

# 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, verification and validation.

## 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 Command & Control Systems
- Carnegie Mellon University, MIT, University of Southern California, University of Maryland, University of Washington, and Sun Microsystems

## CONTACT INFORMATION

Dr. John Penix  
john.j.penix@nasa.gov  
650.604.6576

## IMPACTS

SDMT has two sub-products, High Dependability Computing Project (HDCCP) 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

