A HAZARD CONTROL SYSTEM FOR ROBOT MANIPULATORS

Ruth Chiang Carter
Goddard Space Flight Center
Greenbelt, MD 20771

Adrian Rad
Hernandez Engineering, Inc.
Greenbelt, MD 20770

ABSTRACT

Unlike the industrial robots in wide use around the world today, which generally perform various but limited repetitive tasks, a robot for space applications will be required to complete a variety of tasks in an uncertain, harsh environment. This fact presents unusual and highly difficult challenges to ensuring the safety of astronauts and keeping the equipment they depend on from becoming damaged. The application of system safety engineering to the design and development of the robot ensures that it will not become an instrument of harm or destruction to the space vehicle and its occupants. This paper describes the systematic approach being taken to control hazards that could result from introducing robotics technology in the space environment.

First, this paper will discuss system safety management and engineering principles, techniques, and requirements as they relate to Shuttle payload design and operation in general. The concepts of hazard, hazard category, and hazard control, as defined by the Shuttle payload safety requirements, will be explained.

Second, this paper will show how these general safety management and engineering principles are being implemented on an actual project. It will present an example of a hazard control system scheme for controlling one of the hazards identified for the Development Test Flight (DTF-1) of NASA's Flight Telerobotic Servicer, a teleoperated space robot. The paper will also discuss how these schemes can be applied to terrestrial robots as well. The same software monitoring and control approach will insure the safe operation of a slave manipulator under teleoperated or autonomous control in undersea, nuclear, or manufacturing applications where the manipulator is working in the vicinity of humans or critical hardware.

SYSTEM SAFETY ENGINEERING CONCEPTS

System safety is the overall management and engineering approach to the evaluation and reduction of risk in a system and its operation. In general, system safety activities include systematic identification of hazards, elimination of those hazards to the maximum extent possible, assessment of the residual risk inherent in the system or its operation, management review and acceptance of the risk, and documentation of the management decision and rationale in accepting the risk. In addition, some type of control for the hazards must be instituted.

In order to analyze the safety of any system properly, the system safety engineer must have a thorough knowledge of the system, subsystems, interfaces, functions, characteristics, intended use or operation, and the operational environment. It is therefore necessary for the system safety engineer to work closely with systems engineering, subsystem/component design engineering, mission operations, and support engineering personnel in developing a complete and accurate system description and operations scenario that can adequately support the identification of all potential hazards in the design and use of the system. Once an accurate system description is developed, the basic characteristics and functions of the system are defined, and preliminary operation scenarios are formulated, detailed hazard identification can begin.

The system safety discipline has established standard analysis methods and techniques for identifying hazards and categorizing their potential severity, including Preliminary Hazard Analyses, System/Subsystem Hazard Analyses, Operating Hazard Analyses, and Fault Tree Analyses. The analyses are prepared during system concept definition, design, and development in a cooperative and iterative process. The results can therefore

more effectively support management personnel in making decisions and in accepting risks; system safety personnel in assessing risks and identifying hazards; systems/subsystem, operations, and system safety engineering personnel in developing designs and operating procedures that eliminate and/or reduce hazards; support services personnel in conducting activities, such as configuration management and test and verification; and quality assurance personnel in documenting and verifying requirements and design criteria compliance.

SYSTEM SAFETY ENGINEERING IMPLEMENTED FOR DTF-1

The following paragraphs explain how system safety engineering was implemented for the (DTF-1). This example is intended to illustrate the system safety engineering process. In general, all of the information presented in this paper was gathered from DTF-1 design and safety engineering documents. Some information has been simplified and other information is not presented so as to facilitate a clearer presentation of the process.

System and Operation Description

The DTF-1 consists of the aft flight deck (AFD) element and the payload bay (PLB) element connected by two communication networks or buses. The AFD element, referred to as the workstation, is made up of a handcontroller, handcontroller electronics, and a control display console and assembly, including computer displays and video displays from cameras mounted on the manipulator and on other locations in the PLB, and a keyboard. The handcontroller is a device that is used to relay the motion, displacement, or relocation of the operator's hand as inputs to the control system. The handcontroller electronics transform the inputs into command signals to be sent to the manipulator in the PLB. The computer displays are the available manipulator/system parameters, sensor data, and manipulator position measurements, such as joint position, end-effector position, velocities, forces and torques, temperatures, and computer control system health and status. The AFD elements are provided electrical power through the power control and distribution unit (PCDU).

The PLB element, physically located in the Shuttle's cargo bay, includes the DTF-1 telerobot (TR), a TR control computer (TRCC), a TR redundant controller (TRRC), the power module and controller, and the payload controller (Figure 1). The TR consists of a telerobot body and a seven degree-of-freedom dexterous manipulator (Figure 2) with three computer controllers built into it--the shoulder controller, the upper arm controller, and the lower arm controller. These controllers, collectively referred to as joint controllers, provide joint position control loops and other control system functions. The TRCC provides the primary command and control function. The TRRC provides an independent safety checking and monitoring that includes collision avoidance and safety critical parameter monitoring. The power module and controller perform electrical power regulation and distribution control. The payload controller provides camera control, Shuttle-to-ground data downlink interface, and other support functions. Other PLB elements include an end-effector, a task panel, supporting structures, and other equipment. On the task panel are manipulation and articulation, partial disassembly, reassembly, removal, positioning, and reinstallation tasks.

The workstation bus connects the handcontroller electronics and control display console with the TRCC, the TRRC, the power module controller, and the payload controller. The TR bus connects the TRCC and the TRRC with the joint controllers.

As the operator at the AFD workstation positions and repositions the handcontroller, the handcontroller electronics transform the inputs into command signals that are sent to the TRCC. The TRCC then calculates the joint and end-effector motor commands needed to implement the commands; monitors manipulator position and velocity; and sends joint commands to the joint controllers. The joint controllers receive the commands, generate the needed joint motor currents, and monitor joint position and rotation against predefined limits. The joint position and torque sensors feed back data to the TRCC and the TRRC where the manipulator position and velocity are updated. This process is repeated continually throughout the teleoperation.

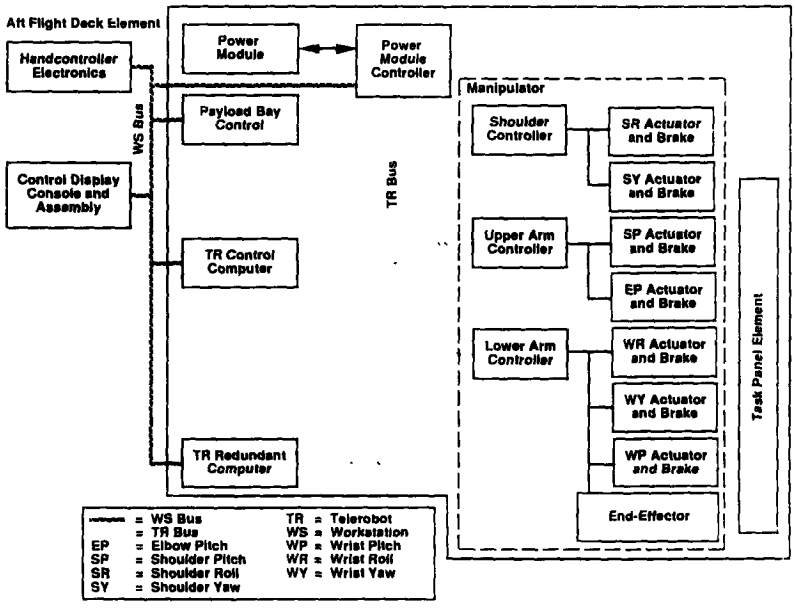


Figure 1. System Description Block Diagram

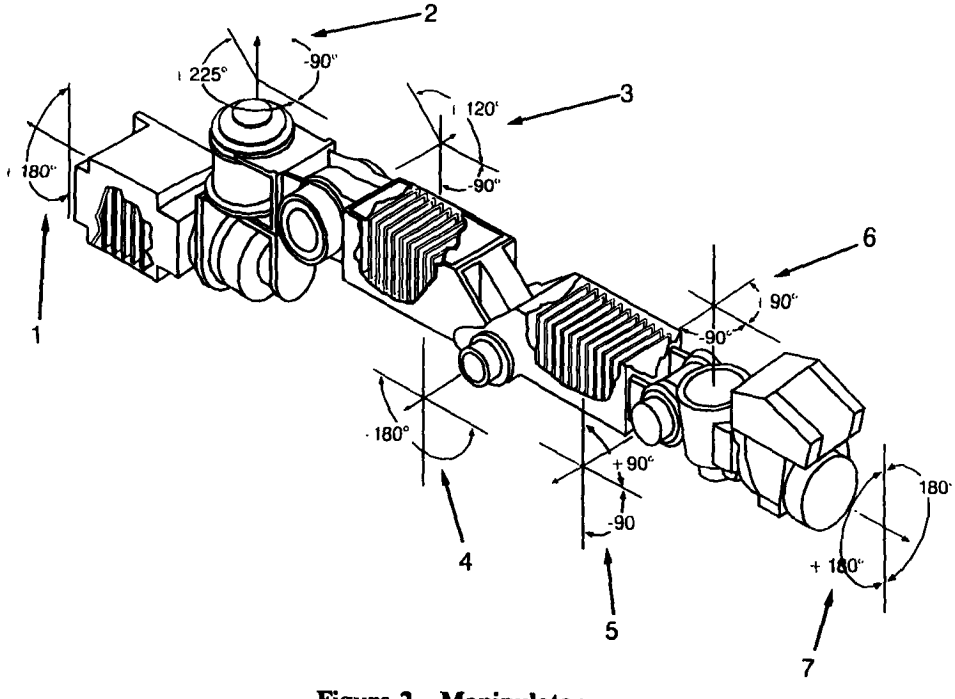


Figure 2. Manipulator

System Safety Requirements and Design Criteria Used

System safety engineering for DTF-1 was implemented with the system safety requirements and design criteria established by NASA's National Space Transportation System (NSTS) Program and defined in the Safety Policy and Requirements for Payloads Using the Space Transportation System, NSTS 1700.7B.
All hazards that could be eliminated were eliminated. The remaining hazards were controlled through safety devices, warning devices, or special procedures. The basic method for minimizing or controlling hazards, as prescribed by NSTS 1700.7B, is a failure tolerant design. The hazard severity category (i.e., critical or catastrophic) determines the failure tolerance design requirements. Critical hazards were controlled in a single-failure manner and catastrophic hazards were controlled in a two-failure tolerant manner.

Specific requirements and design criteria for subsystems, safety-related features, specific hazardous functions, and environmental compatibility were also included in NSTS 1700.7B to ensure the safety of the system design. They included structures, material compatibility, flammability, deployment and separation, contingency return and rapid safing, and others.

Hazard Identification

The potential hazards related to teleoperation of a dexterous, seven degree-of-freedom manipulator in orbit include collision or impact and excessive force and torque generated by the manipulator.

A catastrophic hazard could occur if the TR inadvertently collides into or otherwise impacts its surroundings during in-orbit operation. For example, if the motor and gear actuators generate excessive forces or torques at any of the seven TR joints or if excessive forces or torques are induced at the Cartesian level through the manipulator at the end-effector, then one or more of the manipulator joints may fracture or suffer other damage and the end-effector may generate excessive forces or torques on the task panel, surrounding structures, or equipment. Structural failure will cause the mission to be terminated. Also, it could severely compromise the ability to stow the manipulator safely and may create debris of sufficient size and mass to damage critical Shuttle equipment and prevent the Shuttle from returning home safely.

Another catastrophic hazard could occur if the manipulator is improperly positioned or is moving too fast and violates the predefined workspace. This situation along with other failures, such as loss of control of the manipulator's movement, could prevent closing of the payload bay door and return of the Shuttle.

Potential hazards for DTF-1, such as the ones just described, were controlled for with a two-failure tolerant hazard control system; i.e., three separate hazard control methods have been implemented. If two of the three methods fail, the third one will still control the hazard. The following paragraphs detail this system.

Hazard Control System

The hazard control system controls excessive forces or torques and prevents collision or impact through an integrated DTF-1 computer control, sensor, and feedback system. Forces and torques or position and velocity commands are limited, safety critical parameters are monitored, and redundant safety critical parameters are monitored. If safety limits are exceeded, electrical power is removed from the joint motors and the fail-safe brakes are engaged (Figure 3). This process is termed emergency shut down (ESD).

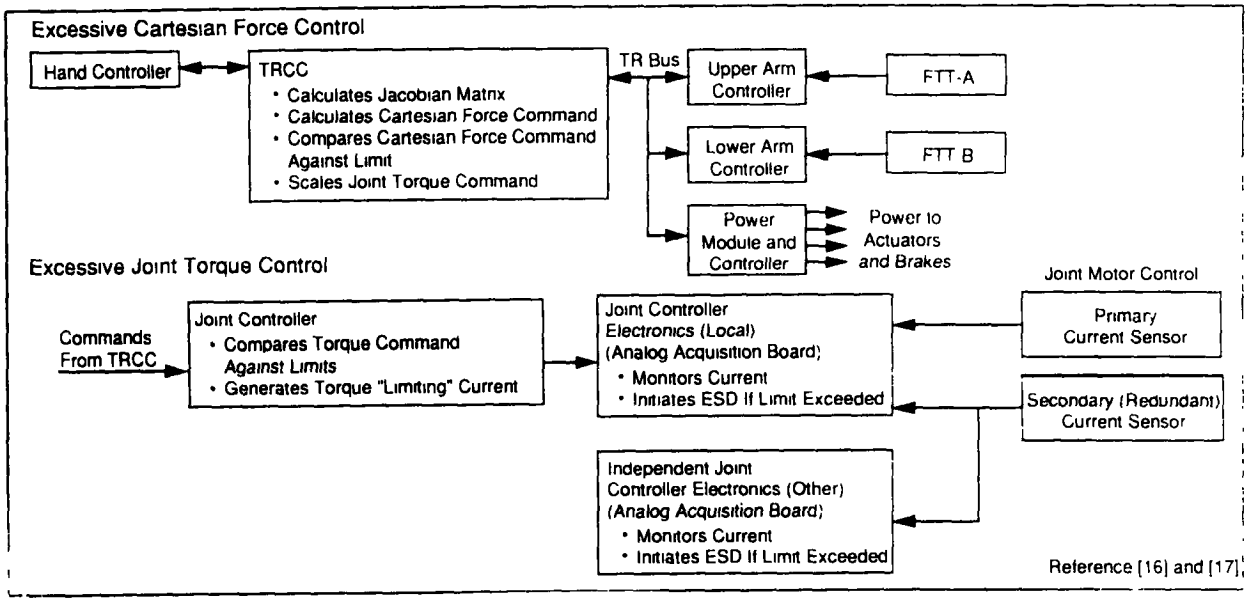


Figure 3. Excessive Force/Torque Hazard Control Scheme

Excessive Force and Torque Hazard Control

Force and torque commands are limited at the Cartesian level and at the joint level. Cartesian-level control limits the Cartesian position, velocity, and force at the manipulator and end-effector. Joint-level control prevents the motor and gear actuator assemblies from exceeding rated design torques. Joint-level control also provides a rapid response to joint "run away."

At the Cartesian level, hazard control is implemented as follows:

1) The TRCC calculates forces and torques for the end-effector from joint command inputs. Then the "commanded" forces and torques are compared against predefined safety limits. If the limits are exceeded, the inputs are automatically scaled down to acceptable levels before being passed onto the joint controllers.

2) Forces transmitted to the upper arm controller or to the lower arm controller by the force torque transducer (FTT) (located near the end-effector at the tool plate) are compared against predefined safety limits. If they are exceeded, an ESD is initiated.

At the joint level, hazard control is implemented as follows:

1) Current to the joint controllers is limited to that corresponding to the actuator-rated design torque.

2) The current in the primary and the secondary current sensors is monitored and compared to predefined safety limits. If they are exceeded, an ESD is initiated.

Collision and Impact Hazard Control

Collision and impact hazards are limited at the Cartesian and joint levels by controlling the manipulator's position and rate of motion (velocity). Limits on manipulator travel distance restrict the manipulator's position to within the predefined workspace. Limits on velocity control the force with which the manipulator impacts its surroundings. Cartesian-level controls limit the manipulator's movement in free space (work space) and joint-level controls limit individual joint movement in joint-space.

The distance at which the manipulator can be stopped is a function of the mass of the load the manipulator is carrying and the manipulator's velocity. The allowed velocity depends on the proximity of the manipulator to another object. Rate limits used in the servo algorithms are adjusted according to this distance. Violations of these limits require that the manipulator position commands be modified enough to slow its movement.

The boundary management and touch control (BMTC) system is used to control collision and impact hazards. This system sets imaginary (invisible) boundaries in and around the workspace, thus preventing unplanned contact which can result in collision and impact. Figure 4 shows how BMTC is implemented in the DTF-1's computer system. Figure 5 shows the functional scheme for BMTC. The four regions (X, A, B, and C) define the distance from geometric objects and are used to model each physical object. When the manipulator is in region C, normal free-space motion limits apply. In region B, the rate limits are reduced. At the outside of region A, a soft stop will occur unless or until the boundary is disabled. At the outside of region x, an ESD will occur unless the boundary is disabled. Region X and region A boundaries are disabled at the same time. A safety rate limit ESD can occur in regions A, B, or C if the operation rate limits are not applied.

Hazard Control System Assessment

Each safety feature of the DTF-1 hazard control system was analyzed at a system level to verify its effectiveness. This activity is important especially for a complicated system like the DTF-1 because failure tolerance is implemented only through the integration of all the safety features. A number of analyses were performed. However, only the fault tree analysis is used to illustrate the methodology and its usefulness in system evaluation.

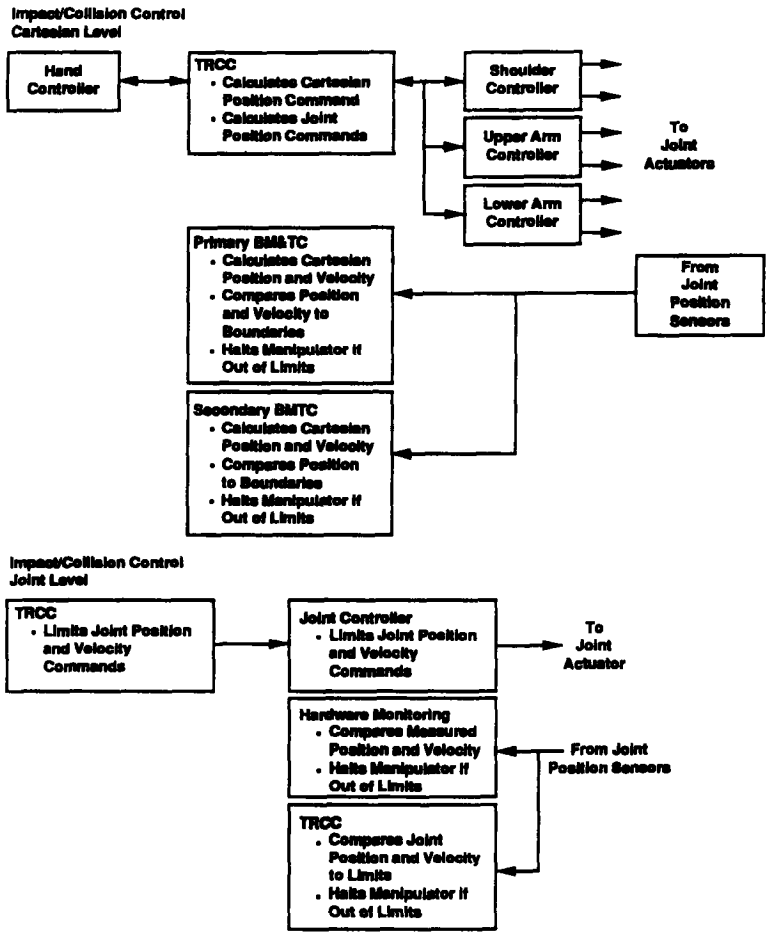
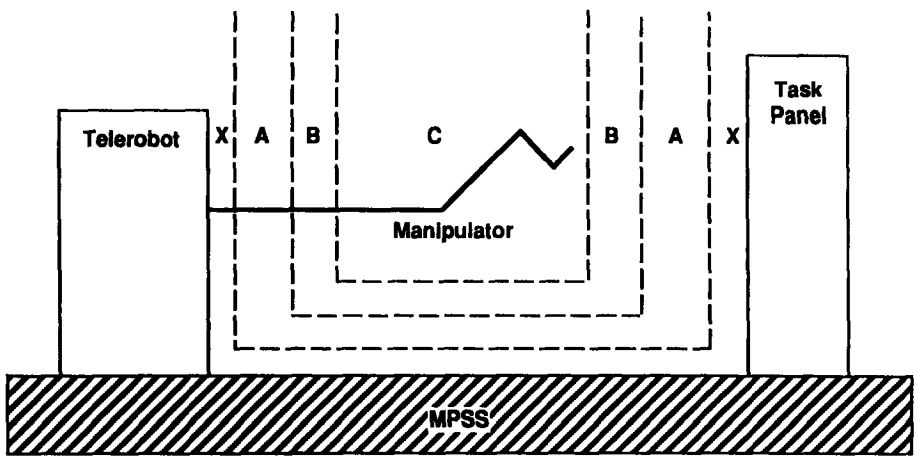


Figure 4. Collision/Impact Hazard Control Scheme



Region X: ESD Region
Region A: Automatic Soft Stop/Safe-Contact Rate Limited
Region B: Automatic Reduced Rate Limited
Region C: Normal Rate Limited

Figure 5. BMTC Functional Scheme

Fault tree analysis was adopted to evaluate hazard controls for excessive force/torque and collision/impact hazards. This analysis was chosen because of its top down approach. Through the analysis, it can be determined what components/functions must fail in order for a hazard to occur. If the results show that more than three components/functions must fail before a hazard can occur, then the implemented hazard control system is at least two failure tolerant. Figure 6 is a fault tree for the excessive force/torque hazard. It specifies the components/functions that directly contribute to the hazard.

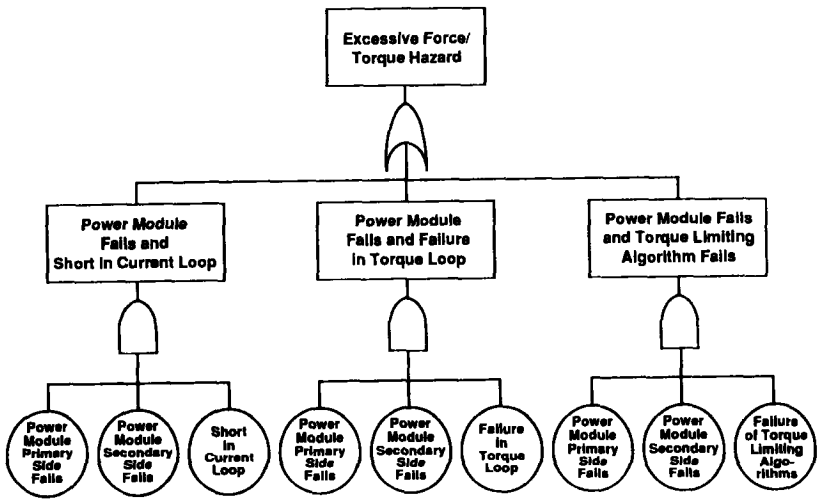


Figure 6. Fault Tree for Excessive Force/Torque

TERRESTRIAL APPLICATIONS

The DTF-1 hazard control system can be applied to any robotic and telerobotic system in which unplanned contact, impact, excessive forces and torques and manipulator motion control are of concern. It is applicable for terrestrial-based telerobotic and autonomous systems that must operate in varying environments, in confined workspaces, and near safety critical or hazardous equipment, such as those used in nuclear power plants, in under the sea operations, or on the factory floor.

In implementing the DTF-1 hazard control system, many of the design features common to all robotic systems, such as joint position sensors, force/torque sensors, and control computers and software have been used. As good system safety engineering dictates, the safety features would need to be customized and modified to the specific system design and operation for which they will be implemented. Equipment or components not available in the robotic or telerobotic system would not need to be incorporated.

CONCLUSION

The implementation of system safety engineering for the DTF-1 has been an iterative process. The initial concept was evaluated against safety requirements, and the system's fault tolerance was determined. In each of the subsystem areas, all possible hazardous events were hypothesized and their controls were evaluated. For example, two hypothesized hazard cases for which the analysis was completed were the excessive force/torque hazard and the collision/impact hazard. Once the possibility of these hazards actually occurring was confirmed, then designs and procedures were created to limit or prevent the hazardous commands from being generated.

The experience of implementing system safety engineering on the DTF-1 indicates that designing safety into the system early in the process maximizes the safety of the design and minimizes impacts to design complexity, development cost, and scheduling. Systems engineers, subsystem/components designers, and system safety

engineers are partners in creating an effective system safety scheme. Together, they will ensure that hazard control becomes integral to mission execution and a balance is achieved between a safe design and one that can accomplish maximum results.

ACKNOWLEDGEMENTS

Portions of this paper have been extracted from various project documents and technical meetings where FTS project staff provided valuable technical inputs. Specifically, Mr. Jim Andary, Systems Manager for the FTS Project, provided technical expertise and advice. In addition, the authors would like to acknowledge Ms. Barbara Hunt, without whose help completing this paper would not have been possible.

REFERENCES

[1] Flight Telerobotic Servicer Requirements Definition and Preliminary Design. SS-GSFC-0028, April, 1987.

[2] Flight Telerobotic Strawman Concept Engineering Report, SS-GSFC-0031, March 15, 1987.

[3] H. E. Roland, B. M. Moriarty, System Safety Engineering and Management, New York: John Wiley & Sons, Inc., 1983.

[4] J. F. Andary, S. W. Hinkal, and J. G. Watzin, "Design Concept for the Flight Telerobotic Servicer (FTS)" presented at the Second Annual Workshop on Space Operations Automation and Robotics (SOAR '88), Wright State University, Dayton, Ohio, July 20-23, 1988.

[5] J. F. Andary, D. R. Hewitt, and S. W. Hinkal, "The Flight Telerobotic Servicer Tinman Concept: System Design Drivers and Task Analysis," in the Proceedings of the NASA Conference on Space Telerobotics, vol. III, pp. 447-471, January 31, 1989.

[6] Safety Policy and Requirements for Payloads Using the Space Transportation System, NSTS 1700.7B, NASA Lyndon B. Johnson Space Center, 1989.

[7] System Safety, NASA Safety Manual, vol. 3, NHB 1700.1 (v3), April 11, 1984.

[8] System Safety for Orbital Flight Projects, NASA/Goddard Space Flight Center (GSFC) Management Instruction (GMI) 1700.3A, August 2, 1988.

[9] System Safety Program Requirements, Military Standard 882B (MIL-STD-882B), March 30, 1984.

[10] J. Hammack, A. Hernandez, S. Smith, "System Safety Training Course," Hernandez Engineering, Inc., Houston, Texas, December 1990.

[11] American National Standard for Industrial Robots and Robot Systems--Safety Requirements, American National Standards Institute/Robotic Industries Association (ANSI/RIA) R15.06, June 13, 1986.

[12] P. A. Lockner, P.D. Hancock, "Redundancy In Fault Tolerant Systems," Mechanical Engineering, pp. 76-83, May 1990.

[13] Hazard Analysis of the RMS (Robotic Arm) Simulation Using the Robot Safety Analysis, NASA/Goddard Space Flight Center (GSFC)/Code 205, December 22, 1988.

[14] Y. Sato and K. Inoue, "Safety Assessment of Human-Robot System: Hazard Identification Based on the Action-Change and Action-Chain Models," Bulletin of The Japanese Society of Mechanical Engineering (JSME), vol. 29, pp. 1351-1361, April 1986.

REFERENCES (Continued)

[15] Y. Sato, E. J. Henley, K. Inoue, "An Action-Chain Model for the Design of Hazard-Control System for Robots," IEEE Transactions on Reliability, vol. 39, pp. 151-157, June 1990.

[16] Space Station Flight Telerobotic Servicer (FTS) DTF-1 System Critical Design Review, 01-MD-02-DCR-01, prepared by Martin Marietta Corporation under contract to NASA/Goddard Space Flight Center (GSFC), September 25, 1990.

[17] Flight Telerobotic Servicer Phase C/D DTF-1 Phase 1 Payload Design and Flight Operations Safety Compliance Data Package, PA-32-05, prepared by Martin Marietta Corporation under contract to NASA/Goddard Space Flight Center (GSFC), May 4, 1990.

TEST AND MEASUREMENT

(Session C6/Room B1)

Wednesday December 4, 1991

- **Knowledge-Based Autonomous Test Engineer (KATE)**
- **Advanced Computed Tomography Inspection System (ACTIS)**
- **High-Resolution Ultrasonic Spectroscopy System for Nondestructive Evaluation**
- **Force Limited Vibration Testing**