Reliability, Safety and Error Recovery for Advanced Control Software

Jane T. Malin
Automation, Robotics and Simulation Division, NASA Johnson Space Center

Abstract: For long-duration automated operation of regenerative life support systems in space environments, there is a need for advanced integration and control systems that are significantly more reliable and safe, and that support error recovery and minimization of operational failures. This presentation outlines some challenges of hazardous space environments and complex system interactions that can lead to system accidents. It discusses approaches to hazard analysis and error recovery for control software and challenges of supporting effective intervention by safety software and the crew.

Reliability, Safety and Error Recovery for Advanced Control Software

Jane T. Malin
Automation, Robotics and Simulation Division,
NASA Johnson Space Center
8/26/03

Workshop: Advanced System Integration and Control for Life Support

1

Overview

- Definitions
- Challenges of hazardous environment and new technology
- Hazard analysis for complex systems
- Hazard reduction for control software
- Future safety-conscious systems

2

Definitions

- Advanced Integration and Control: broadly includes control, procedures, schedules, safety, coordination, communication, and anomaly response
- Performance: throughput, latency, efficiency
- Functionality: level of service
- Reliability and safety: handling of failures, faults and errors
  - Controlled system, control platform, human operators
- Vulnerabilities/hazards: unacceptable system weaknesses or states that can contribute to a loss
- Safeguards: methods to prevent or eliminate vulnerabilities or hazards and reduce risk (likelihood x severity)

3

Challenges of Hazardous Environment, Maturing Technology, and Closed Recycling Systems

- Incorrect specifications and assumptions are inevitable for new technology in harsh conditions
  - Unexpected system states
  - Operators and software will need to solve problems and adapt to unavoidable unanticipated situations
- Complexity and interaction in tight coupling
  - Dynamic interactions in closed set of recycling systems with minimal buffers

4

System Accidents

- Interactive systems, tight coupling, complexity
  - Difficulty in analysis leading to unanticipated situations that are difficult to understand when they happen
  - Combinations and synergistic effects: common causes, canceling failures, side effects, command combinations and timing
  - Interactions in dynamic complex trajectories or histories: distant effects, compensating mechanisms
- Surprise due to mismatch between operations and system state
  - Missing information: concealed, ignored/missed
  - Wrong information: misleading, misinterpreted
- Damaging omissions or errors in control, operations or safety response
  - Failure to respond appropriately – not available or misapplied

5

Vulnerabilities of Control Software

- Incompleteness in software requirements
  - Incomplete or wrong assumptions about operation of controlled system or supporting computer systems
  - Omitted or ambiguous handling of controlled-system states and environmental conditions, including violated assumptions and overload
- Software-related hazards
  - Failing to perform required function
  - Performing function inappropriately
  - Failing to coordinate functions (wrong time, wrong order)
  - Failing to respond appropriately to hazardous condition (not recognized, wrong response)

6

Hazard Analysis for Complex Systems

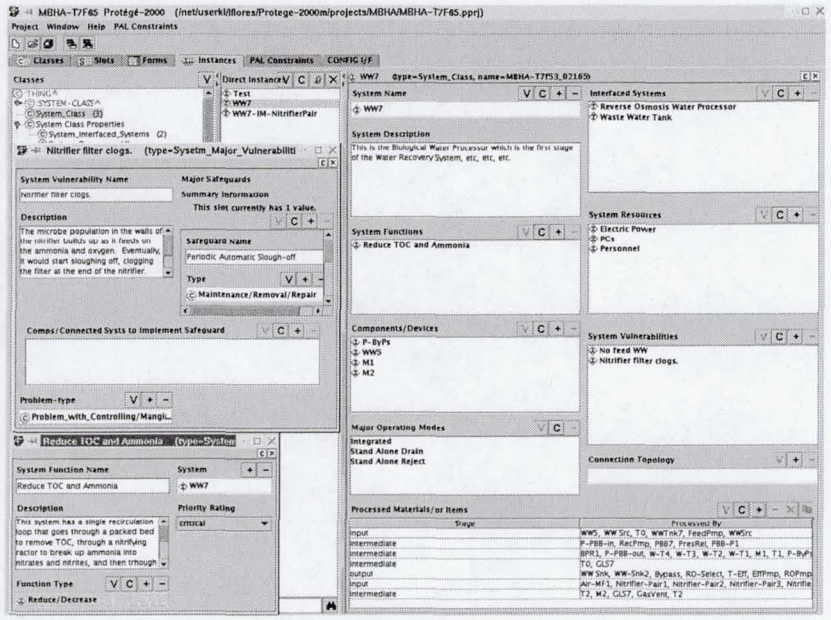
- Model-based hazard analysis project
- Hazard identification tool
- Simulation to evaluate design and operations
- Specifying vulnerabilities and safeguards

7

Model-based Hazard Analysis for Complex Systems

- Address the problem of safety due to system complexity that leads to incomplete requirements
  - Model-Based Hazard Analysis for Interacting Systems - Engineering for Complex Systems Program (J. Malin/PI)
- Guide the engineer in evaluating system designs and identifying hazards and hazard scenarios
- Model, analyze and simulate unanticipated hazards and interactions in system operations
  - Effects of faults, errors and failures to act when expected
- Focus analysis and simulation strategy to find unanticipated system accident scenarios

8

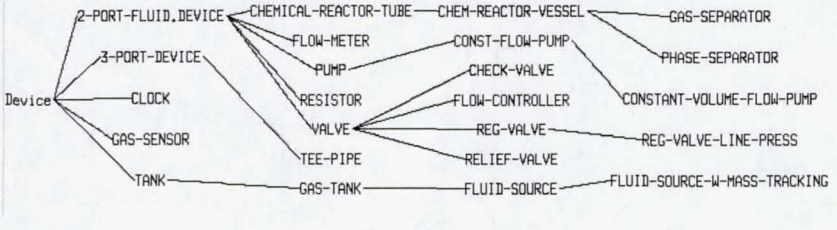


Hazard Identification Tool: Specifying Water System Vulnerabilities and Safeguards 9

Hazards in Generic Component Library

CONFIG hybrid device models for early design, with selectable failure behavior for problem types in system accidents

- Focus is on thermohydraulic processing and management of fluids
  - Water Recovery, Air Revitalization, ISRU and Thermal Control cases
- Capabilities for simulating combined, cascading and global effects of local problems



10

Selectable Failure Behavior

- Styles of modeling failures and degradation
  - Discrete changes triggered by failures and problem inputs
    - Immediate or delayed changes to state, behavior mode or control regime
  - Continuous degradation triggered by failures and problem inputs
  - Nontemporal algebraic relations
    - Performance level affected by conditions
    - Failures to operate or change upon input: stuck flags
    - Random variation in measurement or input
- Degrading and regenerating processing performance
- Reactors and separators with multi-component mixtures
  - Add and remove contaminants in rapid fluid composition changes
  - Migrate products, gas or liquid to wrong outflow
  - Imbalance process with feed or flow reversal problems
- Resource providers with alternative methods for reacting to excessive demands from multiple loads
- Leaks as specifiable additions to simulation scenarios

11

Safeguard specification

- System design protects against vulnerabilities
  - Unacceptable system weaknesses or hazardous states
  - Identify and classify conditions or causes (input) and problem effects (output)
- Safeguards prevent, reduce or mitigate hazards
  - Phase when applied
    - Prevent conditions, prevent evolution to failure state, prevent impacts or damage
    - Respond to failure state, respond to impacts
  - Method
    - Isolation and barriers
    - Detection, analysis and control
    - Robustness: buffers/margins, redundancy/multiples, limited impact (e.g., fail operational)
    - Repair, renewal or maintenance

12

Automated Data Collection and Routine Review for Safeguards

System Safeguard Knowledge:

Safeguard Name: Divert to feed tank

Types: Buffer, control

. . .

Agent: software automation [or hardware or human operator]

Verification

type: inspection

schedule: automated tank level sampling every 5 seconds

date/time last verified: runtime value

Measure of success: level goes below alarm level within 2 hours

Reporting requirements: add record of occurrences to daily performance summaries

13

Hazard Reduction for Control Software

- Types of hazard reduction for control software
- Safety executive for error control
- Error recovery methods for control software
- Support for human analysis and intervention

14

Hazard Reduction for Control Software

- Hazard reduction: make control software failure less likely
  - Barriers: lockouts, lockins, interlocks
  - Detection and control: make system, control software and supporting computer systems easier to control and monitor
  - Robustness: redundancy, safety margins and error recovery

15

Safety Executive for Error Control

- Safety kernel or safety executive to centralize and encapsulate safety mechanisms
- Detection of unsafe conditions by external application modules
  - Safety assertions, safeguard reports and watchdog processes
- Responsibility for enforcing safety policy and deciding safeguard mechanism for handling problem

16

Error Recovery for Advanced Control

- Robustness
  - Robustness and redundancy in data and computation
  - Limited partial shutdowns and reconfigurations
  - Backward recovery (robustness roll back): detect error, return to good state (checkpoint) and proceed with alternative version
- Forward recovery (repair): detect and correct erroneous state and consequences
  - Intervention and resumption need careful checking
    - Possibility of incorrect assumptions in requirements

17

Support for Human Analysis and Intervention

- Help operators gain situational awareness (orienting for intervention)
- Help operators manage varying degrees of autonomy
- Help operators interact with control agent and safety executive for intervention
  - Understand policy and choose recovery mechanisms
  - Complete and negotiate abstract or sketched "command"
    - Change monitoring, control, or constraints and priorities for plans and procedures
  - Evaluate recovery plans and procedures and associated control software changes and commands

18

Future Safety Conscious Systems

- Barriers and robustness to problems
- Coordination with safety executive and intervening human operators
  - Detection with safety assertions, safeguard reports and watchdog processes
  - Control with embedded knowledge of vulnerabilities and safeguards
- Response plan evaluation with simulation before resuming interrupted operations
  - Simulation scenarios with embedded potential failures

19

To Learn More

- Leveson, N. 1995. *Safeware: System Safety and Computers*. Addison-Wesley, 1995.
- Perrow, C. 1984. *Normal Accidents: Living with High Risk Technology*. Basic Books, 1984.
- Malin J. T., Fleming, L. D. and Throop, D. R. Predicting system accidents with model analysis during hybrid simulation. *Advanced Simulation Technology Conference*, 2002.
- Malin J. T., Fleming, L. D., Flores, L. and Throop, D. R. Using CONFIG for simulation of operation of water recovery subsystems for advanced control software evaluation. *International Conference on Environmental Systems* (ICES), 2002, ICES-114.

20