NASA/TM–2010–214800

Automated Tool and Method for System Safety Analysis:

2009 Progress Report

Jane T. Malin, Principal Investigator
Software, Robotics and Simulation Division,
NASA Johnson Space Center
jane.t.malin@nasa.gov
281-483-2046

May 2010

THE NASA STI PROGRAM OFFICE . . . IN PROFILE

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and mission, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at http://www.sti.nasa.gov

- E-mail your question via the internet to help@sti.nasa.gov

- Fax your question to the NASA Access Help Desk at (301) 621-0134

- Telephone the NASA Access Help Desk at (301) 621-0390

- Write to:
  NASA Access Help Desk
  NASA Center for AeroSpace Information
  7115 Standard
  Hanover, MD 21076-1320

NASA/TM–2010–214800

Automated Tool and Method for System Safety Analysis: 2009 Progress Report

Jane T. Malin, Principal Investigator
Software, Robotics and Simulation Division,
NASA Johnson Space Center
jane.t.malin@nasa.gov
281-483-2046

May 2010

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
301-621-0390

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
703-605-6000

This report is also available in electronic form at http://ston.jsc.nasa.gov/collections/TRS/

Table of Contents

Problem Statement …….…….. 1

Technical Approach …….…… 2

2009 Progress …….. 4

Constellation Orion Cases ……. 4

Improvements in Information Extraction and Display …….. 4

Software Safety Engineer Evaluations …….. 5

Model Reuse Study …… 6

Virtual System Integration Laboratory Simulation Model …. 6

2010 Milestones …….. 7

Papers and Publications …….. 7

Problem Statement

Unsafe system-software interactions are a major concern in the software safety community. As shown in Figure 1, operations and stresses in software can "activate" faults and influence failures in the controlled system or the environment. Likewise, operations and stresses in the controlled system or the environment can "activate" faults and influence failures in the software. Interacting cascades are possible. Early evaluation of software requirements and design will reduce system-software integration risks, by identifying relevant factors in complex controlled systems that are easily overlooked. It is also important to assess system failures and anomalous conditions that may challenge software in system integration testing.

Multiple independent analysis approaches are used to assure safety. NASA safety and risk analysts commonly produce and review failure modes and effects analysis (FMEA) documents and the hazard reports that document hazard analyses. These two types of analysis are intended to be complementary, providing a more complete understanding of risks than either analysis alone would provide. FMEAs are produced bottom up from component failures, and identify the causes and impacts of the failure modes in phases of operation. Hazard analyses work from top mishap events down to analyzable hazards. Hazard reports include causes, controls that can be applied to each cause, and verifications for these controls. These two types of analysis should "meet in the middle". Thus, it is useful to trace how entities and failures in one type of analysis map to entities and failures in the other. Terminology variants used by independent analysts make tracing difficult, and performing manual reviews is difficult when there are large numbers of documents. If developed early, models, visualizations, system simulation, and failure mode testing can help safety analysts identify gaps in requirements and safety analyses. This information is needed for better informed failure mitigation strategies. Without the use of such tools early in development, the probability increases that requirements-induced errors and hazards will propagate to subsequent development phases and into operations.

A unified, systematic, and automated approach is needed for extracting early information from requirements specifications and other documents, for system modeling, requirements validation, and safety analysis. Semi-automated extraction of data and generation of models and visualizations can save labor and schedule. Automated information extraction can improve the efficiency, consistency, repeatability, and completeness of modeling and analysis, and it can reduce the time spent reanalyzing when specifications and designs change.

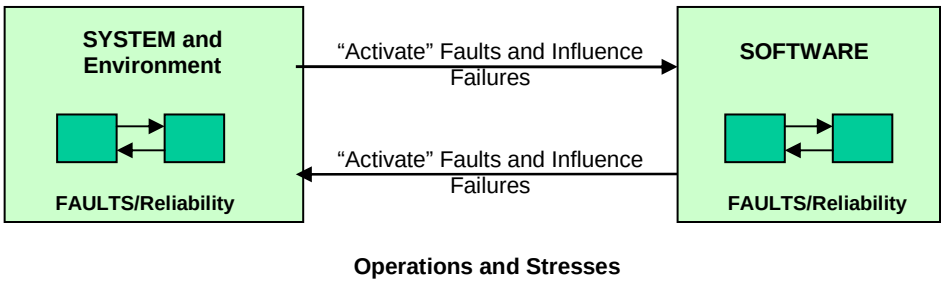

Figure 1 – Concept of System-Software Interactions Related to Hazards

Technical Approach

The Automated Tool and Method for System Safety Analysis project uses a linguistic analysis tool (Semantic Text Analysis Tool – STAT) to extract key information from FMEAs and hazard reports. Model generation software in the Hazard Identification Tool (HIT) integrates this information into visualizations of system architecture models. The primary sources of extractions are FMEA documents, which contain system descriptions, problem descriptions, and statements about connections and dependencies. Interface requirements documents (IRDs) also contain information on components and connections. The component-connection models are linked to text describing failures and failure causes in both FMEA worksheets and hazard reports. Thus, the visualized models summarize information scattered in three types of large document sets (FMEAs, IRDs, and hazard reports). The intent is to make it easier to review hazard paths and find redundant and missing links within and between types of analysis. Prototyping with documents produced prior to the NASA Crew Exploration Vehicle (CEV) Preliminary Design Review (PDR) shows how these visualizations can assist safety engineers in early evaluation of system requirements, preliminary designs, and safety analyses.

The model generation process creates a multi-level component connection model of the system. STAT derives information on the system parts hierarchy both from the organization of document sections that describe parts relationships and from parsed text that indicates part-whole relationships. STAT also extracts and parses text from document sections likely to contain statements about the connections between components and the resources transmitted across connections. For each model component or component connection, the source text excerpt and reference are extracted for use in the visualization. The extracted information is written in a structured form to xml files for use by the application that generates the visualization.

Visualizations of the models are automatic by-products of the model generation process (Figure 2 shows an example visualization). The primary sources of the models are parts hierarchies and component-connection information in FMEAs. In the graphical display or visualization on the left side of Figure 2, a mouse click on a component or connection will display the document citation (document title and worksheet number). On the right-hand side, a pop-up window shows some FMEA documentation for the “Initiator” components in the visualization. The pop-up window can also show information from the FMEA about the item, item function, failure modes and failure mode causes.

Figure 3 shows stages in constructing component connection models. STAT parses a natural language sentence from an IRD about the interaction between the Crew Module (CM) and Launch Abort System (LAS), producing the xml form containing the parsed sentence. The component-connection form at the bottom maps extracted terms from the sentence to elements of the component connection model, by using criteria based on Aerospace Ontology (AO) classes for physical objects and functions. The terms and hierarchical classes in the AO are used to reconcile terminology differences among documents and to filter out irrelevant information during model generation by HIT.

A system-level simulation was created from PDR documentation to model the Orion LAS and CM control avionics. This Virtual System Integration Laboratory (VSIL) provides a means of dynamically evaluating the impact of failure modes on the executing system design. Failure modes of safety plugs, Safe&Arm valves, initiators, thermal batteries, and electronic control signals can be used to evaluate system responses to such events. Orion system behavioral models in the VSIL are necessarily abstract due to lack of available design information and project scope.

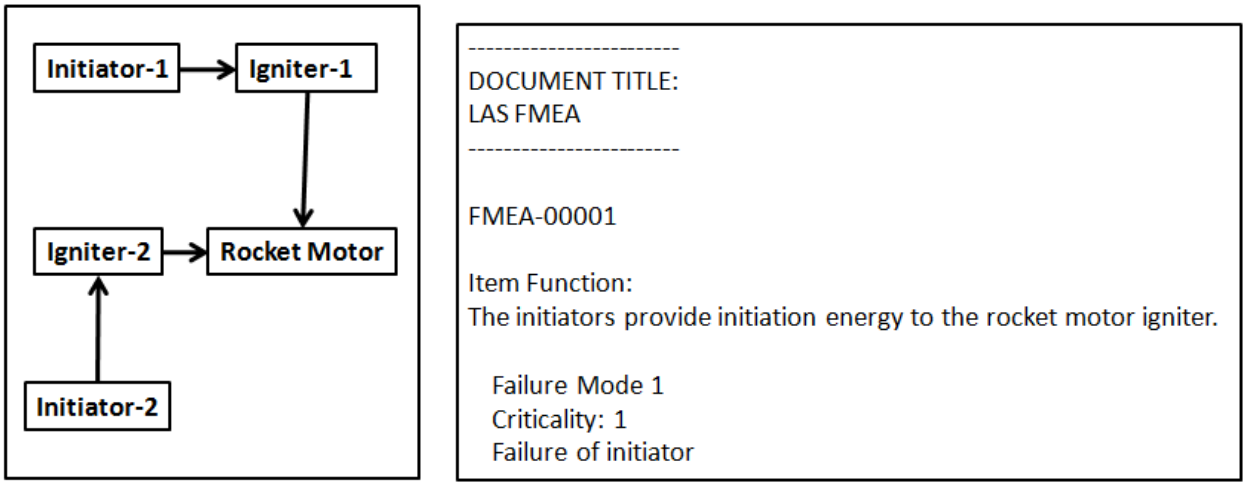

Figure 2 – A Rocket Subsystem and FMEA Display for Initiators

The CM shall receive health and status data from the LAS in accordance with TBD-NNNN-MMMM.

```
<Scope count="0">
    <objHead text="HEALTH AND STATUS DATA"/>
    <prepHead preposition="FROM" text="FROM THE LAS">
        <nounphr text="THE LAS" />
    </prepHead>
    <prepHead preposition="IN" text="IN ACCORDANCE">
        <nounphr text="ACCORDANCE" />
    </prepHead>
    <prepHead preposition="WITH" text="WITH TBD-NNNN-MMMM">
        <nounphr text="TBD-NNNN-MMMM" />
    </prepHead>
    <subjHead text="THE CM">
        <nounphr text="THE CM" />
    </subjHead>
    <verbHead text="RECEIVE" verb="RECEIVE">
        <modifiersHead text="SHALL" />
    </verbHead>
</Scope>
```

```
((:SENDER "LAS" :MATCHES (#<CONCEPT-CLASS "Abort_System">))
(:RECEIVER "CM" :MATCHES (#<CONCEPT-CLASS "Aerospace_System">))
(:OBJECT "DATA" :MATCHES (#<CONCEPT-CLASS "Information_or_Signal_Obj">))
(:VERB "receive" :MATCHES (#<CONCEPT-CLASS "Receive">)))
```

Figure 3 – Interface Requirement, Parsed Sentence, and Form Indicating the Component Connection

2009 Progress

Constellation Orion Cases

The main case for this project has been the Orion LAS pyrotechnics system. The CM Vehicle Management Computers connect to and control the Pyrotechnic Event Controllers (PECs) in the Remote Interface Unit. The PECs drive the LAS Pyrotechnics and control ignition of the LAS motors, including the Abort Motor (AM), Jettison Motor (JM) and Abort Control Motor (ACM). A network of Flexible Confined Detonating Cords (FCDCs) connect many of the components that support ignition. In 2009, this work was extended to include another Orion case, the propulsion subsystem of the Service Module (SM). This subsystem was selected because the propulsion subsystem data book for the Orion PDR included well developed FMEAs and hazard reports for extraction. Documents for other subsystems were developed as well. Challenges arising from the SM case included new formats and text styles in the FMEA worksheets and hazard reports.

Improvements in Information Extraction and Display

In 2009, STAT capabilities were extended to handle more complex sentences and extract model information from hazard report text. Components, subcomponents, connections, and faults and failures can be extracted from Cause Descriptions and Cause Controls fields. Currently, this capability is not being fully used, but can be integrated in the future. The current hazard information pop-up windows highlight all instances of text in a hazard report that correspond to a FMEA model component. Improvements were also made to the automatic layout of the visualization and in model generation.

An example from the LAS pyrotechnics subsystem is shown in Figure 4. Green highlighting shows the components that are referenced in hazard reports. Highlighting and pop-up windows make it easy to see which FMEA components are mentioned in corresponding hazard reports. It is also easy to compare FMEA and hazard report information with side-by-side pop ups. Figure 5 shows a scrollable pop-up window with hazard report references to Through Bulkhead Initiator 2 (TBI-2 in Figure 4). In Figure 5, one of the cause controls involves use of rigorous design for minimum risk (DFMR) processes to achieve fault tolerance.

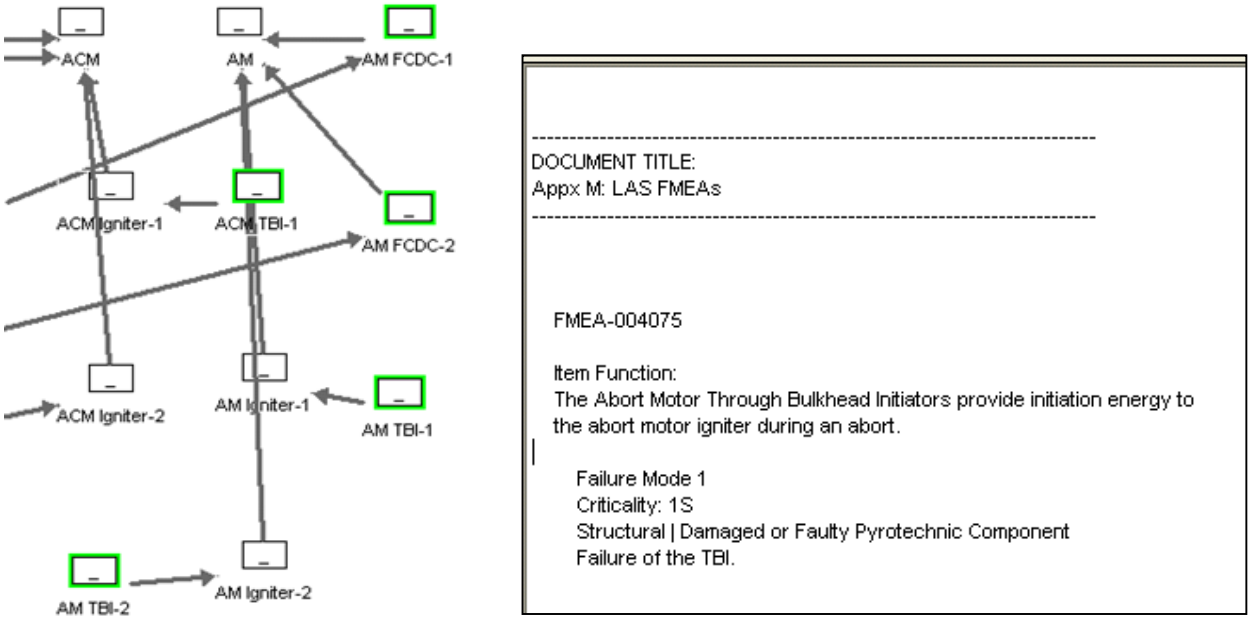

Figure 4 – LAS Pyrotechnics Model Fragment and FMEA Pop-up Window for AM TBI-2

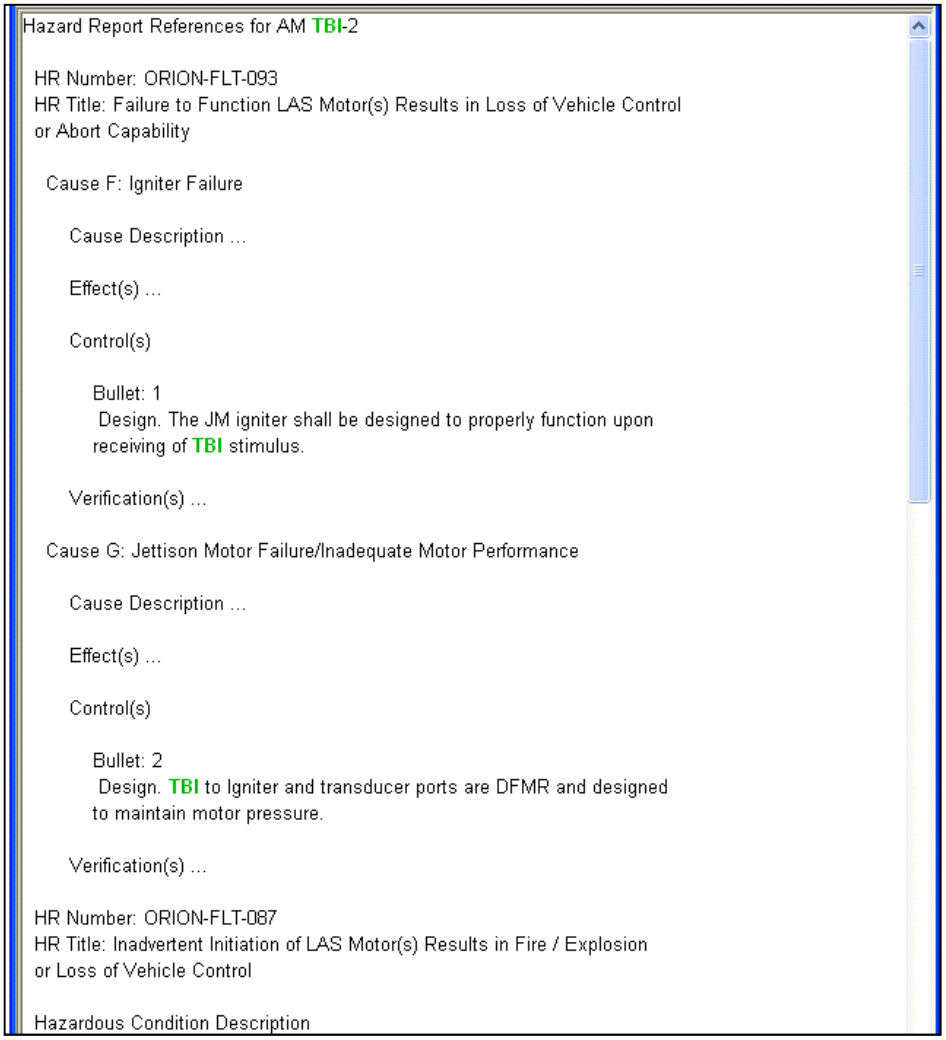

Figure 5 – Pop-up Window with Hazard Reports that Refer to TBIs

Software Safety Engineer Evaluations

Safety engineers reviewed visualizations in two evaluation sessions. The visualizations were for the Orion LAS pyrotechnics case. The reviews were positive; the engineers found that the organized information made it easier to inspect for problems and missing information in the documents. The engineers noted these advantages:

- Putting all the information related to a system component or a connection in one integrated visualization can reveal what information is redundant, inaccurate, or out of date. For example, there were several instances where more than one FMEA worksheet described the same component, possibly because the document had more than one author or because an outdated FMEA worksheet was not deleted when a new one was added. Such redundant FMEAs are noticeable in the pop-up information displays.
- Visualizing connected components helps the safety engineer check for components that have no outputs to any other component and components that have insufficient inputs. Either case may be an indication of omissions in system design or, more likely, the system documentation. The visualization also helps the engineer check whether the architecture fulfills requirements.
- Combining extractions from three types of documents helps build a more complete picture of the system. It helps to highlight terminology disagreements and missing and inconsistent information.
- References to specific information in the source documents for each component or connection are easily accessible.

Model Reuse Study

The STAT and HIT application suite can output an xml file containing the components, connections, and other properties of the system architecture model for use in other applications. The xml output function uses a specification of properties of the model to output, how to access them in the model, and the form they should take in the xml file. The specification facilitates updating and customizing information output for other uses.

A study was conducted to determine how other types of aerospace models can benefit from the types of information that can be extracted with the automated tools in this project. The study examined information requirements for functional fault models in the Testability Engineering and Maintenance System (TEAMS) tool and Finite State Machine (FSM) behavior models. It was determined that while the techniques used in the generation of FSM and TEAMS models cannot be completely automated, HIT models can be extended to include much of the necessary information used as inputs. Reusable model information includes:

- Component hierarchy and component-connection architecture - system models, configurations and phases
- Functions and actions of components
- Component modes/states and transitions - operating and failure modes, state transitions and triggers
- Faults and hazards, disabled functions, actions and transitions
- Instrumentation and key value constraints

Virtual System Integration Laboratory Simulation Model

The LAS VSIL simulator development has been completed to a functional state. The CM VMC commands and receives status from LAS pyrotechnics. The VSIL component hierarchy comprises the functional blocks that are involved in the LAS decision logic and execution of a launch abort sequence. VSIL parts include CEV and LAS avionics, pyrotechnic separators for LAS and CM, avionics connections to the pyrotechnics, AM, ACM, JM, the thrusters for each motor, valve assembly and control system, igniter assemblies, canard, fairing, spacecraft adapter, ground systems, mission systems, and communication network node. All essential LAS pyrotechnics parts from a system diagram have been modeled. Tests have been written to verify nominal VSIL functionality. Figure 6 shows an example output from a single test group in the test result file after verification testing.

```
Test 2: LAS Safe/Arm Valve Tests

Step 2a. Verify Safe/Arm Valve Initial State == SAFE
    Abort Motor Valve Status == SAFE:  +++ PASS +++
  Jettison Motor Valve Status == SAFE:  +++ PASS +++

Step 2b. Verify SA Valves switch to ARMED State under
command
  VMC commanding both SA Valves to ARMED State...
    Abort Motor Valve Status == ARMED:  +++ PASS +++
  Jettison Motor Valve Status == ARMED:  +++ PASS +++

Step 2c. Verify SA Valves switch to SAFE State under
command
  VMC commanding both SA Valves to SAFE State...
    Abort Motor Valve Status == SAFE:  +++ PASS +++
  Jettison Motor Valve Status == SAFE:  +++ PASS +++

Test 2 Final Result: +++ PASSED +++
```

Figure 6 –Example from VSIL Test Result File

Early testing in a VSIL complements FMEA by helping safety analysts to dynamically verify the effects of component failures on the system design. Progress has been made toward automating the process of translating failure modes identified in the FMEAs into a collection of failure mode test files. The VSIL model reuses the HIT xml model file to parse and extract failure mode identified and analyzed in the FMEAs, for testing in the VSIL simulation. These files serve as frameworks for developing failure mode tests, with direct pointers to component instances. This approach eliminates transcription errors and takes half the time of manual test framework generation.

Since the VSIL was developed from information in the requirements and design documentation, the names of the model components sometimes differ from the names used in the FMEA documents. In order to use information extracted from the FMEAs, an xml file was manually created to map FMEA document nomenclature to VSIL component nomenclature. To support efficient scaling of automated failure mode test framework generation, some coding progress has been made to provide for the automatic generation of this map file.

2010 Milestones

Q2 Complete and evaluate visualization for safety engineers
Complete automated VSIL failure mode test framework generation
Q3 Complete path analysis algorithms and evaluation
Complete VSIL user guide and test method documentation
Manage and compare model versions when source documents change
Complete enhanced version of integrated tool suite
Q4 Software Assurance Symposium Presentations and Demonstration.
Complete project software source files and documentation and deliver on CDs.
Complete evaluations and final methods document.
Complete project analysis results files or reports to Orion S&MA customer
Complete project Final Report.

Papers and Publications

Malin, J. T., Millward, C. , Schwarz, H. A., Gomez, F., Throop, D. R., and Thronesbery, C. “Linguistic Text Mining for Problem Reports,” 2009 IEEE International Conference on Systems, Man and Cybernetics, San Antonio, TX, October 2009, 1578-1583.

Malin, J. T., Fleming, L., Thronesbery, C., Throop, D. R., and Bennett, T. “Integrated Visualization of Information from Requirements, Safety Analyses and Hazard Reports,” submitted to 28th International System Safety Conference.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 2010	NASA Technical Memorandum

4. TITLE AND SUBTITLE
Automated Tool and Method for System Safety Analysis: 2009 Progress Report

5. FUNDING NUMBERS

6. AUTHOR(S)
Jane T. Malin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Lyndon B. Johnson Space Center
Houston, Texas 77058

8. PERFORMING ORGANIZATION REPORT NUMBERS
S-1057

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
TM-2010-214800

11. SUPPLEMENTARY NOTES
NASA Johnson Space Center

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Available from the NASA Center for AeroSpace Information (CASI)
7115 Standard
Hanover, MD 21076-1320 Category: 38

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
This is a progress report for work performed in 2009 concerning the development of automated tools for system safety analysis. This involves a suite of two application software packages, Semantic Text Analysis Tool (STAT) and the Hazard Identification Tool (HIT). STAT is used to extract key information from FMEAs and hazard reports, then HIT generated models integrate the information into a visualization or graphical display. These visualizations are helpful to safety engineers by revealing information that is redundant (e.g., multiple FMEAs on the same component), innaccurate or out of date.

14. SUBJECT TERMS	15. NUMBER OF PAGES	16. PRICE CODE
system safety analysis, FMEA, hazard report, , STAT	16	

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited