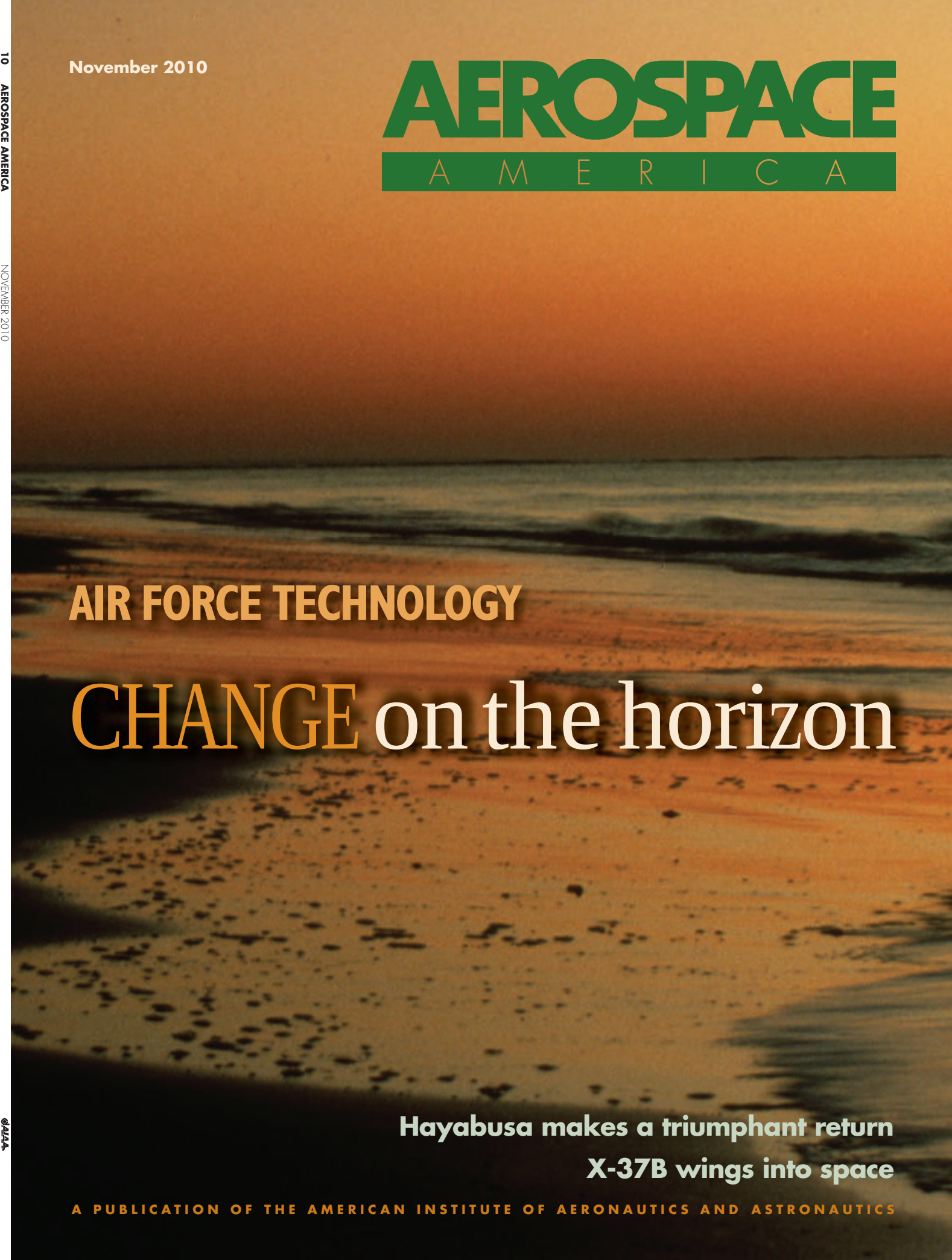
November 2010

AEROSPACE AMERICA



AIR FORCE TECHNOLOGY

CHANGE on the horizon

Hayabusa makes a triumphant return

X-37B wings into space

A PUBLICATION OF THE AMERICAN INSTITUTE OF AERONAUTICS AND ASTRONAUTICS

COMBINING SAFETY and

Human spaceflight is a risky business. Spacecraft undergo very large acceleration forces during launch; travel through the atmosphere at great speeds; and, in the harsh environment of space, either connect with the international space station, remain in low Earth orbit trying to avoid orbital debris and meteors, or continue farther into outer space. Then, after what could be weeks or months, crew and passengers return to Earth, again traveling at very high speeds and under very high deceleration loads.

As difficult as this process is, it has been completed many times, thanks to the efforts of the NASA/industry human spaceflight community. One spacecraft, the space shuttle, has been launched 133 times since 1981. Unfortunately, two shuttles and their crews have been lost, Challenger during launch in 1986 and Columbia during reentry in 2003. These tragedies have resulted in a 'loss of vehicle and crew' rate of 1.5 per 100 launches, which is approximately the same as the combat loss rate of the B-17 bomber in WW II. This very high loss rate must be reduced if human spaceflight is to grow.

THE MILITARY AIRCRAFT MODEL

One way to lower the loss rate of spacecraft is to adopt some of the design processes and technology used to increase the survivability of military aircraft in combat. An aircraft takes off toward the target, which may be defended by one or more weapons or threats. As it approaches, it may be detected by enemy air defense sensors, tracked, engaged, and hit and possibly killed by ballistic projectiles, warhead fragments, or high explosive blasts. A large number of U.S. military aircraft have been downed, lost, or killed in this man-made hostile environment since the early 20th century. For example, approximately 5,000 U.S. fixed- and rotary-wing aircraft were killed in combat during the Southeast Asia (SEA) conflict from 1964 to 1973, with an overall loss rate of approximately one per 1,000 sorties. That's a lot of aircraft.

As a result of those losses, a new aircraft

As we move to the next generation of manned spacecraft, new initiatives would benefit from combining the survivability concepts of military aircraft design with the safety discipline of the spaceflight community.

SURVIVABILITY *for future spacefaring*

design discipline called aircraft combat survivability (ACS) was developed, starting in the early 1970s. Fundamentals have been established for this discipline, including a viable, cost-effective technology for enhancing survivability and a methodology for assessing it. Live-fire testing for survivability is congressionally mandated, top-level survivability design guidance is prescribed, and quantified survivability requirements are now routinely specified by the Dept. of Defense.

The goal is the early identification and successful incorporation of those specific survivability enhancement features that increase the combat cost-effectiveness of the aircraft as a weapon system. In situations where the damage would lead to an aircraft kill, those survivability enhancement features should enable a gradual degradation of system capabilities, giving the crew a chance to eject over friendly territory.

As a consequence of this emphasis on increasing survivability, the number of U.S. military aircraft killed in combat since the SEA conflict has dropped dramatically, and loss rates have been significantly lowered.

Although manned spacecraft are not currently threatened by weapons in space, this

Flak damage completely destroyed the nose section of this Boeing B-17G, a 398th Bomb Group aircraft flown by 1Lt. Lawrence M. Delancey over Cologne, Germany. USAF photo.

Robert E. Ball is a distinguished professor emeritus in the Department of Mechanical and Aerospace Engineering, Naval Postgraduate School, Monterey, California. He is the author of the AIAA Education Series textbook The Fundamentals of Aircraft Combat Survivability Analysis and Design, *First (1985) and Second (2003) Editions. He started the first-ever graduate-level course in Aircraft Combat Survivability at NPS in 1978, and 19 of the 33 astronauts who graduated from NPS have taken one of his courses. He currently is working with the NPS Center for Survivability and Lethality on several survivability projects, including the merging of the safety and survivability disciplines for spacecraft.*

During Operation Iraqi Freedom, A-10 maintenance members from the 392 Air Expeditionary Wing inspect their aircraft for any additional damage after it was hit by an Iraqi missile in the right engine. The A-10 made it back to the base safely. USAF photo/Staff Sgt. Shane A. Cuomo.

relatively new discipline could contribute to the needed improvement in the naturally hostile space environment.

AIRCRAFT SURVIVABILITY VS. SPACECRAFT SAFETY

Aircraft combat survivability is applicable to flight in a man-made hostile environment, but survivability can be more broadly applicable to flying in any hostile environment, including severe turbulence, lightning, birds, or crashes. Aircraft survive either by avoiding being hit by a damage mechanism—known as susceptibility reduction—or by withstanding any hit that does occur—vulnerability reduction. Stealth and electronic countermeasures reduce susceptibility because they make it less likely an aircraft will be hit; fuel system fire and explosion protection and redundant and separated flight control components reduce vulnerability because they make it less likely the aircraft will be killed given a hit.

The spaceflight community has a similar discipline devoted to safe travel. It is part of a package of disciplines known as safety, reliability, and mission assurance, or just safety and mission assurance. One of the major activities within NASA's Office of Safety and Mission Assurance is "improving methodologies for risk identification and assessment, and providing recommendations for risk mitigation and acceptance."

During STS-115, micrometeoroid orbital debris struck the shuttle Atlantis and left a 0.108-in. ding in its right-hand payload bay door radiator. Credit: NASA.

Risks are associated with hazards or conditions that can cause injury to a spacecraft's occupants or damage to the vehicle. For example, a piece of foam insulation could break away from the surface of a spacecraft and impact a critical portion of the craft's thermally protected exterior, a phenomenon known in combat survivability as cascading damage. The impact damage could cause a loss of the spacecraft upon reentry. If the hazard occurs, and people are injured or killed and the vehicle damaged or lost, as happened to Columbia, the result is known as a mishap.

Any potential hazard can pose a threat to the safety or mission capability of a spacecraft. In any safety program, risks or hazards are identified and then assessed, first by determining the severity of the subsequent mishap, possibly using a failure mode and effects analysis (FMEA), and then by estimating the probability the mishap will occur.

Risks, hazards, or mishaps deemed unacceptable because of their combination of severity and probability of occurrence must be avoided, mitigated, or, as a last resort, accepted if no satisfactory avoidance or mitigation technique can be found. Avoidance and mitigation techniques include eliminating the hazards through design selection, incorporating safety devices, providing warning systems, and developing procedures and training.

Comparing the two disciplines, safety is achieved by avoiding hazards, survivability by avoiding hits and thus reducing the likelihood a hazard or hit will occur. Safety is also achieved by mitigating hazards, survivability by withstanding hits, reducing the severity of the subsequent mishap or damage.

One difference between the two disciplines is the operational environment. The threats to the survival of a military aircraft are external and man-made. The current threats to the safety of a spacecraft are not man-made (except for orbital debris) and are both external (micrometeorites, orbital debris, radiation) and internal (such as mechanical or electrical breakdown).

When considering external threats, the survivability fundamentals can be applied to spacecraft as well as aircraft: Avoid being hit by the damage mechanisms, if possible, and withstand any hits that do occur. (One could

consider the external threat to spacecraft as a threat to its survival rather than a safety issue.)

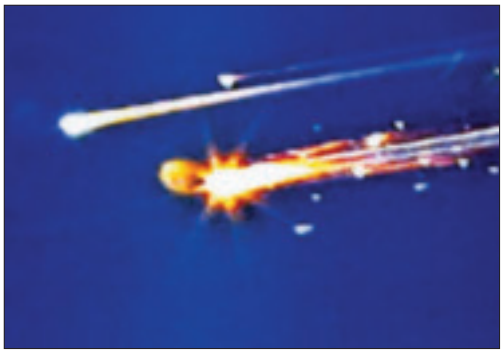
When considering internal threats, the safety discipline relies on the traditional approach of hazard avoidance and mitigation. The survivability discipline, although developed for external threats, can also be used for internal threats if the definition of a hostile environment is expanded to include them. A leak, a fire, or a burst pressure vessel on board a spacecraft creates an internal hostile environment that must be withstood if the spacecraft is to survive. (Again, one could consider the internal threats as threats to the survival of the spacecraft rather than a safety issue.)

The difference in the nature of the threats to survival in combat and to safety in spaceflight influences how they are dealt with by the two disciplines. For example, the primary emphasis in system safety is the avoidance of hazards, particularly by preventing component failures through improvements in reliability. Similarly, the primary emphasis in survivability is to reduce the likelihood a hit occurs. Preventing a hit on a component is conceptually the same as preventing its failure—the component continues to function as needed.

The difference between the two disciplines shows up in safety's mitigation of hazards versus survivability's withstanding hits. In safety, if a pump fails, an adjacent back-up pump can be used. The severity of the mishap associated with the hazard occurrence is mitigated by the use of redundant pumps, and the resultant two-pump design is failure tolerant.

This is not the situation in survivability. When an aircraft is hit, damage can cascade. This cascading damage must be withstood if the aircraft is to survive. If a pump is hit and killed, an adjacent back-up pump could also be killed by the same hit or by cascading damage from the hit pump, and the functions provided by both are lost. Survivability requires redundancy with separation. As a consequence of this difference between safety's component failures and survivability's component damage, the combat survivability discipline conducts a damage mode and effects analysis (DMEA) after the FMEA when identifying the consequences of a hit.

The DMEA can also be used to analyze the survivability of a spacecraft design. In this situation, although the components are not hit by a damage mechanism, more energetic component failures are assumed, such as a liquid oxygen tank that bursts. This particular damage mode occurred on Apollo 13 when one of the two O_2 tanks in the service module burst. Cascading damage caused a loss of the adjacent O_2 tank and a subsequent loss of electrical power and air in the command module. In a more survivable design, the two tanks would have been separated so that a rupture of one tank would not cause the loss of both.



The loss of the shuttle Columbia and its crew of seven was a stark reminder that human spaceflight, though now viewed as routine, is still a high-risk undertaking.

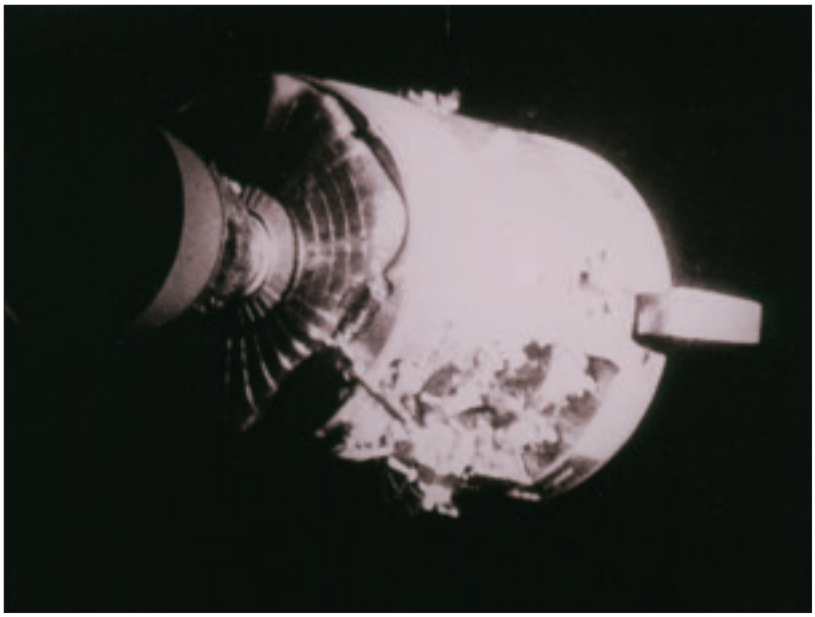
Among the larger pieces of debris recovered from the crash of Columbia was its nose gear, shown here with its tires still intact.

In short, the safety discipline focuses on hazard elimination and mitigation, whereas the survivability discipline focuses on avoiding hits and withstanding the subsequent damage when hits do occur. Safety is an a priori condition where hazards are avoided or mitigated during design; survival is a beneficial outcome of an undesired event. When safety fails, survivability is there to save the vehicle.

COMBINING SAFETY AND SURVIVABILITY

Because the fundamentals of the aircraft combat survivability discipline have direct applicability to the design of spacecraft, a merger or combination of both could be beneficial for future human spaceflight. The merger could

"When safety fails, survivability is there to save the vehicle."



An entire panel of the Apollo 13 service module was blown away by the apparent explosion of oxygen tank number two, located in sector 4 of the SM. Two of the three fuel cells are visible just forward of the heavily damaged area.

take the form of a combined discipline known as safety and survivability, or a separate discipline could be developed known as spacecraft survivability.

If a combined discipline is chosen, NASA Procedural Requirements 8705.2B, Human-Rating Requirements for Space Systems, should be expanded to include the fundamentals of survivability enhancement developed for military aircraft. ("The human factor," page 3, and "Human rating for future spaceflight, A Roundtable Discussion," page 26, July-August, examine the ramifications of rating systems for human spaceflight.) If a separate spacecraft survivability discipline is chosen, a new process and requirements document should be developed.

This proposed combination has already begun for internal threats to the Orion crew exploration vehicle, originally part of NASA's Constellation program. Michael Saemisch, former safety and mission assurance manager for Project Orion on the Lockheed Martin contract, and Meghan Buchanan, lead engineer for the company's spacecraft survivability innovation for Orion, in collaboration with the Naval Postgraduate School Center for Survivability and Lethality, are developing a spacecraft survivability program based upon the fundamentals of the ACS discipline. Several design changes to Orion were made using this new approach. In June, the NASA/Lockheed Martin Orion team completed the Phase 1 Safety Review, making Orion the only spacecraft in development that meets all of NASA's human-rating criteria for missions beyond low Earth orbit.

Now is an opportune time to formalize the merger. NASA's Commercial Crew Development Program is currently working on a standardized integrated safety and design analysis process for the NASA commercial crew initiative that will be used for risk assessment during design, development, and demonstration of vehicles for human spaceflight. This work will focus on the integrated analysis process instead of prescriptive failure tolerance requirements to generate a safety-optimized solution. The DMEA and other design and analysis processes developed for enhancing the survivability of military aircraft should be incorporated into this new analysis, to ensure safer and more survivable spacecraft.

RECOMMENDATIONS

As the shuttle era draws to an end, new commercial initiatives are under way for human spaceflight. They can all benefit from the following recommendations, drawn from experience during the development of the aircraft combat survivability discipline:

•Safety and survivability should be merged or combined to form a new discipline for space systems, leading to improvements in both the safety and the survivability of human spaceflight in all environments. They should be essential elements, just as they are in military aircraft. This does not mean there will be no more losses—as long as there are flights, there will be losses. It does mean that any mishap will not be the result of a lack of foresight, insight, or oversight.

•Safety and survivability should be considered from the inception of any program, whether for military aircraft or a human-rated space vehicle. Any changes that have to be made well into the program because of postponed or neglected safety and survivability concerns will most likely be very costly in weight and dollars and may result in cancellation of the program, or even loss of life.

A production assembly crew lowers a full-scale Orion mockup onto the crew module holding structure during an assembly pathfinding maneuver at the Operations & Checkout Facility at NASA Kennedy.