VIRTUAL IRON BIRD

ENGINEERING FOR COMPLEX SYSTEMS

CHALLENGES

- Visualizing and communicating complex systems
- Corporate knowledge loss
- Effective what-if analysis tools

OBJECTIVES

Knowledge-integrating virtual vehicles & process models integrate key information from many sources, helping users to develop a 'big picture' understanding of design and operational tradeoffs.

Develop a component architecture/toolkit for building knowledge- integrating virtual vehicles; Develop and demonstrate components in use by enterprise customers:

- behavioral trade tool for the ISS vehicle system engineers, linked to backing docs and telemetry
- risk-advised maintenance process for orbiter processing
- process and tool suite for migrating legacy CAD and developing as-built models
- collaborate with industry and evaluate future options, such as simulation-based procurement

CUSTOMERS & COLLABORATORS

Currently customers and collaborators are:

- Shuttle Program
- ISS Vehicle Integrated Performance, Environments and Resources Team
- JSC EVA Program Office

CODE T CONSIDERATIONS

Applicability - 100%

- VIB Technologies address the same types of subsystems and components that will be used in Code T missions

Optimization Opportunity - 25%

- Shift the VIB test case on Space Shuttle to Moon or Mars Design Concept Models. Use Space Station test cases as pilot evaluations at the subsystem level for Code T Missions

IMPACTS

The systems supporting manned spaceflight are among the most complex engineered systems ever created. As a result, communication and coordinated decision-making are critical problems for NASA and its contractors, and the overall technology ensemble for all large engineering organizations.

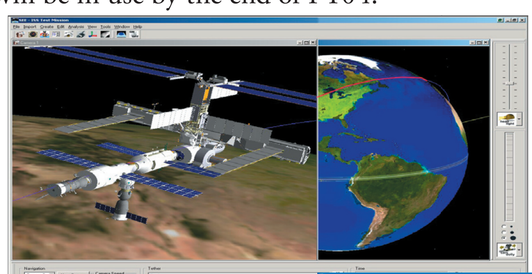
The ECS Virtual Iron Bird project will improve NASA's ability to make coordinated engineering decisions by developing ways to integrate engineering knowledge with fast-time simulations for decision-makers at many levels in the organization.

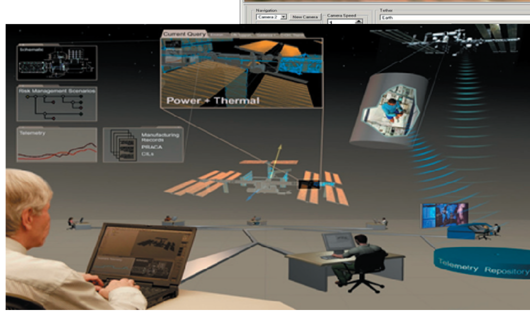
TECHNOLOGIES USED

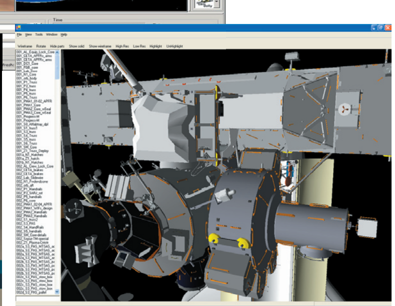
A Virtual Iron Bird (VIB) is a computer-based model of vehicle structure (where are the parts and how are they connected?), function (what roles do they play?), component behavior (how do outputs relate to inputs? how do they fail), and operational procedures (what is the validated action sequence for doing X?). The VIB project complements and extends the Lifecycle Data Management (LDM) Systems currently being installed at NASA centers. These important systems are information libraries. The VIB project is working to turn them into tools for better thinking through these steps:

- Provide a formal semantic foundation for integrating models across the organization
- Prototype by building models to show integration across significant shuttle and station datasets
- Demonstrate utility by partnering with the Shuttle and Station programs to build and use applications with these integrated datasets, effectively leveraging these programs as test beds for new engineering tools and processes
- Lock in advances by partnering with industry and influencing NASA procurement policy

Some VIB components are already in use. Laser scanning technology for creating as-built geometry models of the orbiters was used to support the CAIB reconstruction of the Columbia debris by registering critical RCC panels and TPS tiles against orbiter geometry. An ISS geometry and environment simulation tool is in daily use by the ISS VIPER team to perform rapid, what-if analysis; three additional components will be in use by the end of FY04.







INVESTIGATION ORGANIZER

ENGINEERING FOR COMPLEX SYSTEMS

CHALLENGES

Current NASA investigations of mishaps and anomalies struggle to deal with:

- geographically distributed investigation teams
- diverse, extensive information that must be organized, analyzed, and shared
- no standard and efficient methods or tools for information storage, management, dissemination or analysis
- lack of formally trained team members for mishap investigation
- lack of learning from past anomalies and mishaps by broader NASA constituents

OBJECTIVES

- Enable systematic investigation processes through improved storage and structuring of information gathered and analyzed by distributed teams
- Help optimize investigation directions and tasks by tracking the investigation state through system framework and causal models

CUSTOMERS & COLLABORATORS

Columbia Accident Investigation Board

CONTOUR Mishap Board

HELIOS Mishap Board

IMT tools will be broadly applicable to the full spectrum of Agency customers, and to customers external to the Agency; particular focus to NASA Engineering Safety Center. DoD and NTSB have expressed interest in the tool. Xerox is currently commercializing this tool.

CODE T CONSIDERATIONS

Applicability - 100%

- IO Technologies address the same types of subsystems and components that will be used in Code T missions

Optimization Opportunity - 15%

- Conduct mock mishaps for moon/mars missions to test IO tool capabilities

IMPACTS

Through the fusion of accident investigation methodology with collaborative, information sharing technology, the Investigation Organizer tool enables key elements of successful investigation:

- gathering and sharing disparate types of information
- identifying the relationships between pieces of information
- understanding the significance of such relationships
- preserving the evidential chain
- providing a systematic workflow to improve investigation integrity & efficiency

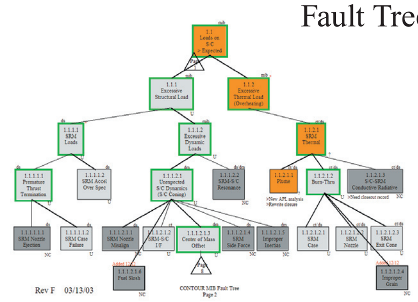
With investigations like SwissAir 111 consuming 4.5 years and $40 million dollars and future investigation likely to increase in size and complexity, tools that can improve the effectiveness and efficiency of investigators and investigative teams are not only desirable but vital.

TECHNOLOGIES USED

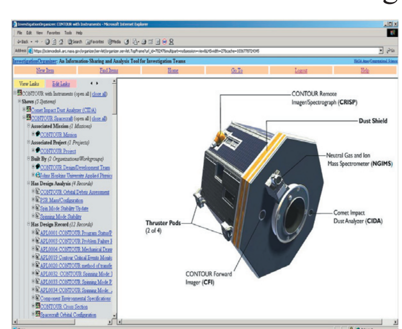
The tool enables the first element through a web-based application that can be accessed by distributed teams to store and retrieve any type of digital investigation material in a secure environment. The second is accomplished by making the relationships between information sources explicit through the use of a semantic web—a structure that literally allows an investigator or team to "connect -the-dots." The third element, the significance of the correlated information, is established through causality and consistency tests using a number of different methods embedded within the tool, including fault trees, event sequences, and other accident models. And finally, the evidence gathered and structured within the tool can be directly, electronically archived to preserve the evidence and investigative reasoning.

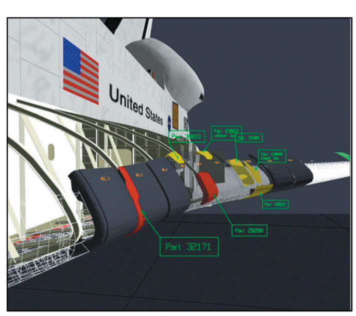
This initial architecture provides the foundation to develop intelligent software agents that can assist in the investigation process by testing hypotheses, suggesting optimum courses of investigation and other decision support activities.

Fault Tree



Information gathering and structuring





Columbia wing digital reconstruction

RISK TOOL SUITE FOR ADVANCED DESIGN

Engineering for Complex Systems

CHALLENGES

NASA needs effective and efficient evaluation of full breadth of risks for a complex program, project, or technology effort that explicitly includes improved risk insight for management and technical decision-making. Challenges include:

- capturing risk assumptions, mitigations, results generated during the design, development and deployment of a complex system
- development of a sufficiently agile system design and trade capability for its wide array of mission types, applications and time scales
- comparison of highly disparate architectural and technology options
- Expanding emerging collaborative model-based design and decision structures to include the full breadth of associated risks
- Continued development and deployment of discrete system analysis capability supporting technology investments in Code T/MSM

OBJECTIVES

This product has two primary goals:

- capabilities to allow more effective evaluation of program and project technology risks and risk trade-off with performance, cost and schedule
- enable effective integration of risk measures into design, build, and operate decision-making

CODE T CONSIDERATIONS

Applicability - 100%

- RTSAD Technologies address the same types of subsystems and components that will be used in Code T missions

Optimization Opportunity - 40%

- Continue to focus at JPL on robotic exploration missions in Product Design Center; Refocus test case studies at GSFC to Lunar Missions in the IMDC; Reprogram ECS funds to JSC to accelerate test case studies on Human Mars Missions for RTSAD tool development

IMPACTS

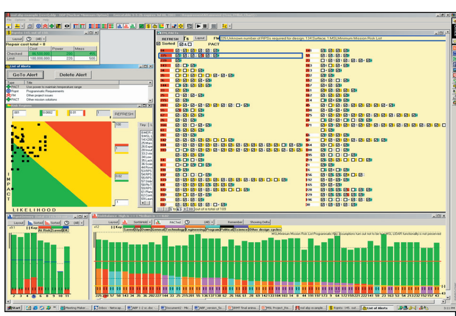
The Risk Tool Suite for Advanced Design (RTSAD) product will:

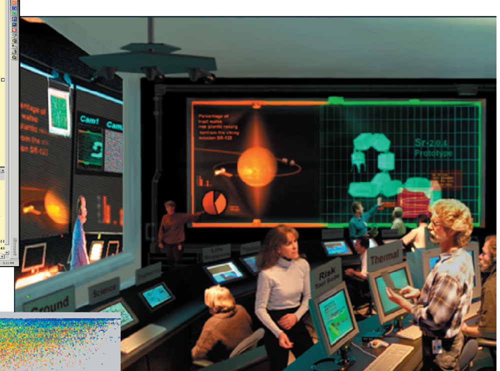
- Develop the capability to fully characterize and visualize risks early and consistently for NASA missions
- Provide a broad design space that includes a variety of risk types including programmatic, technology, human/organization, and software and hardware technical risk.
- Focus on risk measures for the early phases of the NASA project lifecycle, but ensure scalability to the implementation and later project phases
- Use risk to explore various project trade spaces and as a criteria for design selection and optimization
- Provide risk-based design capabilities that are sufficiently agile and responsive to be useful in the assessment of early designs in rapid design environments
- Support risk decision-making in collaborative design environments for complex spacecraft systems.

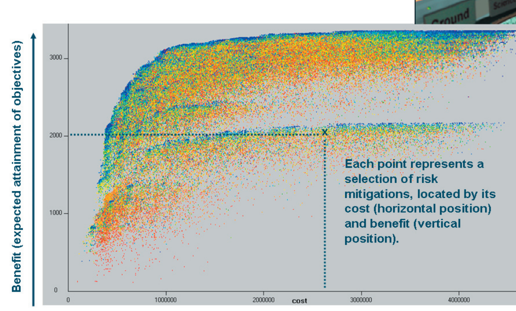
TECHNOLOGIES USED

RTSAD will develop and provide access to a number of components (tools, processes and data sources). These components are of three types: Data Gathering (Access to various databases of historical risks, mishaps, failure reports, etc. is provided, along with intelligent search capabilities), Model Building (Fault Trees, Performance Models, PRAs, cost/benefit models, constraints, etc.), Model Exploration (Optimization, sensitivity, simulation, what-if scenarios, etc.). These components will be available in an integrated fashion in a collaborative environment for decision-making support for technologists, managers and engineers, tested with real projects and other space flight missions and technologies.

By applying risk management as an active element throughout the NASA product life-cycle, rather than an exercise on a point design, higher quality (and potentially more cost-effective) products and programs can be achieved.







ORGANIZATIONAL RISK TECHNOLOGIES

ENGINEERING FOR COMPLEX SYSTEMS

CHALLENGES

Organizational Risk Technologies (ORT) is designed to help NASA understand and reduce its agency-wide mission risks. ORT will address and improve poor understanding of system, human and organizational risk. Its tools and technologies will address how knowledge is managed, and methods on how human teams and organizations should operate to mitigate risk.

OBJECTIVES

Three major ORT efforts will evolve to:

- perform analysis and design of enterprise architecture to support mission design
- assess risk perception and management by teams and organizations in a real-time mission operations context at Johnson Space Center (JSC)
- study human judgment and decision making processes in risk based decision making in conceptual design of complex engineering systems at JPL
- integrate with Risk Tool Suite for Advanced Design

CUSTOMERS & COLLABORATORS

ORT current customers include

- JPL Product Design Center TeamX
- JSC Mission Operations Directorate

Major collaborators include, CMU, Stanford Univ, UIUC, Washington State Univ, UCI, Naval Postgraduate School and Arizona State Univ.

CODE T CONSIDERATIONS

Applicability - 100%

- ORT Technologies address the same types of human & organizational entities that will be used in Code T missions

Optimization Opportunity - 5%

- Continue to use JSC/MOD/Station operations as a test case for Code T Ops; Continue to use JPL/PDC as a test case tool for robotic designs. Use Code T formulation as another test case for ORT

IMPACTS

Organizational Risk Models have been developed to characterize team and organizational activity, decisions, and risk management from conceptual and detailed design through operations and maintenance. At least one model will be computational and used for simulation experiments. It is the goal that all these models will converge to a common representation in the development of Organizational Risk Technologies.

TECHNOLOGIES USED

ECS started the development of ORT in late 2001 and schedules to deliver this product before the end of 2007. This 6-year effort will bring the NASA Technical Readiness Level (TRL) in this area up from 1 to 4.

The technical approach includes two main aspects. First, establising an Organizational Risk Model by:

- collecting data to identify Organizational risk issues with customer studies
- developing Organizational Risk Model using computational model of Organizational performance and how it affects mission risk with validation from customer/expert panel concurrence and prediction
- developing conceptual framework based on the analysis of existing research literature on risk perception and management, organizational culture and structure, cognition, and performance in teams and organizations.

The second aspect is to develop Organizational risk assessment for design and Organizational risk tools for operations by

- obtaining customer requirements and needs
- developing Organizational risk tools and technologies with evaluation and technology assessment.

RESILIENT SYSTEM TECHNOLOGIES

Engineering for Complex Systems

CHALLENGES

Resilient Systems and Technology (RST) is a product that ECS is developing to help NASA develop and test the feasibility of resiliency technologies for human rated systems. ECS will accomplish this goal by addressing inadequate state assessment and brittle control strategies. The development of RST will also help NASA motivate and enhance student education through demonstrations & applications of ECS unique technologies & research.

OBJECTIVES

The ultimate goal of the RST product is to produce resilient vehicle systems capable to carry out a system-level self-assessment and perform real-time adaptive control based on hazards encountered. The intelligent vehicle envisioned will be capable of planning and executing its mission, managing its health and scheduling its own repairs. Development and implementation of safe communications/interactions of the system with humans (on board or on the ground) is critical to the success of intelligent systems and operations.

CUSTOMERS & COLLABORATORS

- Codes M and R
- Space Station
- Boeing
- US Air Force

CODE T CONSIDERATIONS

Applicability - 75%

- RST core technologies are developing intelligent, autonomous, and reconfigurable systems that are applicable to Code T Missions

Optimization Opportunity - 50%

- Discontinue aircraft related reconfigurable system test cases and refocus efforts on spacecraft systems in particular command & control and power & propulsion systems; Continue to develop Personal Satellite Assistant technology to support human operations on Mars Spacecraft Missions

IMPACTS

RST supports technologies required to design, build, test, operate and maintain future resilient systems. It develops integrated autonomous operations and low-level adaptive flight control technologies to direct actions that enhance the safety and success of complex missions despite component failures, degraded performance, operator errors, and environment uncertainty. Inherent in this endeavor is monitoring, management, and ultimately control, integrating high-level reasoning and autonomous capabilities with multiple subsystem controllers. RST has three sub-products:

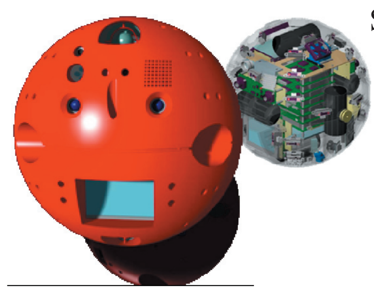
- Spacecraft Mobile Monitor (SMM), maturing mobile robotic environmental monitoring systems that interact with both humans and avionics software to improve environmental fault detection, isolation, & recovery as well as enhancing the crew's productivity via mobile IT capabilities
- Autonomous Propulsion System Technologies (APST) develops advanced engine control and diagnostic software to maximize engine performance to meet mission needs
- Adaptive Flight Control Integration (AFCI) integrates and assesses neural net flight controllers for aircraft avionics resiliency capabilities
- Intelligent Vehicle Health Management (IVHM) for X34/X37

TECHNOLOGIES USED

RST will:

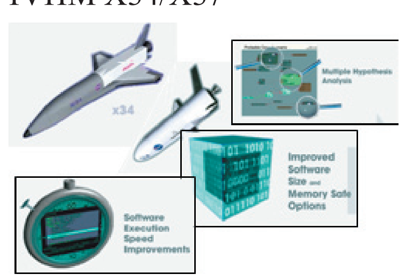
- develop adaptive operations and control strategies
- provide system intelligence to enable reconfiguration or adaptation in response to unanticipated events
- develop intelligent diagnostic technology to allow reliable, accurate, and autonomous assessments of system state
- develop testbeds to verify/validate the integrated software/physical system packages.

SMM



APST

IVHM X34/X37



AFCI

SOFTWARE DEPENDABILITY METRICS & TOOLS

ENGINEERING FOR COMPLEX SYSTEMS

CHALLENGES

Software Dependability Metrics and Tools (SDMT) is an ECS product to help NASA understand and reduce its agency-wide mission risks in the area of software. SDMT will accomplish this goal by developing software engineering tools and methods to reduce the risk of software in complex systems, and the improvement of the quality of software engineering processes, such as, requirements, reuse, and V&V.

OBJECTIVES

- develop the techniques that use well-defined, comprehensible and analyzable specifications of system components and software requirements to manage risks introduced by technical communication gaps among life-cycle phases, organizations, and subsystem elements
- use NASA relevant test-beds to evaluate impact of software engineering tools and techniques on software quality and dependability
- integrate with Risk Tool Suite for Advanced Design

CUSTOMERS & COLLABORATORS

- Testbed: Mars Data System: JPL, Code S, Mars Smart Lander
- Testbed: Real Time Java for C3
- Carnegie Mellon Univ, MIT, Univ of Southern California, Univ of Maryland, Univ of Washington, and Sun Microsystems

CODE T CONSIDERATIONS

Applicability - 100%

- SDMT Software Research and tools address the same types of avionics and ground systems that will be used in Code T missions

Optimization Opportunity - 20%

- Continue to use Mars Data System as a test case for Code T software requirementa; Collaborate with Code T researchers on modular systems software requirements as an additional test case for SDMT

IMPACTS

SDMT has two sub-products, High Dependability Computing Project (HDCP) and Intelligent Software Engineering Tool Suite (ISET).

The primary goals are:

- Identify dependability attributes of software artifacts, engineering practices, and operational environments, along with measures for their causal relationships between technical decisions and dependability outcomes
- Create notations supporting description of software artifacts and dependability
- Define and prove engineering techniques, tools, design principles, practices and processes to support affordable creation of dependable systems
- Disseminate the processes and practices in educational software programs

Additionally, ISET develops software engineering tools and methods to reduce the uncertainty of software, emphasizing model-based techniques that use well-defined, comprehensible and analyzable specifications of system components and requirements to manage the risks introduced by technical communication gaps among life-cycle phases, organizations, and the subsystem elements.

TECHNOLOGIES USED

SDMT will utilize and develop a variety of technologies:

- appropriate hardware, avionics code, project data and environment simulators to enable high fidelity simulations and tests for a system infrastructure that enables mission managers and remote research collaborators to jointly run and assess testbed simulations
- testbeds with appropriate software and hardware tools to empirically evaluate dependability performance
- research results and empirical data structured to support the formulation of national standards for pre-cursors and metrics for software reliability

Empirical validation of models for measuring and predicting computing system dependability and demonstrated risk-mitigation tools, will include:

- metrics and attributes must be applicable to computing systems of size and complexity relevant to NASA
- models must be able to guide application of dependability improving techniques and lead to a measurable improvement in dependability
- tools must provide cost-effective mitigation or management of mission-critical software risk factors across software lifecycle
- tool methodologies must integrate with existing mission development processes
- prototype libraries developed for software risk mitigation strategies to be used by the Prototype Model-Based System Analysis Tool Suite