DEVELOPING A SAFE ON-ORBIT CRYOGENIC DEPOT

Nicholas J. Bahr[1]

Webb, Murray & Associates
Houston TX 77258

New U.S. space initiatives will require innovative technology to realize planned programs such as piloted lunar and Mars missions. Key to the optimal execution of such missions are high performance orbit transfer vehicles and propellant storage facilities. Large amounts of liquid hydrogen and oxygen demand a uniquely designed on-orbit cryogenic propellant depot. Because of the inherent dangers in propellant storage and handling, a comprehensive system safety program must be established. This paper shows how the myriad and complex hazards demonstrate the need for an integrated safety effort to be applied from program conception through operational use. Even though the cryogenic depot is still in the conceptual stage, many of the hazards have been identified, including fatigue due to heavy thermal loading from environmental and operating temperature extremes, micrometeoroid and/or depot ancillary equipment impact (this is an important problem due to the large surface area needed to house the large quantities of propellant), docking and maintenance hazards, and hazards associated with extended extravehicular activity. Various safety analysis techniques were presented for each program phase. Specific system safety implementation steps were also listed. Enhanced risk assessment was demonstrated through the incorporation of these methods.

DEVELOPING A SAFE ON-ORBIT CRYOGENIC DEPOT

The National Aeronautics and Space Administration (NASA) currently has new U.S. space initiatives to develop piloted lunar and Mars missions. Central to these programs are orbital transfer vehicles (OTVs) and extensive cryogenic propellant storage facilities operating in Earth's orbit. It is known from *Stubbs et al.* (1987) that large quantities of cryogens, such as liquid hydrogen and oxygen (on the order of 200,000 lb for geosynchronous Earth traffic and 400,000 lb for lunar traffic), require the advancement of on-orbit cryogenic propellant storage technology.

A NASA On-Orbit Cryogenic Depot Technology Task Force is presently studying the various concepts. The definition stage is sufficiently prefatorial that the exact purpose of the depot has yet to be defined. Its primary function is to fuel OTVs. However, secondary functions and modes of completing the primary function have not been determined. Primary functions of the depot will include propellant storage, acquisition, expulsion, conditioning, refill, measurement and control, thermal control, venting, data/communication, inspection and diagnostics, and vehicle proximity operations. All these functions will demand unique systems creation. Technology development requirements for the depot must be identified and solved prior to full-scale deployment.

Several options have been proposed for the propellant depot and maintenance facility. These include (1) a single OTV maintenance facility with refueling capability attached to the space station, (2) a space-station-attached maintenance facility and separate co-orbiting cryogenic propellant depot, and (3) a co-orbiting OTV maintenance and propellant storage platform. The task force is currently strongly pursuing the second option, the attached servicing facility with co-orbiting propellant depot.

Now is an opportune time to seriously develop a safe OTV cryogenic depot. The inherent hazards of the above-mentioned options are considerable. Even though the task force is studying the second option more seriously than the others, a comprehensive system safety effort must be expanded in tandem with technology and trade studies.

Failures of the cryogenic propellant depot would not only affect the facility operators, but may possibly damage the space station. Loss of the depot would severely affect the mission and could cancel the program. If all the fuel were lost at a critical path point, new launch windows (for refueling both the depot and planetary spacecraft) would have to be established. Questions regarding man-tended (or partially man-tended) vs. automated operations must be addressed. The proximity of the depot to the space station is of critical importance. The magnitude of an explosion of 200,000 lb of liquid hydrogen and oxygen could directly affect the space station.

There are numerous depot configuration trades that must be analyzed. One such issue that has been suggested is the utilization of tethers to facilitate and simplify propellant transfers. However, the safety implications are profound; the less automated the system, the greater the human risk. Engineering optimization is fundamental to realizing an efficient and cost-effective system. Another important issue is growth potential, which is key to expanding NASA's dynamic mission capabilities. This well illustrates the need for continual system safety analysis. Any small change in this complex system could negatively affect the system.

Safety trade-offs for efficacious operations will not enhance the overall and continual use of the depot. Because hazards may not be readily apparent, an ongoing safety effort is needed to bring problem areas to light. The results of a serious risk assessment will positively contribute to a viable technology trade-off decision. The purpose of this paper is to show how and where system safety can be applied to develop a safe cryogenic depot.

[1]Now at Hernandez Engineering, Inc., Commerce Center II, Suite 305, 7601 Ora Glen Drive, Greenbelt MD 20770

SYSTEMS LIFE CYCLE OF THE CRYOGENIC DEPOT

The essential factor in governing a congruous safety effort is to be intimately involved in the entire cryogenic depot program. The way for system safety to become an integral member, from conception through deployment, is to participate as a working member (with equal status and voice) in the following program phases: (1) concept; (2) definition (flight experiment definition and analytical models development); (3) development (pathfinder, technology demonstrator design and testing, prototype hardware design and testing, and final development); (4) production; (5) deployment (space transport system (STS) use and depot amplification) (Fig. 1).

INTEGRATED SYSTEM SAFETY FOR THE CRYOGENIC PROPELLANT DEPOT

Cryogenic Depot Technology Requirements

Various planned programs impel the cryogenic depot development. The significant mission drivers are manned Mars, manned lunar, robotics exploration, and planet Earth (*Ride,* 1987). These drivers have various technology requirements.

Technology requirements are abundant and fall into general categories of fluid storage, supply, handling, and transfer; advanced instrumentation; and materials and structures. A partial listing of technology requirements identified to date includes cryogenic fluid resupply; reusable Earth-to-orbit cryogen transport; long-term orbital cryogen storage; control, instrumentation, and diagnostics; fluid thermodynamic analytical models (chilldown, vapor liquefication, vent characterization, etc.); pressure control techniques for long-term storage; zero-gravity fluid quantity gauging; mass measurement accuracy (expulsion and refill); quick disconnect; fluid leak operations/detection; fluid venting/dumping; thermodynamic vent; refrigeration requirements; fluid motion effects on controls; pretransfer conditioning of receiver vessel (chilldown, ventdown, purge, etc.); nonvented receiver refill; transfer line conditioning; storage loss reduction; and material development (*Stubbs et al.,* 1987).

Many of these technology development requirements are high risk, both in terms of technology payoff and system safety significance. Many must be demonstrated in orbit since the technologies and analytical models cannot be validated in Earth's gravity. Each one of the requirements has a potent system safety implication. Only through a well-defined and integrated system safety effort can the issues be appropriately understood.

Technology Development

To safely develop the appropriate technology, program considerations should be analyzed. NASA has identified three main technology considerations that must be addressed: mission, manufacturing, and performance (*Davis et al.,* 1970). System safety studies should be conducted for all of them. System concerns are discussed below.

Safety Task	Concept	Definition	Development
1. Develop system safety plan	Initial	Final	----------
2. Conduct hazard analysis	PHA	PHA/FTA	FMEA/OSHA/FTA
3. Define safety design requirements	Initial	Final	Final
4. Conduct failure analysis	Historical data review	Historical data review	Test results
5. Conduct risk analysis	Preliminary risk assessment	Update risk assessment as new material becomes available	Update risk assessment as new material becomes available
6. Conduct safety test	----------	Flight definition tests and path finder tests	Pathfinder/technology demonstrator and prototype hardware
7. Conduct safety training	----------	----------	Support

Production	Deployment
----------	----------
OSHA	Update hazard analyses
----------	----------
Update database	Update database
Update risk assessment as new material becomes available	Update risk assessment as new material becomes available
Hardware qualification tests	----------
Monitor	Monitor

Fig. 1. System safety tasks. Safety tests should be both ground- and on-orbit tests. PHA: Preliminary Hazard Analysis; FTA: Fault Tree Analysis; FMEA: Failure Mode and Effect Analysis; OSHA: Operating and Support Hazard Analysis. From *Roland and Moriarty* (1983).

Mission considerations.

Operational pressure: Cryogens may be stored as single phase (supercritical) or two phase (subscritical). It appears that NASA is supporting the subcritical storage system over the supercritical.

Quantity measurement: The accuracy of quantity is paramount for operational use and system diagnostics. Quantity measurement with a subcritical system is much more difficult than with a supercritical system; the liquid-vapor mixture involves a more complex measurement media. NASA is currently developing subcritical cryogen (for anhydrous ammonia) measuring devices for the space station.

Pressure control: A subcritical system may undergo pressure instabilities (including boiloff). If the depot is hard-fixed to the space station, vapor releases may cause small perturbations, affecting space station experiments and possibly polluting the outer skin of the station. Thermal stratification also may affect pressure control.

Manufacturing considerations.

Reproducibility: Manufacturing repeatability and accuracy for system operation is critical for mission success.

Shelf life: The depot has a designated shelf life of 10 to 20 years.

Weight: Launch costs and weight, especially for a 200,000-lb to 400,000-lb fluid, dictate optimal design.

Materials: They must be compatible with the environment (of both deep space and the fluid media itself) and have high strength-to-weight ratios. Some of the major material concerns are fracture toughness, fatigue properties, chemical properties, permeation, creep properties, embrittlement, and joint efficiency.

Envelope constraints: Depot (whether attached, tethered, or completely autonomous to the space station) interfacing mechanisms will influence the physical and structural design parameters.

Performance considerations.

Standby time: The dormant period between use and nonuse is important. Cryogen residue in the line can vaporize and cause a pressure barrier when fuel is extracted in the next run.

Fluid quantity: The quantity cannot be accurately determined until the depot purpose has been more clearly delineated.

Power requirements: Power requirements for pumps, fans, and diagnostics, are contingent on fluid usage requirements.

Environmental conditions: Temperature variations, due to thermal cycling, will significantly affect thermal and thermodynamic design. Micrometeoroid and space debris impact also are important for design.

METHODOLOGY FOR SYSTEM SAFETY

To fully support each phase of the system life cycle, various system safety techniques can be exploited. Most of these methods should be used for every serious technology option. The choice of system safety analysis depends on the program phase and level of developmental detail. Each one of the methods has been successfully proven on numerous NASA, Department of Energy, Department of Defense, and Nuclear Regulatory Commission projects. The most common methods are listed below with a brief description of each safety tool and program phase application. It is not within the scope of this paper to go into in-depth explanations of each analysis technique.

Preliminary Hazard Analysis (PHA)

The PHA is the base-line document for the integrated system safety effort. The word "preliminary" denotes first hazard search of the system. The analysis addresses the major hazards of the system and allows early tracking of problem areas. The initial PHA is not to affect control of the hazard (this will come later in the program life cycle with other techniques), but rather to provide management with knowledge of potential risks for feasibility studies and program definition activities. Tradeoff studies are greatly enhanced with the hazard identification method of the PHA, allowing establishment of design and procedural requirements, to eliminate or control hazardous conditions before the system becomes so advanced that design changes become prohibitive in terms of cost. The PHA is most frequently used during the concept and definition program phases.

Subsystem/System Hazard Analysis (SSHA/SHA)

The SHA (the format and use are exactly the same for the SSHA) is an inductive method of analysis. Interest is focused on system-level design features that may affect overall performance or safety. Special interest is concentrated on interface considerations. System information is then used for the integration of the full system hazard analysis. The analysis is usually conducted during system definition and development phases.

Operating and Support Hazard Analysis (OSHA)

The focus of the OSHA is on system operation. Analysis emphasizes human factors engineering and operating conditions. Areas considered are use of safety guards or devices, special procedures or training, and identification of timing of operations or functions and other ergonomic concerns. The OSHA should be initiated early enough in system development for technical input. However, the technique is very useful in the development phase as an overall safety verification.

Fault Tree Analysis (FTA)

The FTA is a powerful deductive analytical tool. The method employs a Boolean logic model that mimics the relationship between events in a system. The final outcome is called the top event. Even though the method is called fault tree, the top event may be either a desired or undesired outcome. This safety and reliability tool is very useful in the early design phases and in studying operational systems. The output may be of a quantitative or qualitative nature, depending on the input information.

Failure Mode and Effects Analysis (FMEA)

The FMEA is sometimes called a failure mode and effects and criticality analysis (FMECA). Though this is primarily a reliability tool, the analysis does furnish much useful information. The FMEA focuses on single-point and piece-part failures and their propagation effects through the system. The technique tends to concentrate primarily on component failure instead of human error.

Other tools frequently used in system safety are change analysis, human factors analysis, common cause failure analysis, training, audits, and mishap investigations.

Because the PHA, OSHA, and SHA are all very similar, frequently they are grouped into a comprehensive hazard analysis. This

would require that the hazard analysis be updated at program milestones to incorporate operational (and human factors) and system hazards.

Sequence of Hazard Control

It is of importance to remember that risks always exist. The only way to mitigate the hazards is to control them; the use of the sequence of hazard control is the optimal method. The following are important in applying the sequence of hazard control activities: design for acceptable hazard, use of safety devices, use of warning devices, and finally, the use of procedures and training.

Design for an acceptable hazard means to minimize through design methods the hazardous condition. For example, if heat is an added hazard to loss of cryogen control, then one should try to design without the need for external heating. Another example is the use of separate quick disconnects for oxygen and hydrogen cryogens. If incorrect mating is made impossible by separate, incompatible disconnects, then the risk of mixing fluids by incorrect connection is alleviated.

Safety devices are additions to the system to control the hazard. The best example is a pressure relief valve on a cryogen storage vessel. The hazard of tank rupture is always there, but mitigated through the relief system.

Warning devices are used to alert personnel and machinery to impending danger or harm. The purpose of the warning device is to prepare personnel and machinery for an emergency contingency. Gas and leak detection devices are good examples of this.

Procedures and training are the least successful of the sequence elements. Because people are fallible, it is always best to try to control the hazard by hardware design methods. People tend to reach a 50% error rate during highly stressful situations. Even though the operator may be well trained in transferring cryogens to the OTV, the operator is unlikely to perform as well during an emergency situation. The same well-trained operator may also fail during normal operations due to unforeseen stresses such as personal problems, physical distances between operating devices, unusual environmental conditions, tedious tasks, etc.

Risk Assessment Hierarchy

Risk analysis and control are the ultimate goals of system safety. Various techniques, applied during different phases of the life cycle, will achieve that goal. However, to adequately assess and manage the risks, hazard severity and probability of occurrence must be studied. Each of the analyses allows for hazard severity and probability identification. When the hazard is identified, a severity and probability is assigned. This permits one to classify the hazard. A matrix gives an overall risk assessment code. The decision maker now has something tangible to review for trade-off studies or system changes.

It is best to try to be quantitative whenever possible. However, inaccurate or ambiguous numbers can lead to invalid risk assessment. Probability numbers are easily attainable for series-manufactured items or items with a large historical or scientific database. To use quantitative probability analysis for state-of-the-art hardware, in outer-envelope design conditions, is both misleading and dangerous. Therefore, one is forced to assign a qualitative designation for probability of occurrence. An example of a qualitative risk matrix is shown in Table 1.

TABLE 1. Risk assessment code (RAC) matrix.

	Probability Estimate			
Severity Class	A	B	C	D
I	1	1	2	3
II	1	2	3	4
III	2	3	4	5
IV	3	4	5	6

RAC 1: Considered imminent danger; requires immediate attention and initiation of abatement procedures.
RAC 2: Considered serious and requires priority attention.
RAC 3-6: Considered nonserious; however, a priority ranking is established for corrective measures.

Severity Classification

I.	Catastrophic	May cause death or major system destruction.
II.	Critical	May cause severe injury, occupational illness, or major property damage.
III.	Marginal	May cause minor injury, minor occupational illness, or minor property damage.
IV.	Negligible	Probably would not affect personnel safety or health, but is a violation of specific criteria.

Qualitative Probability

A.	Likely to occur immediately.
B.	Probably will occur in time.
C.	May occur in time.
D.	Unlikely to occur.

System Safety Implementation

In order to implement system safety into the program, it is necessary to have a safety representative as a permanent member of the task force. That person must not only have equal status to the other members, but must also be a participant. The representative will be charged with ensuring that all viable safety concerns are addressed and acted upon. An integrated system safety program is only useful if the system safety engineers have adequate power to confirm that safety issues are not only identified and resolved, but, more importantly, that controls are put into place.

A system safety review panel, comprising technical experts, should be established to review trade-off studies and decisions. The knowledge and experience of technical experts at this management level would be utilized to the fullest in order to appropriately review system safety analyses. System reports will be generated by the system safety engineers on each of the various design, analysis, and development teams. The system safety engineering reports emanating from this level must be highly technical and comprehensive. To ensure adequate decision making, the review panel must be equally qualified.

The design, analysis, and development teams will have the most knowledgeable engineers for a particular component, system, or concept. If system safety engineers are not thoroughly integrated on these teams, investigation and research decisions will be made without adequate system safety engineering input.

Because an orbiting cryogenic depot is extremely complex, safety is critical. Unfortunately, pertinent safety information is lacking. The technology is sufficiently new that a system safety database has not been established. A special safety test program and test bed may be required to validate trade studies and create

the database. The primary purpose of this safety test program and test bed would be to investigate safety implications of various technologies in a highly structured and scientific manner. Numerous safety-related scenarios could be investigated before final design acceptance. To provide a cost-effective safety test program, the test bed need not be specially built. Many hazard potentials could be researched in the same test beds as the actual chosen hardware. Only certain destructive tests require remote facility testing (i.e., at NASA White Sands Test Facility). Because of the unique difficulties with zero gravity, some tests will need to be conducted in orbit—not only flight definition tests, but also an orbital subscale test bed (*Schuster et al.,* 1987).

Some Identified Top-Level Hazards of the Cryogenic Depot

Even though the OTV depot is still in the conceptual phase, many generic hazards are readily apparent. A private-sector-company PHA was conducted on various prephase A conceptual alternatives (*Aerospace Corporation,* 1971). Some of those hazards, along with other identified hazards, are fire/explosion, environmental and thermal, mechanical (vibration shock/acoustic), pressure, impact, biological (toxicity), electrical, and human factors (operations), and are discussed below. The generic hazards can be divided into various groups. Please note that this list will expand as the system is more clearly defined.

Fire and explosion are the most serious hazards. Improper mating of oxygen and hydrogen systems, thus allowing the incompatible fluids to mix, can cause an explosion. Another hazard is the rupture, or leakage, of a common bulkhead oxygen and hydrogen system. Because this system is being considered by NASA, a trade study investigating the safety concerns of common bulkhead vs. modular tank design would be interesting. A line or disconnect rupture during transfer operations may release sufficient propellant, causing a fire or explosion. In designing the depot one must assure that ignition is eliminated by preventing pneumatic impact on certain soft goods in oxygen lines.

The most obvious hazards are due to long-term environmental effects. The probable life cycle of the depot will be 10 to 20 years. During the entire life cycle, extreme thermal conditions will affect the depot. This creates heavy thermal loading and fatigue. There are not only thermal cycling problems associated with the cryogen (and its thermal stratification), but also the temperature variances of space. It is obviously not convenient to have the depot receive direct solar radiation. Space vacuum conditions will require careful design. Long-term vacuum, thermal, and radiation degradation of thermal coatings and mechanical components are significant concerns. Material selection and design strategies will be a key factor in confronting this problem. One probable temperature variance concern is the growth and shrinkage of components. Currently there are few data on the effects of large cryogenic storage systems submitted to long-term space environments.

Because of the large surface areas required, coupled with the vacuum environment, the area surrounding the storage facility could be a major heat sink for the cryogen. Adequate insulation around the storage tanks would be needed to prevent heat transfer in either direction. Another possible problem would be how noncondensible gas is purged from the system. The noncondensible gas is a potential hazard for pump cavitation. Studies should also investigate the effects of inadvertent dumping of large quantities of cryogens into Earth's orbit. Not only the combustible hazard, but also the pollution hazard is of concern.

Mechanical-related hazards are a significant category. Vibrations from pumps or other sources, in tandem with normal duty cycles, can cause serious mechanical fatigue problems of components or structures. Another important hazard is the lock-up of the deployment mechanism in either an unlatched, latched, or partially latched position. This immediately compromises the mission capability. Docking integrity will need to be studied thoroughly when a docking mechanism is defined.

Pressure system integrity is critical in the cryogenic system. Normal venting (or burping) would be made difficult if the depot is attached to the space station. Leakage could be catastrophic in this system. A transfer line leakage during active pumping could cause a high overboard dump rate with propellant possibly momentarily residing near the depot, producing a potentially combustible situation. Uncontrolled transfer line boiloff during transfer may cause pressure surges. A loss of pressure can lead to low net pressure suction head to the transfer pumps. Propellant leakage is not only a safety hazard but also a mission hazard. Small leak rates are critical due to the time and expense needed to launch and refuel the depot.

Cryogenic vessel overpressurization is a catastrophic hazard. An overpressurization may be caused by a water-hammer effect during transfer. If a runaway pumping situation exists, then the result could be loss of the pressure vessel. Failures in the propellant quantity measurement device can cause the system to be hardfilled. Ullage problems and thermal stratification may be handled by some type of system rotational or linear acceleration and fluid mixing. These added features introduce potential problems, such as overspeeding of rotational thrusters, thruster gas impingement on the depot, overspeeding of mixing fans, etc.

Approximately 7030 man-made objects are currently in orbit around the Earth. The majority of these tracked objects are from spacecraft breakup or explosion. There was a 10% increase in 1987 (*Johnson Space Center,* 1988). The inherent hazard caused by this situation is the problem of ancillary equipment impact. Depot and OTV dockings are risks themselves. Although NASA has a successful history of low-impact docking, study is needed to map out techniques for docking and rendezvous for this configuration. Gas impingement from the OTV on the depot would be catastrophic. Other impact sources are extravehicular activity (EVA) crewmember, EVA retriever robot, tools, and any other structural device that may be placed in this orbit. Micrometeoroids are another evident hazard. Pressure vessels holding 200,000 lb of oxygen and hydrogen will be very susceptible to this danger. High pressures and large surface areas considerably increase the hazard and risk.

If a cryogenic spill does occur, care must be taken to ensure that crewmembers do not introduce contaminated EVA suits or equipment into the space shuttle, space station, or OTV. Spilling of cryogens on equipment might also damage or affect the reliable operation of that hardware.

Electrical shocks are another hazard group. Improper electrical design or subsystem power surges may create problems. The danger is not only shock to personnel, but also damage or interference to equipment. Arcing at electrical interfaces is a potential hazard to crewmembers, and also may cause a fire or explosion. Arcing sources can originate from a variety of foci: EVA, OTV docking (or docking mechanisms), electric pump motors, and instrumentation and controls. Other radio signals from nearby orbiting spacecraft may affect delicate electronic signals.

Operational hazards (or human factors) add to the list. The use of incorrect procedures and ergonomically poorly designed machinery may cause problems. Emergency evacuation (from the depot area) options must be studied to verify that optimal personnel protection is always maintained.

CONCLUSIONS

The use of system safety techniques, applied in a carefully designed, methodical form, is the most effective avenue to enhanced system risk assessment and control. However, to efficiently engender safety, an integrated system safety approach must be used. The cryogenic propellant depot is at an optimal point in the program for safety to become involved.

The comprehensive system safety approach requires that system safety engineers become intimately involved in the program at all levels. Because the cryogenic depot is now at the prephase A conceptual stage, it is an opportune time to apply an active system safety participation. The system safety engineer must share in the conceptual and definition trade studies. Development of hardware, from pathfinder prototype, and then final flight article, requires safety cooperation.

Various technology requirements have already been identified for the cryogenic depot program. Though the conceptual development has not really begun, system safety can help in reviewing and investigating each technology. The safety effort is then led into the logical progression of technology development participation. Enhanced risk assessment requires that system safety supports three major areas: mission, manufacturing, and performance considerations. Consideration areas must address, and safely control such things as operational pressure, quantity measurements, manufacturing requirements, and environmental conditions.

System safety has well-developed and time-proven technologies that will further good risk assessment. Different analysis methods are applied at all stages of program development. The techniques have been used successfully on programs in the nuclear, chemical, and aerospace industries. Some of the appropriate methods to be used are preliminary hazard analysis, system hazard analysis, operating and support hazard analysis, fault tree analysis, and failure modes and effects analysis.

These safety tools will identify hazards and help categorize them for applying the sequence of hazard control. Optimum hazard control is through design, the least effective control is through procedures and training. The hazard criticality, coupled with probability of occurrence (though both may be qualitative), betters risk assessment and control.

System safety tools are meaningless if system safety is not an integral part of the team. The system safety engineer must be a working member (with equal status and voice) on design, analysis, test, manufacturing, and deployment teams. An independent system safety review panel, comprising technical experts, should ensure the objective and autonomous verification needed before deployment.

Although the depot is in a preconceptual phase, various generic hazards have been identified. The significant hazard categories are fire/explosion, environmental/thermal, mechanical, pressure, impact, biological, electrical, and operational.

The above-mentioned safety techniques, applied at the appropriate program phase, will explicate the hazards and verify the controls, thereby developing a serious and comprehensive risk assessment and control program. The cryogenic depot is replete with inherent hazards. A safe on-orbit cryogenic depot can be designed if an integrated system safety approach is applied.

REFERENCES

Aerospace Corporation (1971) *Orbiting Propellant Depot Safety, Vols. 1-3.* Aerospace Report No. ATR-71 (7223)-3. El Segundo, California.

Davis M., Allgeier R., Rogers T., and Rysavy G. (1970) *The Development of Cryogenic Storage Systems for Space Flight.* NASA Office of Technology Utilization, Washington, DC.

Johnson Space Center (1988) *Johnson Space Center Research and Technology Annual Report 1987.* NASA TM-100463. 106 pp.

Ride S. (1987) *Leadership and America's Future in Space; Report to the Administrator.* NASA Headquarters, Washington, DC. 63 pp.

Roland H. E. and Moriarty B. (1983) *System Safety Engineering and Management.* Wiley, New York. 339 pp.

Schuster J., Brown N., and Hueter U. (1987) *Evaluation of Cryogenic System Test Options for the OTV On-orbit Propellant Depot.* 22nd Thermophysics Conference. AIAA-87-1498. American Institute of Aeronautics and Astronautics, New York.

Stubbs R., Corban R., and Willanghby A. (1987) *On-Orbit Fuels Depot Technology Roadmap.* NASA Lewis Research Center, Cleveland, Ohio.