Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

ENGINEERING PROTOTYPE DEVELOPMENT

Failure Environment Analysis Tool (FEAT)

D. G. Lawler, ER22
Section Head
Advanced Automation Section
August 8, 1991

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

DEVELOPMENT BACKGROUND

SPACE SYSTEMS FAILURE ANALYSIS:

- Several approaches used by NASA SRM&QA, e.g.:
  - Failure Modes and Effects Analysis/Critical Items List
  - Integrated Hazards Analysis
- Digraph Modeling:
  - Developed in late 60's for nuclear power systems
  - Supports existing analysis methods
  - Supports Fault Tolerance and Redundancy Mngt Analysis

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

NOTES FOR PAGE I OF: DEVELOPMENT BACKGROUND

- Detailed understanding of the nature and extent of failures within an engineered system is absolutely vital for the successful deployment of such systems.
- Current NASA practice employs a number of different analysis techniques to determine the probability of system failures, the nature of these failures, the effect of these failures on other system components and the ultimate consequence of these failures on safety and overall mission effectiveness.
- Typical of these analyses are the Failure Modes and Effects Analysis/Critical Items List and the Integrated Hazards Analysis.
- In response to the need for a detailed understanding of system failures and their effects, a technique called Digraph Matrix Analysis was developed from work done at Lawrence Livermore National Laboratories on nuclear reactor safety analysis.
- This technique utilizes a directed graph modeling technique extended with the use of simple boolean -and- gates to model the propagation of failures throughout a system; both working from initial failure to final consequence as well as the reverse case.
- Such a technique is very useful in determining the effectiveness of the fault tolerance and redundancy management in the system's design.

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

DEVELOPMENT BACKGROUND (cont'd)

FEAT PROJECT HISTORY:

- Shuttle use of digraphs began in 1988
- FEAT development began in 1989
  - Early general release in 1990
  - FEAT version 3.3. currently available
- SSFP directive for digraph use issued 7/91

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

NOTES FOR PAGE 2 OF: DEVELOPMENT BACKGROUND

- Use of the digraph technique for modeling STS systems began in 1988 under the STS integration contract with Rockwell.
- Modelers soon realized the need for software to ease the burden associated with both modeling and the analysis of the model.
- FEAT development began in 1989, sponsored by C. Vaughan, Chief of the NASA - JSC Propulsion and Power Division.
- FEAT operates on an Apple Macintosh II computer and displays in color the effects of user selected failures. It also displays the possible initial failures for user selected conditions. Selection and display can be on either the digraph or a system schematic.
- FEAT has the capability to handle very large, orbiter size models. It includes the capability to reconfigure the digraph and schematic by preselecting numerous failures as having occurred, and then observing the causes and effects of additional failures.
- Sponsorship of FEAT was shifted to Automation & Robotics in the fall of 1990, with funding from the SSFP.
- The Digraph Editor was released in the spring of 1991 to assist in building models.
- In July 1991, R. Moorehead (director of SSFP/Level II) directed that Digraph modeling methods be utilized for support of Integrated Failure Modes and Effects Analysis, Integrated Hazards Analysis and Fault Tolerance and Redundancy Management Analysis. He also directed that FEAT be used for this support.

1008

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

DEVELOPMENT BACKGROUND (cont'd)

OBJECTIVE:

- To demonstrate advanced modeling and analysis techniques to better understand and capture the flow of failures within and between elements of SSF and other large complex systems

TECHNICAL CHALLENGE:

- Provide efficient modeling and analysis capabilities
- Capture system failure knowledge for use throughout program lifecycle
  - Integrate into other applications and environments

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

NOTES FOR PAGE 3&4 OF: DEVELOPMENT BACKGROUND

- This project is being pursued to enable SSFP managers to capture the flow of failure effects from within each element out to other elements, including those of the international partners.
- Successful completion of this project will provide a capability to quickly and efficiently predict effects from multiple failures in different station elements. It will also permit determination of the set of potential failures which are the most likely to have caused a given set of observed effects.
- FEAT will provide a means to demonstrate compliance with fault tolerance and redundancy requirements in a highly efficient manner. Also, design decisions can be affected by information available through FEAT and presented during design reviews.
- The model in FEAT will provide Engineering, Safety, Reliability, Supportability, Training, and Mission Operations support personnel with equal capability to determine the answers to "What if . . . ?" questions. When discussing issues, all of these organizations will be utilizing the same data set for these analyses.

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

DEVELOPMENT BACKGROUND (cont'd)

BENEFITS/APPLICATIONS:

- Support for SRM&QA analyses of large complex systems
  - Increase systems reliability and systems safety
  - Enables the comprehensive analysis of large complex systems
- Capture of system failure knowledge
  - Support for engineering design (e.g. system evolution) training, operations, etc.
  - Cost savings from maintenance of single data source

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

TECHNICAL APPROACH

OVERVIEW:

- Develop base capabilities on Macintosh
  - FEAT & Digraph Editor
- Port identical capability to Unix and X-Windows environments
  - Integrate into TMIS environment
- Support modeling activities
  - STS (e.g. MMU) & SSFP systems
- Support additional digraph applications

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

NOTES FOR PAGE 1 OF: TECHNICAL APPROACH

- Macintosh versions of FEAT are being produced first. The code is then ported to Unix operating system computers supporting the X Window interface environment, including the SSFP TMIS standard Intergraph CIE workstation. All coding is in the K&R C programming language. There is no PC version in development or planned at this time.
- All machines running the same version of FEAT will have the same look and feel to the user.
- At the end of August 1991 FEAT 3.3 and the Digraph Editor 3.0 will be released and forwarded to COSMIC. This will provide the basic functionality required to begin modeling Freedom and to analyze the resultant models.
- Model development is currently being funded separately from the software enhancement effort.

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

SSFP BASELINE INTEGRATION

GENERAL SUPPORT:

- Level III funding near term analysis support needs
- Level I funding advanced development efforts

SSFP LEVEL II:

- Digraphs and FEAT have been adopted for supporting Integrated FMEA, Integrated Hazards Analysis, etc.
- Support for MTC Phase Review and CDR

SSFP OPERATIONS:

- Support for SSCC Fault Detection and Management function (under consideration, decision by 1/92)
- Support for SSFP & STS training script development (under consideration)

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

NOTES FOR PAGE 1 OF: SSFP BASELINE INTEGRATION

- FEAT project funds are provided are by SSFP Levels I and II. - Level II, through level III Engineering at JSC, is funding the features needed in the near future to support Program decision points.
  - Level I is funding capability development to support needs required later in the Program.
- New versions of FEAT will support FMEA development and be integrated with the SSF TMIS.
- Initial Freedom modeling will focus on areas with the greatest payback in design evaluation at the MTC CDR.
- Digraphs and schematics in FEAT will support needs of at a minimum the following organizations:
  - Program Engineering (including design engineering integration, safety, reliability, and supportability)
  - Mission Operations (including training and mission support)

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

GROWTH AND EVOLUTION

FEAT ENHANCEMENTS:

- Integration of FEAT with other SRM&QA tools
- Digraph Editor enhancements
- Large model processing

ADVANCED DEVELOPMENT:

- Smart Digraph Editor will provide automated support to model development
- Advanced modeling support
  - e.g. - Temporal modeling and analysis

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

NOTES FOR PAGE 1 OF: GROWTH AND EVOLUTION

- Enhancements to FEAT are being pursued by SSFP Levels I and II. - Level II, through level III Engineering at JSC, is funding the features needed in the near future to support Program decision points.
  - Level I is funding capability development to support needs required later in the Program.
  - This includes support of the Space Station Control Center Fault Detection and Management capability, as well as a Smart Digraph Editor to reduce the manpower intensity of digraph modeling.
  - Large model analysis is very expensive computationally. Parallel processing capability is being developed to significantly reduce the turn-around time required for transitive closure calculations.

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

SUMMARY

- FEAT is available now and in use by SSFP
- Robust, ongoing, development program
- Many significant potential applications
  - Significant cost avoidance/savings anticipated through use of common models

Engineering Prototype Development: Failure Environment Analysis Tool (FEAT)	Automation and Robotics Division	
	D.G. Lawler/ER22	8/8/91

NOTES FOR PAGE 1 OF: SUMMARY

- FEAT is available now to support various types of engineering applications and is undergoing continuous improvement. It will be used to assist in the analysis of failure effects across Freedom, but the broad application of advanced modeling techniques is only now becoming understood within the NASA community. Significant cost savings is anticipated through the use of common models over a broad range of applications.