>GCOLLECT</td>
</tr>
</tbody>
</table>
Commanding the ARS Control System

Select a Procedure

Procedure to start the Air Revitalization System (ARS). The ARS consists of a carbon dioxide removal system (VCCR), a carbon dioxide reduction system (CRS), and an oxygen generation system (OGS). Typically, the ARS

Execute a Procedure

- 4. Set OGS current completed
  - Description
  - Conditions
  - Effects

- 5. CRS to Standby completed
  - Description
  - Conditions
  - Effects

- 6. CRS to Operate failed
  - Description
  - Conditions
  - Effects

Procedure Step
Text Instructions & Annotations
Conditions Prior to Task Execution
Effects of Task Execution
Enhancing 3T with Model-based FDIR

- NASA Ames has developed a model-based state assessment tool called Livingstone
  - System Model
    - Components connected by data paths
    - Each component model includes nominal and fault states with transition conditions
  - Use of this model
    - Assess the most likely state by reasoning about the expected and observed consequences of commands

1. Command heat exchanger on
2. Observe no temperature drop over the device
3. Livingstone concludes heat exchanger UNEXPECTEDLY OFF
Caution and Warning with Livingstone

Mode Diagram for VCCR Blower Pump

Table of VCCR Livingstone Modes
AAT Demonstration: Architecture
Operation of Air Revitalization System (ARS)
Operation of the VCCR

VCCR normally operates autonomously

- Human operations
  - Startup and shutdown system
  - Inform system of HX state
- Livingstone identifies nominal and failure states
Demonstration Scenario

• Nominal Case: Startup the 3 systems of the air system
  – VCCR: removes CO2 and stores it in a tank
  – CRS: converts CO2 and H2 to H2O and methane
  – OGS: convert H2O to O2 and H2

• Failure Cases: Air blower or heat exchanger turn off unexpectedly
  – Livingstone detects the failure based on temperatures from skill manager and notifies the sequencer
  – Sequencer selects and executes recovery procedures in response to the failure notification
    • Blower: sequencer automatically turns the blower back on
    • Heat Exchanger: sequencer asks human to turn the heat exchanger back on
  – Skill manager issues procedure commands to the sim and receives data from sim indicating commands have taken effect
  – Livingstone notifies sequencer when the fault has been corrected and nominal control resumes
  – Throughout, human can monitor the activity as it occurs or after the fact