Threat-Strategy Technique: A System Safety Tool for Advanced Design

R.L. Peercy Jr.* and R.F. Raasch†
Rockwell International, Downey, California

Although definitions of system safety analysis techniques are relatively mature, several innovations were found to provide a significant enhancement to space station safety. There are a finite number of threats to which a project or program can be exposed (in the case of the space station, a total of 23 were identified). Threats may be grouped as simple or complex according to the physics of their causative factors. Threats may also be grouped as natural, configuration-oriented, and operationally induced. Fire and its causative factors are examined in some detail with proposed countermeasures for each factor. The countermeasures taken to mitigate each threat should be planned early in the development cycle. The aggregate of these countermeasures is termed "the strategy" for each threat. In addition, since solutions or strategies may be simple or complex, based on the causative factors, optimum solutions depend on selecting those strategies that have synergistic properties which minimize the risks associated with the strategy chosen. The strategy for the threat of fire also minimizes the threat of explosion and toxic contamination of the space station atmosphere.

Background

SAFETY approaches to risk assessment vary with the program type, its dynamism, and sensitivity. Space Shuttle hazard identification approaches consisted of the techniques shown in Table 1, which have been characterized in terms of strengths and limitations. In general, these approaches summarize the major safety analysis techniques that were state-of-the-art in the early 1970s. However, these techniques are applied after requirements definition; consequently, vehicles thus developed tend to contain a greater quantity of hazards or accepted risks than if this effort had been integral to, and early in, the design cycle.

Fifteen years of accumulated space station conceptual assessments are currently being evaluated by NASA for an initial operational capability during the early 1990s. A technique of examining the potential solutions to families of risk-generators or "threats" was created, in part, to integrate the wealth of America's lessons learned in manned space early in the station design and operational planning process. The threat—often referred to as a hazard group—forms the basis for most discrete hazards. It was found that crew safety threat considerations formed a very significant contribution to configuration and operational definitions. A threat and its relationship to hardware design and operational considerations is defined below.

Definitions:

Hazard: The presence of a potential risk situation caused by an unsafe act or condition.[1]

Threat: Situation that endangers either the crew or the space station or STS Orbiter.

Potential threat: Threats that might arise, without regard to probability, frequency, or severity.

Potential hazards: Threats that have been determined to have a combination of probability, frequency, and/or severity for a given scenario and that must be dealt with and appropriately resolved.

Components of a threat: 1) mission scenario, 2) configuration/mechanization-oriented hazards, 3) operational mode.

The threats that are considered applicable for the space station are (the first eight are the principal design drivers): 1) fire, 2) biological or toxic contamination, 3) injury/illness, 4) explosion/implosion, 5) loss of pressurization, 6) radiation, 7) meteoroid penetration, 8) debris, 9) leakage, 10) tumbling/loss of control, 11) grazing/collision, 12) corrosion, 13) mechanical damage, 14) out-of-control intravehicular/extravehicular astronaut (EVA), 15) inadvertent operations, 16) lack of crew coordination, 17) abandonment of space station, 18) stores/consumables depletion, 19) structural erosion, 20) orbit decay, 21) loss of access to a hatch, 22) temperature extremes, 23) free orbit (EVA astronaut).

Introduction

The purpose of this paper is to describe a technique of identifying threats (or hazard groups) and developing candidate solutions while addressing the corresponding elements of risk attendant to these threats. Three key points are considered significant: First (philosophy): "how much safety is necessary?"; second: "what are the threats that the program must deal with?"; and third, "what are the strategies and interdependence of these strategies developed to deal with the threats?" The interrelationship of these key points is logically illustrated in Fig. 1. There are a number of options for the philosophy of design and operations (Table 2). Of course, the most desirable philosophy option is the first entry in Table 2 or a completely safe option that allows no damage whatsoever to the space station or injury to the crew. At the other extreme is a candidate philosophy that considers crew survival at the expense of the space station. This candidate philosophy, in essence, assumes one would be willing to entertain routine planned evacuation from the station by the crew. Using this philosophy also implies that evacuation and rescue may be acceptable design or operational solutions. Due to the program objective of a planned, permanent, productive presence of man in space, the middle philosophy was chosen for a low-Earth-orbit station. Although it is not uniquely a safety definition, it appears to be the most compatible with the national and international space station objectives. The philosophy chosen as a baseline is "no event would cause an injury to the crew or damage to the station that would result in complete suspension of operations." The threats listed above contain

Presented as Paper 85-0397 at the AIAA 23rd Aerospace Sciences Meeting, Reno, NV, Jan. 14-17, 1985; received Feb. 4, 1985; revision received Sept. 23, 1985. Copyright © American Institute of Aeronautics and Astronautics, Inc., 1985. All rights reserved.

*Manager, Reliability and Safety, Space Transportation Systems Division. AIAA Associate Fellow.

†Senior Engineering Specialist, Space Transportation Systems Division.

Table 1 Strengths and limitations of typical hazard analysis tools and techniques

Technique	Strength	Limitation
Fault tree analysis	Pictorial display of the safety attributes considered and their interrelationships Identifies weak points ("or" gates) in the system Early identification of operational constraints Can be computerized for quantification probability prediction	Effectiveness dependent on ability to select top-line hazard Limited in use below the black-box level Difficult in multiple-redundancy systems Difficult for the unindoctrinated to supervise Long lead time analysis tool
Checklist	Can be done at any phase of program High visibility technique Low cost for cursory preliminary hazard analysis	Does not accommodate subtle interface/synergistic issues Accounting tool only Tends to give rosy picture and customer false sense of security Totally inadequate if not supported by in-depth technical analyses for each entry
Sneak circuit analysis	Ties subsystem circuits together, identifies nonfailure incompatibilities Inductive logic instead of deductive Excellent for change evaluations if system is baselined	Long lead time procurement Limited sources of technical expertise Highly specialized personnel Costly, except when limited to critical functions
Failure mode and effects analysis (FMEA or FMECA)	Most thorough and systematic of the analytical tools May be computerized/mechanized for diagnostic activities (trouble-shooting of a given symptom) Leaves excellent record of potential failure consequences Effective for multiple redundancy when screen is used	Configuration-(hardware) oriented Will generally give an optimistic response since operational decisions tend to limit full capability of hardware Voluminous documentation Addresses internal system only
Hazard analysis	Looks at multiple configuration and safety attributes other than failure modes Addresses internal and external systems When done in concert with nontradeable safety requirements, will drive design solutions Provides documented history of risks that have been accepted by program management	Configuration-oriented Unless strongly regimented, safety analyst may tend to reflect his area of specialty Lack of uniformity
Mission phase hazard analysis	Effective in identifying hazards experienced in operational situations Analytically superimposes assumed operational condition upon configuration design solutions and flags problem areas Rapid response time Has provided greatest payoff for effort expended; includes all factors contributing to hazard Addresses total system	Needs other ancillary analyses for optimum benefit Techniques limited by capability of experts Must be maintained as a living baseline

the spectrum of those arising from several station configurations, a multitude of operational scenarios, and considers both manual and automated modes of operation.

The technique used to control a threat is to identify a strategy or group of strategies that will be effective in eliminating or mitigating the threat. An effective hazard-reduction precedence, used on the Space Shuttle,[1] consists of the following sequence of hazard mitigation actions: 1) design to preclude, 2) design to control, 3) provide protective devices with operational work-arounds, or 4) define risk and conditions for acceptance. Each of these steps of hazard reduction, as applied, drives one or more threat mitigation strategies.

Approach

Threats may be categorized as simple or complex based on the physics of their causative factors. For example, a simple threat such as depressurization of the habitable volume could result from a cabin puncture or a leaking component, e.g., vent valve. The strategy to ameliorate a simple threat is usually straightforward. For the cabin puncture issue, atmospheric revitalization system design capable of making up

Table 2 Space station safety philosophy precedence (how much safety?)

Current options	Comments
Cause no damage whatsoever to space station and no injury to crew	Desirable: cost trade
Cause no damage to space station beyond routine maintenance capability	Cost trade
Cause no damage to space station or injury to crew that will result in a complete suspension of operations	Baseline philosophy
Space station repairable and operational within a specified time period	May require escape/rescue
Crew survival at expense of the space station	Implies evacuation and rescue as a minimum

Table 3 Strategy development for the threat of fire

Threat	Causative factors	Strategy(ies)
Fire	Fuel/oxidizer/ignition sources coexist (ground and space habitable areas)	Exclude two of the three elements When two elements are present, inert Materials controls
	Fuel/oxidizer/ignition sources/ temperature/pressure coexist (space nonhabitable areas)	Exclude three of the five elements Materials control
	Catalytic reaction	Inert environment Control surface temperature Materials control
	Chemical reaction	Inert environment Materials controls Extinguishing agents
	Ignition sources (electrical/electrostatic)	Proper grounding/bonding Wiring controls Proper circuit protection Isolation of circuits from combustible materials Material selection

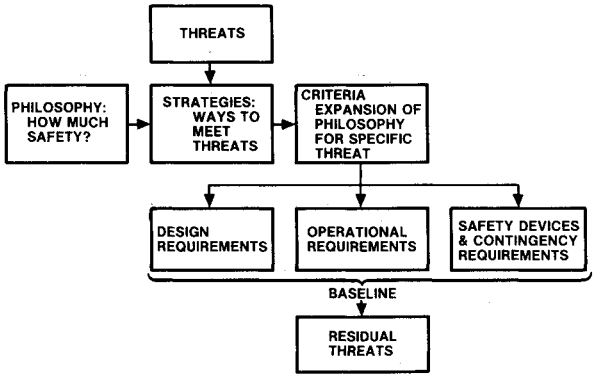

Fig. 1 Threat-strategy development.

pressure losses for the largest credible puncture, coupled with the capability of puncture detection and repair within an acceptable time limit, adequately addresses this issue.

Table 3 illustrates fire, a complex threat.[2] Its complexity arises from the numerous causative factors and synergistic considerations associated with each. The causes of fire are various and diverse and fire is one of the most feared threats in space environment scenarios. The strategies to mitigate each group of causes are seemingly unrelated. However, taken as a whole, each strategy element is a basic building block for the system design and operational requirements agenda. Although a number of causative factors and several corresponding strategies are identified in Table 3, this is not an all-inclusive list; there are other causative factors and attendant strategies (for example, among the issues that are not addressed is the special case of firefighting and fire-suppression considerations).

Consider the first entry in Table 3, which is perhaps the most simple cause of fire. To illustrate the strategy, visualize a fire triangle consisting of fuel, oxidizer, and an ignition source. Generally, one is safe whenever one leg of a fire triangle is broken. In the case of the Space Shuttle, it was part of the fail-safe design philosophy to break two legs of the fire triangle so that should another leg occur as the result of a failure, the vehicle would still be safe. This means that the vehicle was always fail-safe so that if fuel exists, oxidizer and an ignition source are excluded, etc.[3] (If two of the elements exist, then there are other methods of providing safing, such as inerting.)

However, exposure to any leg of the fire triangle begins to define discrete hazards (i.e., fire/explosion of vented battery effluents). It should be noted that the generic issues always deal with the parent threat, whereas control of hazards may have only local impact. This approach to risk assessment assigns threat definition and impact as precursors to system/program requirements definition.

Another option that is available here is the judicious selection of materials. If proper care is given to the selection of materials, problems can be reduced significantly. Particularly important is the requirement that flammable materials or fluids are minimized for use within a habitable area.

Added considerations for materials for manned habitable volumes for space usage are shown below.

1) All Orbiter materials (metallic and nonmetallic) are analyzed, controlled, approved, and recorded via material analysis and tracking control to assure compatibility.

2) Compatibility of materials/fluids with systems and fluid leakage past single barriers within the system are compatible.

3) Compatibility of materials exterior to the system with natural environments such as humidity, sand, dust, salt spray, etc.

4) Materials flammability, odor, and offgassing characteristics.

5) Materials criteria considerations: stress corrosion, galvanic corrosion, heat treatment, impact ignition, catalytic reaction, degradation, thermal vacuum stability, moisture/fungus resistance, etc.

6) Materials compatibility with unnatural (induced) environments such as fluid leakage exterior to the system being evaluated.

It is interesting to note that material controls is a portion of each strategy and must be defined prior to system development. Failure to do this will result in a myriad of hazards, each with patchwork fixes distributed throughout the program. Table 4 illustrates, from Shuttle Orbiter experience, how fluids usage is controlled and compartmentation is applied to eliminate risks in evolving designs. In addition to the basic elements of the fire triangle, there are two added parameters for consideration in spacecraft design. These are pressure and temperature, which modify the fire triangle into a "fire penta-ring" when on-orbit operations are a design consideration. [The attributes of a threat can vary with different ambient environments. The classical fire triangle (fuel-oxidizer-ignition) in 1 atm differ from an orbital situation where the normal ambient conditions include low pressures and low temperatures. By expanding this triangle to a fire/explosion penta-ring (adding pressure and temperature), the contributions of these two physical characteristics provide additional options for control of fire and explosion.]

Some of the strategies used on the Shuttle as methods of counteracting the particular threat of fire are shown in Table 5.[3] The first line of defense is "design to preclude." It should be noted that, for a complex threat, the solution is generally complex; in the case of fire, the issue is not the fire itself but rather dealing with the causative factors, such as the ignition sources, fuels, and oxidizers. Another point of significance is that there is not one simple solution, but rather a family of solutions. Some approaches to preclude fire may be very helpful in controlling some of the other threats shown in Table 5. This is not always the case, and some of the solutions in controlling threats have just the opposite effect. In these cases, steps to control a given threat may have an adverse consequence to another threat. Caution must be exercised to assure that the solution to one threat will not create a worse situation for other threats.

The second line of defense against fire is "design to control," also shown in Table 5. In essence, what this presumes is that the "design-to-preclude" strategy was not 100% effective. If it is assumed that a fire will occur, some of the options are shown in this figure, such as building compartments. (There are a number of compartments on the Shuttle Orbiter that are there solely to deal with fire and/or toxicity.) Other lines of defense deal largely with detection, method to extinguish a fire, and firefighting.

Table 4 Orbiter compartmentation fire-toxicity control criteria

Compartment	Operational fluids normally present	Zone[a]	Maximum allowable surface temperature to prevent an ignition, °F[d]
Nose sphere	None	I	—
Forward reaction control subsystem	N_2O_4, MMH, He	II	352
Nose gear well	Hyd fluid (83282 & 5606)		
Forward module plenum	Hyd fluid (83282), H_2O	III[b]	352
Window cavities	None		
Star tracker cavity	None		
Midfuselage	LH_2, LO_2, hyd fluid (83282), MMH, He, N_2O_4, F21, H_2O, N_2, FC40[c]		
Crew module	N_2/O_2, GO_2, Halon 1301, H_2O	IV	—
Wing leading edge (L&R)[e]	None	V, VI	—
Wing box (L&R)	None	VII, VIII	423
Main gear well (L&R)	Hyd fluid (83282&5606)		
Wing/elevon intercavity (L&R)	Hyd fluid (83282)		
Aft fuselage	LH_2, LO_2, hyd fluid (83282), MMH, NH_3, lube oil, N_2H_4, F21, HeH_2, N_2O_4	IX[b]	352
Vertical stabilizer forward of rear spar	None		
Vertical stabilizer aft of spar (rear)	Hyd fluid (83282)	X	432
Orbital maneuvering subsystem/reaction control subsystem pod (L&R)	N_2O_4, MMH, He, N_2	XI, XII	352
Main engine LO_2 disconnect	LO_2	XIII	—[c]
Body flap	Hyd fluid (83282)	XV	432
LH_2 umbilical cavity	LH_2, hyd fluid (83282), F21, He, N_2	XVI	432
LO_2 umbilical cavity	LO_2, He, N_2	XVII	—[c]

[a] Zones are one or more compartments that are singly or collectively sealed internally (vented externally) from all other zones.

[b] 352°F is 30°F below the 382°F AIT of MMH at sea level. (423°F is 8% below the 460°F of MIL-H-5606 hydraulic fluid at sea level—only used in gear struts. 598°F is 8% below the 650°F AIT of MIL-H-83282 hydraulic fluid at sea level. 989°F is 8% below the 1075°F AIT of hydrogen at sea level.)

[c] Although oxygen is not flammable, it is a strong oxidizer; therefore, electrical ignition sources should be prevented.

[d] Check valves in Orbiter station 1307 bulkhead permit flow from zone III into zone IX during ground purge.

[e] Left-hand, right hand.

A similar examination of the causative factors for the threat of explosion (Table 6) reveals that a number of things can be done to preclude explosion in addition to those shown in Table 5 dealing with fire.[4] However, there are also several practical architectural strategies. The first line of defense is design to preclude, or isolation, while a second is design to control, as illustrated in Table 7. It is presumed that the basic uses of the space station will include operations such as R&D laboratory experiments, hardware fabrication, or materials processing that may contain hardware with pressure vessels. In those areas where there is a pressurized vessel or the potential for an explosion, one operational solution is to employ hatch pressure module management to minimize the secondary impact of an incident.

Table 5 Typical strategies to counteract threats

DESIGN TO PRECLUDE

ELEMENTS THAT PRECLUDE / THREAT	FIRE	TOXICITY	EXPLOSION
2-GAS SYSTEM -14.7 PSI	•		
MATERIALS/WIRING CONTROL	•	•	•
FLUID LINE CONSTRUCTION	•	•	•
BONDING/GROUNDING	•		•
IGNITION SOURCE CONTROL	•		•
FAIL-SAFE DESIGN & SAFETY FACTORS	•	•	•
PRESSURE VESSELS FILAMENT WOUND HIGH SAFETY FACTOR	•		•

DESIGN TO CONTROL

ELEMENTS THAT CONTROL / THREAT	FIRE	TOXICITY	EXPLOSION
COMPARTMENTATION	•	•	•
PURGE & HAZARDOUS GAS DETECTION	•	•	•
CABIN SMOKE DETECTION	•		•
ACTIVE VENT SYSTEM	•		
REMOTE & PORTABLE FIRE EXTINGUISHERS	•		
DAMAGE CONTROL INSTRUMENTATION & ANNUNCIATORS	•	•	

A second strategy would place the pressure vessels with a TNT equivalent greater than some threshold value outside the habitable area.[4] Figure 2 shows two suggested ways of doing this. One is to move the pressure vessels completely outside and put a shrapnel shield between the habitable volume and the pressure vessel. An alternate approach is to place the hazardous elements inside a volume that has a bulkhead and a fragmentation shield between the habitable volumes, thereby allowing a certain margin of safety. The primary purpose of these strategies is to preclude penetration of the habitable pressure module. Good design practice implies that these high-pressure vessels should not be colocated unless the station is designed to be tolerant of the loss of neighboring pressure vessels.

Of particular interest is the threat of depressurization, since a popular concept of firefighting is that of rapidly depressurizing the habitable volume in an attempt to lower the partial pressure of oxygen below that which will support combustion. Table 8 identifies the causative factors and typical strategies for the threat of depressurization. Only in selected cases does depressurization appear to be the optimum fire-suppression technique. Some of the negative aspects of rapid depressurization include: convection within the volume, more rapid burning with the potential of explosion at lower pressures if flammable liquids are involved, and turbulence that may intensify a fire.

Using the preceding approach, a number of safety design criteria and their attendant guidelines were developed for the Space Station program for each of the threats. Table 9 shows several crew safety criteria and indicates the related threats thus accommodated. Criterion A-8 emphasizes the need for onboard capability for isolation within the volumes and monitoring of the cabin atmosphere. The threat impacts in Table 10 for the same criterion, A-8, provide guidance to the design disciplines. Many of these criteria became mission, operational, and/or design requirements for the current

Table 6 Strategy development for the threat of explosion

Threat	Causative factors	Strategy(ies)
Explosion	Leakage	Isolation (keep hatches closed where explosion is a potential)
		Real-time cabin atmosphere monitoring
		Proper material selection
	Ruptures/structural failure	Place pressure vessels (<0.01 lb TNT) outside or inside with shrapnel shield and pressure bulkhead
		Maximum separation between incompatible fluids
	Relief valve fails closed	Fail-safe design
	Fire/overtemperature	Separate legs of fire triangle
		Detection/suppression
		Proper material selection
	Chemical reaction	Cooling
		Purge
		Isolate materials
		Chemically neutralize

Table 7 Typical explosion containment strategies

Isolation (design to preclude)	Damage control (design to control)
Peripheral containment rings for high-energy rotating parts	Machinery inspection and servicing; verifying guards in place
Compartmentation	Provide damage control lists (structural leak/tear repair) in major modules
Active (hatches)	Close active hatches during explosive risk operations
Passive (structural webs)	Provide maximum access to module pressure walls
Provide shielding/shrapnel deflectors (Fig. 3)	

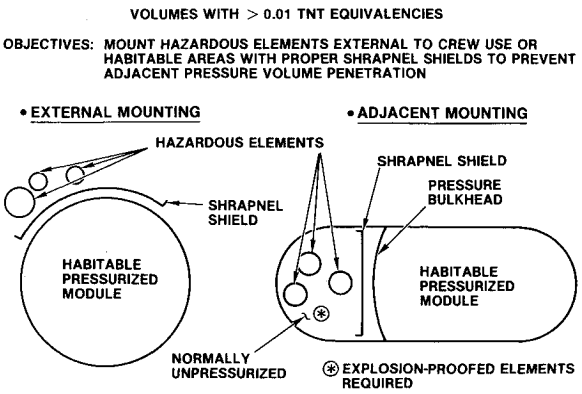

Fig. 2 Typical safety design driver installation constraints.

Space Station program. Once developed, these criteria and their related guidelines form an expandable data-base that may be used for any program where risk control is a paramount consideration.

It is assumed that the space station will make maximum use of design flexibility in the concept phase and have the Shuttle Orbiter available at regularly scheduled resupply intervals. Basically, this study indicated that, for a mature station that has well-defined operational scenarios with creative configuration solutions including redundancy and other appropriate technical provisions, current technology is capable of dealing with all identified threats except injury/illness. (Illness can be precipitated by issues beyond the scope of system design or operational planning.) For study purposes, intrusion/attack was considered a survivability issue rather

Table 8 Strategy development for the threat of depressurization

Causative factors	Strategy(ies)
Unplanned:	
Puncture from debris Inadvertent crew action Internal/external leakage	Capability to inspect/repair inside pressure vessel Station minimum survival functions (mandatory operations at all times) should be coldplated Hardware for other critical functions should be capable of being turned off Need to know location of all personnel in all modules Discrete definition of "time to survive" needed Contamination/toxicity Explosive decompression Interim survival devices Inflatable pressure bulkhead Provide subsystem designers with "maximum hole" to size life-support system with number of cycles (press/depress) stated
Planned:	
Remove contamination Fire control—alternate Maintenance depressurization	Station should be capable of (TBD) pressure volume changeouts (3 minimum)

Table 9 Crew safety criteria-related threats

GROUP: DAMAGE TOLERANCE

ITEM		FIRE	LEAKAGE	TUMBLING/LOSS CONTROL	CONTAMINATION	INJURY/ILLNESS	GRAZING/COLLISION	CORROSION	MECHANICAL DAMAGE	EXPLOSION/IMPLOSION	LOSS OF PRESSURIZATION	RADIATION	OUT-OF-CONTROL IVA/EVA	INADVERTENT OPS	LACK OF CREW COORD	ABANDONMENT	METEOROID PENETRATION	CONSUMABLES DEPLETION	STRUCTURAL EROSION	ORBIT DECAY	ACCESS TO HATCH	TEMPERATURE EXTREMES	DEBRIS	FREE ORBIT
A-5	Potentially rupturable containers should contain less material (gas, liquid, solid) than would cause unacceptable overpressure if all the material were released in a leakage, rupture or explosion	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
A-6	Redundant accommodations for command and control of the space station should be provided such that the primary control center has complete capability, but the backup control center will have, as a minimum, control of critical functions	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
A-7	Design inhibits to prevent failure propagation from one volume/subsystem/component to another should be incorporated	●	●		●				●	●	●						●				●			
A-8	The space station should be designed and operated so that any damaged module can be isolated as required. Provisions shall be made for pressure isolation within the volumes. Modules should be equipped and provisioned so that the crew can safely continue a degraded mission and take corrective action to either repair or replace the damaged module	●	●		●				●	●	●					●	●				●	●		

Table 10 Crew safety criteria impacts

GROUP: DAMAGE TOLERANCE

ITEM		SPACE STATION IMPACT							
		DUAL REDUNDANT	MAINTAINABLE	C&W/COMM	SAFE HAVEN	SS SIZING	MATERIAL CONTROL	ACCESS/DUAL EGRESS	BARRIER SYSTEM	HUMAN FACTORS
A-5	Potentially rupturable containers should contain less material (gas, liquid, solid) than would cause unacceptable overpressure if all the material were released in a leakage, rupture or explosion	●		●					●	
A-6	Redundant accommodations for command and control of the space station should be provided such that the primary control center has complete capability, but the backup control center will have, as a minimum, control of critical functions	●		●	●				●	
A-7	Design inhibits to prevent failure propagation from one volume/subsystem/component to another should be incorporated	●						●		
A-8	The space station should be designed and operated so that any damaged module can be isolated as required. Provisions shall be made for pressure isolation within the volumes. Modules should be equipped and provisioned so that the crew can safely continue a degraded mission and take corrective action to either repair or replace the damaged module	●	●	●	●		●		●	

than one of safety. One other pertinent point is that during a build-up phase, one could expect to experience some hazardous situations or risks that one must accept; but with the proper care, these risks should not be excessive.

Summary

Several benefits are observed from our study of the threat-strategy technique for minimizing design and operational risks. The thrust for the space station is to use the threat/hazard-to-strategy option development agenda to determine the design and operational criteria and attendant safety guidelines that should be applied in the requirements definition phase of the program. Of major significance are the architectural implications that must be considered from a total-station perspective. It becomes obvious that if each station segment is encouraged to deal with fire as a hazard rather than having a total system perspective, redundant and potentially incompatible solutions will arise. A second observation regarding some of the threats with less severe consequences is that these lend themselves to a total-station solution far more readily than if accommodated on a module-by-module or even a subsystem-by-subsystem basis. The hazards having threshold limit values can be accommodated best by having a total system solution. For example, acoustic stressors can be minimized by placing them in a location nearer the workstations than the habitable volumes. Greater concentrations of undesirable atmospheric contaminants can be tolerated if isolated to a volume, provided that appropriate atmospheric protection against the entire vehicle being exposed is taken.

Finally, the focus of program resources on threats rather than hazards has the benefit of a balanced effort for risk reduction and eliminates duplication, divergence of design and operational solutions, and results in an optimum product. Current space station planning incorporates many design and operational requirements developed using the threat-strategy technique. Addressing risk issues up front by judicious use of controls minimizes expansive safety patches to ameliorate risk impact later in the program cycle.

References

[1]"Safety Reliability, Maintainability, and Quality Provisions for the Space Shuttle Program," NASA NHB5300.4 (D-2), 1979.

[2]Peercy, R.L. Jr., Raasch, R.F., and Rockoff, L.A., "Space Station Crew Safety Alternative Study—Final Report," Vol. I—Summary, NASA CR-3854, 1985.

[3]Baker, C.O. Jr. and Peercy, R.L. Jr., "Space Transportation System-1 (STS-1) Safety Assessment Summary," Fifth International System Safety Conference, Denver, CO, July 1981.

[4]Peercy, R.L. Jr., Raasch, R.F., and Rockoff, L.A., "Space Station Crew Safety Alternative Study—Final Report," Vol. 2—Threat Development, NASA CR-3855, 1985.