EVOLUTION OF SAFETY ANALYSIS TO SUPPORT NEW EXPLORATION MISSIONS

Chad W. Thrasher [1]

[1] *National Aeronautics and Space Administration, Marshall Space Flight Center, Mail Code QD34, MSFC, AL 35812, United States of America, Email: chad.w.thrasher@nasa.gov*

NASA is currently developing the Ares I launch vehicle as a key component of the Constellation program which will provide safe and reliable transportation to the International Space Station, back to the moon, and later to Mars. The risks and costs of the Ares I must be significantly lowered, as compared to other manned launch vehicles, to enable the continuation of space exploration. It is essential that safety be significantly improved, and cost-effectively incorporated into the design process. This paper justifies early and effective safety analysis of complex space systems. Interactions and dependences between design, logistics, modeling, reliability, and safety engineers will be discussed to illustrate methods to lower cost, reduce design cycles and lessen the likelihood of catastrophic events.

1. MOTIVATION FOR IMPROVEMENT

Why is it essential to improve the overall safety of space systems and reduce the costs? The answer is simple: public expectations. The public must clearly understand that the benefits of space exploration outweigh the risks and costs in order to support long-term space exploration. This paper will not address the benefits of space exploration, but will address how to reduce the risks and costs to increase the general population's support of space exploration. The public generally has a limited understanding of the magnitude of risks or costs associated with space exploration. The current Space Shuttles use three Space Shuttle Main Engines (SSME), and two Solid Rocket Boosters (SRB) to generate a combined 6.3 million pounds (28.0 million newtons) of thrust at liftoff and use a combined 535,000 gallons (2.03 million liters) of liquid propellants and roughly 2.2 million pounds (0.98 million kilograms) of solid propellants in less than ten minutes [1] to achieve orbit. The average person has little or nothing to compare this energy output to. Just the thrust from the two SRBs are compared to "14,700 six-axle diesel locomotives" [2] in one NASA publication. It is very unlikely that the average person has ever seen one hundred, much less a thousand, locomotives passing at one time. The public also does not fully understand the harsh environment of space such as the vacuum of space, temperature extremes, and operational limitations which drive the complexity of space systems. Similar challenges are encountered by those engaged in or designing submarine/ deep-ocean exploration and high altitude flight systems. However, this is a relative small portion of the population employed in these high-risk professions.

1.1 Public Safety Perception

The world population is generally trending towards being more risk-adverse. Just looking at historical data we can see this trend. During World War II, between 1939 and 1945, an estimated 16 millions Americans died as a direct result of that conflict. However, since the beginning of US operations in Iraq beginning in 2003, only an estimated 4,177 have died and there has been 30,633 wounded as September 2008 [3]. Clearly the divisions evident in the media, protests, and speeches of politicians indicate less support for the Iraq conflict than World War II. Yet the public opinion is less in favor of military involvement in world affairs, with 36%, the highest percentage since 1947, believing that the US should stay out of world affairs [4].

An estimated 16,692 Americans died in 2005 due to acts of homicide inside the country's boarders [5]. Another 41,059 died in 2007 due to motor vehicle crashes a 3.9% decline from 2006, which was also the lowest level since 1994 [6]. The study results show a 1.37 Fatality Rate per 100 million Vehicle Miles Traveled (VMT). This continues that trend estimated roughly as at 3.4/100M VMT in 1975. Why is the American public not outraged by the deaths with the country's boarders? Is it because the trend in both homicides and motor vehicle accident fatalities is a gradual reduction over time? I argue that it is the public's perception that one's individual risk is relatively low. The population of roughly 303 million deems 50,000 fatalities a year as being acceptable because some other individuals are taking higher than necessary risk and that the number of fatalities is relatively low when compared to the total exposure. Driving while intoxicated, under the influence of drugs, or at speeds in great excess of the posted limits are examples of taking higher than necessary risks. The current American drives an average of 15,000 miles per year which results in a fatality rate of roughly 5.1×10^{-4} per driver, using the data above.

1.1 Reducing Cost per Failure

The monetary cost is another area where each failure of a major space system is deemed unacceptable. The Space Shuttle Endeavour cost approximately $1.7 billion (real dollars) in 1992, and approximately another $450 million per launch [7]. The single unit cost comparison is similar to the $2 billion cost of a B-2 aircraft but, much higher than the F-22 Raptor at a cost of $137.5 million (2008 flyaway estimate) [8]. When compared over time, the aircrafts' operational costs are significantly lower due to the number of missions in a year and the significantly lower cost of maintenance and support activities. Similarly, the loss of a single Raptor or mission doesn't necessary imply that the primary system capability is lost. Aircraft loses are expected during a conflict and would not ground the entire fleet. Even when a specific aircraft type is grounded due to safety issues there are enough systems with similar capabilities to ensure that the overall capability is not lost, only temporarily reduced. The single-day loss of a Space Shuttle mission is at least $2.15 billion dollars [7], significantly higher than most high-performance military aircraft and at least a one year stand-down.

The typical person accepts the choice to become a fighter pilot or astronaut as a personal choice to pursue a high-risk profession. However, the loss of a Space Shuttle or the International Space Station is also financial risk of the nation and therefore shared by all citizens. The financial cost of the Iraq conflict has been over $845 billion to the U.S. with a total cost to the economy has been estimated at $3 trillion [9]. The public perceives the cost of the Iraq conflict, $845 billion and growing, as more expensive than the $341 billion spent to fund World War II, even though the cost would be $3.89 trillion after adjusting for inflation. The cost of World War II, using 1945 dollars and US population estimates based on the census figures would have been $2.25 per citizen as compared to $2.78 per citizen for the current Iraq conflict.

The public considers a Space Shuttle failure as a much higher financial risk than a motor vehicle accident. This is because of three factors: Americans are 76 times more likely to be injured in a motor vehicle accident instead of being killed [6], the loss of capability is only temporary - another vehicle is readily available and can be purchased, and the majority of drivers have insurance which mitigate the financial costs.

The conclusion is that the general population is not willing to continue to accept a very high chance of death given a very limited exposure time in conjunction with a perceived high monetary cost – such as the cost of funding a war or space exploration.

2. EVOLVING SAFETY PRACTICES

It is generally accepted that to build safety into a system it must be involved early in the development of a system. The Constellation Program involved a few key experts during the mission concept phase but the staffing and involvement of safety in the requirements development increased as the program grew. Safety engineering was involved evaluating the design and coordinating requirements prior to the completion of the System Requirements Review (SRR). The initial design evaluation, completed prior to the SRR milestone emphasized safety critical functions and aspects of the system that were not expected to meet the initial set of safety requirements. By the Preliminary Design Review (PDR) the requirements had been updated to reflect the physical design limitations, had eliminated or addressed many earlier concerns, and effectively communicated areas where safety risks remained high**.**

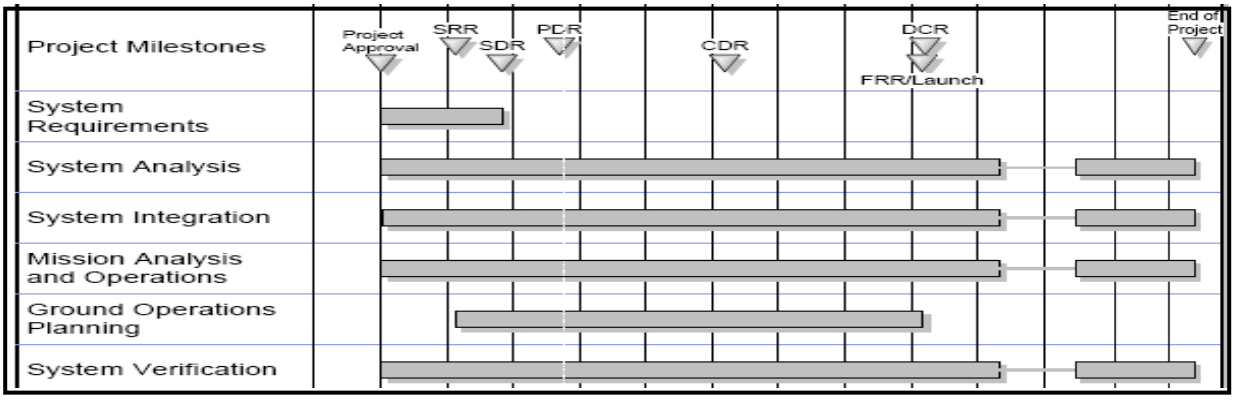


Figure 1. NASA Phasing of System Engineering Tasks

2.1 Driving Requirements and Design vs. Documenting the Design

The primary problem in system safety is that the safety analysis in any organization is usually a design cycle behind the design. Generally, a designer develops an initial design, provides it to the safety engineer, and returns to iterating the design while it is being evaluated for the first time for safety issues. The designer has already completed his second design iteration by the time the safety engineer provides the assessment of the initial design.

Ares I decided to jump-start the safety analysis by using the vast data already available. Initially a review for applicable lessons learned from the history of manned launch vehicles, expendable launch vehicles, satellites, robotic missions, ISS, and ISS payloads were used to generate a significant list of possible hazards and causes to help assess the requirements prior to the SDR. After SDR an extensive study of 6093 past launch failures, including manned and unmanned launch systems was performed. Each failure was categorized by failure mode and then determined if it would be applicable to the Ares I system. Concurrently, Space Shuttle hazard reports were reviewed for applicability as well. Initial designs, based on shuttle hardware, were evaluated to identify areas were the design failed to meet the initial set of requirements and to determine if causes of previous failures were being considered in the design. This allowed the safety engineering community to make earlier recommendations to add or change requirements. It also provided a mechanism for safety engineers to present information to the design engineer that would be helpful early in the program – early enough to drive the design and establish a relationship. The initial efforts are represented in the upper left side of Figure 2.

Next, the probability of a given failure mode due to a limited set of causes was calculated by using Probabilistic Risk Analysis (PRA). This data was then used to prioritize work, and develop a list of findings and recommendations which were communicated to the entire project.

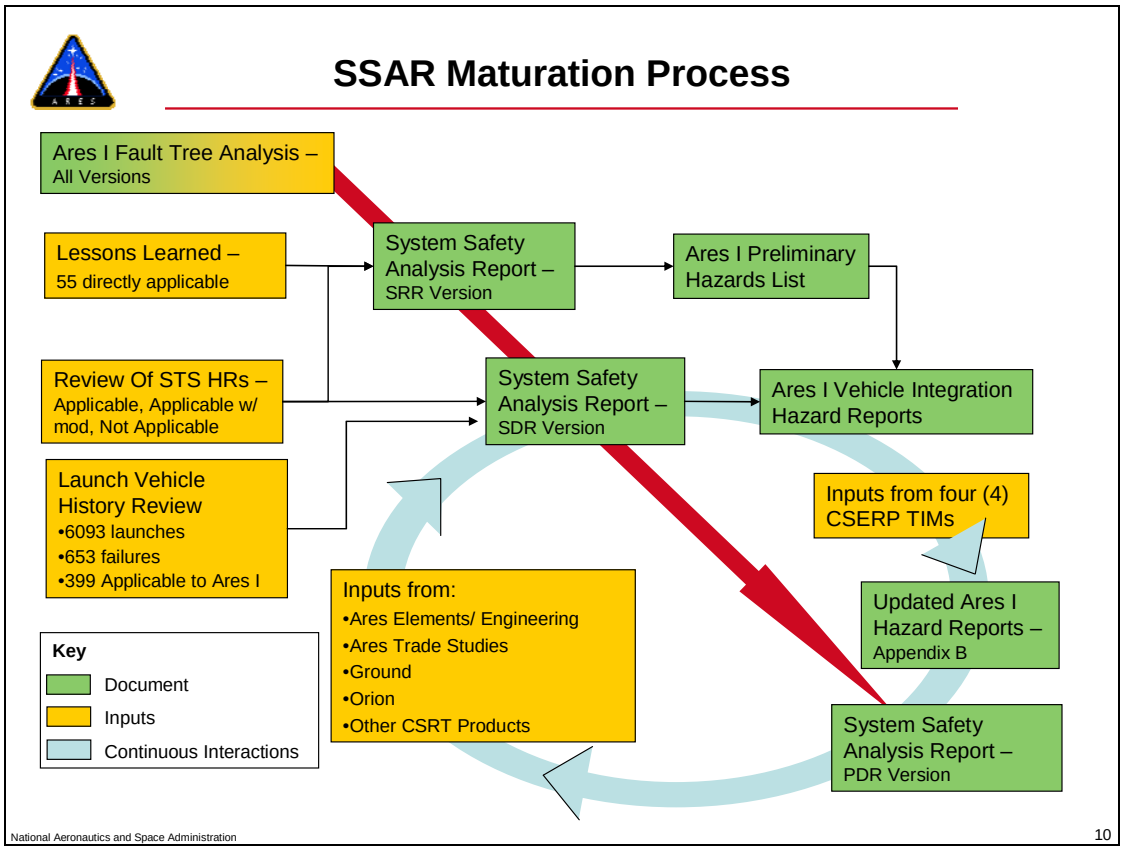


Figure 2. System Safety Analysis Report Maturation Process

2.2 Dependences and Interaction

One can already see how that the design development of any complex system has numerous dependencies and interactions. The safety analysis of a system is no different, it has dependencies and interactions. Unfortunately, those linkages have not been fully understood or appreciated until after the design has matured through two design cycles. Remember, the safety engineer usually didn't receive the design until the second cycle was starting. The engineering group responsible for the design was not made aware of any safety issues until well into the second design cycle. What can safety contribute prior to and during the first design cycle? Prior to or beginning the first design cycle, a new system can be compared to similar known systems, such as Ares I use of Space Shuttle hardware data. Then requirements to preclude potential weaknesses of the known system can be added to the requirements. Requirements should be added which ensure that previously used failure recover techniques are available. The safety organization should also contribute a list of possible hazards and causes to the design engineer. The discussion of possible hazards and causes allows the safety community to better understand the system and the planned controls. It also allows the design community to ensure that all the safety aspects of a design are being considered.

An example of incorporating safety into the early design decisions was when a critical actuator for the Ares I design was being selected. Three single failure tolerant options existed: hydraulic, electro-mechanical, and a design that incorporated both the hydraulic and electro-mechanical. The hydraulic design was based on heritage and had known safety issues, the electro-mechanical design had few safety issues but more unknowns and very little flight heritage, and the last design attempted to be fully one failure tolerant through unlike redundancy. The last option was eliminated because of the risk of manufacturing, servicing, and using two dramatically unlike systems created twice the number of risk and challenging operability issues. The remaining two options were traded considering design, safety, operability, and other issues. The heritage design was selected but the study revealed specific components that needed to be re-evaluated due to the different environments and loads.

The interdependencies between the design, operability, reliability, and safety can be seen in the example. However, a number of other relationships are not as clear. The Ares I project is divided into three major Elements (First Stage, Upper Stage, and Upper Stage Engine) and Vehicle Integration. The Vehicle Integration Office has divided tasks into functional areas as designated in Figure 3. The Crew Safety and Reliability (CSR) group is assigned risk analysis [Table 1].

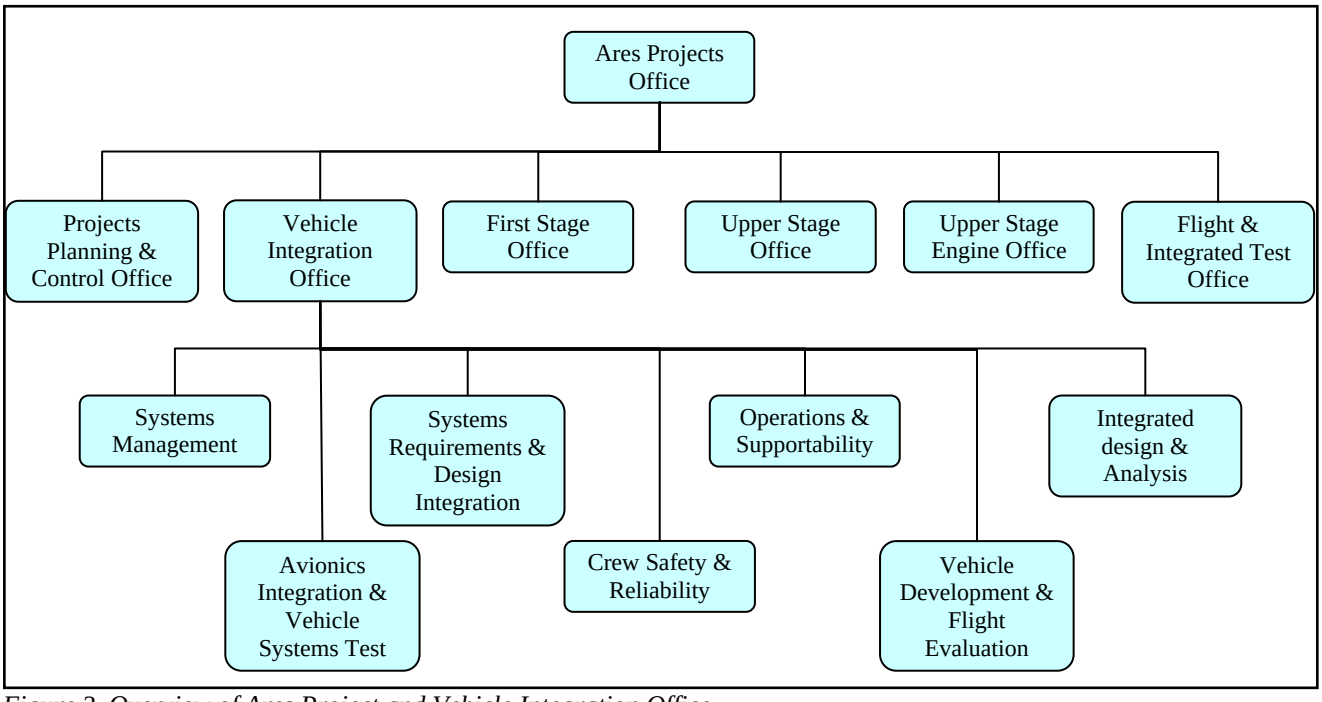


Figure 3. Overview of Ares Project and Vehicle Integration Office

WBS 5.2.7 - Crew Safety and Reliability		
Working Group	Deliverables	Assigned Tasks
Ascent Risk Analysis	Ares I Crew Safety and Reliability Ascent Risk Analysis Report	• Provide integrated vehicle level PRA estimate • Identify key risk drivers and potential areas of improvement • Document ground rules and assumptions
Fault Detection, Diagnostics, and Response	Ares I Abort Conditions Report	• Identify abort conditions, assess which conditions must be monitored
	Ares I Abort Failure Detection and Response System Definition Document	• Define abort algorithms • Develop/ document abort architecture and recovery management • Sensor qualification logic
Integrated Aborts	Ares I Integrated Aborts Plan	• Outline approach and methods to support aborts
Probabilistic Design Analysis	Abort Risk Assessment Engineering Memorandum	• Physics-based analyses to assess severity of failure environments • Monte Carlo simulations of failure environments • Input to loss-of-crew estimate • Document modeling ground rules and assumptions
Reliability	Ares I Integrated failure Mode and Effects Analysis and Critical Items List	• Identify failure modes and results to the vehicle • Eliminate critical failure modes • Establish risk retention rationale
Safety	Ares I System Safety Analysis Report (SSAR)	• Provide recommend actions with regard to safety risks • Document hazard reports and FTA findings • Summarize critical/high-risk events
	Ares I Fault Tree Analysis Report (FTA)	• Identify initiating failure causes including non-hardware causes

Table 1. Crew Safety and Reliability Working Groups and Responsibilities

These working groups regularly share information and communicate results to each other and the design community. The Integrated Aborts group is tasked with developing the abort philosophies, the Fault Detection, Diagnostics, and Response (FDDR) group identifies critical sensors necessary to detect and determine failure modes during flight, the PDA develops specific models to better understand failure mechanics, the SARA working group models the failure effects, such as blast effects, to determine the effectiveness on any abort options. The other working groups have recognizable deliverables and tasks.

Typically, either the safety or reliability group identifies failure cases which the Ascent Risk Analysis working group ensures is included in their analysis and is credible. When the likelihood of a failure case was relatively high, when compared to other failure modes, the PDA group would model the failure case to fully understand the chain of events leading to and resulting from the failure. The Integrated Aborts working group would determine if there were sensors which would detect a failure and what abort mode(s) would be used. Lastly, the SARA group would determine if the resulting abort would be successful by determining if the command module and crew would survive the failure effects through numerous simulations. These are labor intensive analyses which are prioritize to address high-risk areas based on when the required data is available.

There remain two relationships to discuss: logistics and management. The relationship between logistics and safety is very critical. It is impossible to identify all possible hazards without understanding the flow of operations. Where will hazardous activities, like loading of toxic consumables such as hydrazine, take place? What precautions (controls) and capability (hardware or software) are necessary to safety perform pre-flight and contingency maintenance activities? These types of questions drive design changes such as adding accommodations for access, such as wider access panels, and/or identifying were additional capability, such as hazardous gas detection, would allow activities to be performed quicker and safer.

The most important relationship is with the design community. The relationship with management is likely to be next in importance. The relationship with management important not just because they decide were resources will be spent but, because without a good working relationship it is extremely difficult to ensure that results of safety analyses impact the design. The ideal state is that both the Project Manager and the Chief Engineer wants to here the opinion of the safety community prior to concurring or making critical design decisions. As a safety engineer, you want a chance for your recommendations to be heard and fairly considered.

How can your safety program position itself such that its analyses and opinions are sought by management? Meet or exceed management's expectations. The goal of any manager is to produce a system that works, on-time, and within budget. Managers expect detailed schedules, good products, feedback on proposed major changes, and information that improves the design. Pitfalls regularly include: schedules which fail to produce timely inputs to support other groups, inadequate or no evaluation of requirements and proposed design changes, products that are inconsistent with the current design, lacking communications concerning how risk and hazards are being identified and shared with the design community are just a few examples. Even early in the design safety should participate in trades. Keep a record of where safety's input was or could have been the driver for the design. Often safety takes the position of a requirement enforcer, telling engineering and management why the design is unacceptable but not providing any suggestion on how to resolve the unacceptable condition. Sometimes this is necessary but it should be avoided. Instead communicate the issue and focus on arriving at a resolution. Can the design be changed? If the design can not meet the requirement as written can it meet the intent of the requirement? Focus on changing the design where it lowers the overall risk of the system. By impacting the design, coordinating tasks with other groups, and working the high risk items first; you will focus on value-added work which reduces redesign cycles and effectively lowers the cost of the safety analysis for the project.

The Ares I System Safety Analysis (SSAR) report, along with other CSR deliverables, summarizes the safety analysis process, results of the analyses, and provides findings and recommendations for project management to consider for emphasis during the next design cycle. Management can evaluate the recommendations in the SSAR against the level of detail in other engineering documentation and decide which areas of the system need additional attention. The decision is based upon being well-informed early in the design cycle, including the safety risks. In past NASA programs the safety analysis was often a design cycle behind or just documenting the hazards and causes and existing controls in the system without being able to influence the design decisions.

3. GOALS, EXPECTATIONS, AND PLANNING

There are key activities any safety organization involved in space exploration must perform to support system development. It must develop and well-define the system goals and the goals of the group supporting the safety effort. Understand the expectations of multiple customers of the safety organization and fully explain the implications of those expectations down to the design engineer. Lastly, perform the short and long-term planning to ensure that the results of safety analyses impact design and ensure sufficient resources exist to accomplish the defined tasks.

3.1 Ares I Safety Goals

The driving goal of the Ares I safety organization is: Prevent the Loss of Life during a mission. This can be broken down into multiple sub-goals which can also be divided into lower level goals as depicted in Table 2.

Constellation Program Goals (A partial list)
1.1. Develop a crew launch vehicle to provide transportation to LEO as close to 2010 as possible to minimize the gap with Shuttle retirement
1.2. Provide a substantial increase in safety and reliability in the launch phase compared to present human transportation systems.
1.3. Provide a launch vehicle system that supports a substantial reduction in total mission operation costs compared to present human transportation systems.
Ares Project Goals (A partial list)
2.1. Ensure flight/ground safety, while meeting system performance requirements and achieving mission objectives. (1.1,1.2)
2.2. Utilize current, proven technology in the designs of the Ares I and Ares V. (1.2, 1.3)
2.3. Implement the Integrated Logistics Support approach and methodologies at the earliest stages to achieve the lowest ownership costs. (1.3)
Vehicle Integration Goals (Technical Performance Metrics)
3.1. Mass to Orbit (2.1)
3.2. Loss of Mission (2.1)
3.3. Launch pad processing time. (2.3, 2.3)
Crew Safety and Reliability Goals (A partial list)
4.1. Generate a integrated vehicle level PRA estimate (Loss of Mission / Loss of Crew) (3.2)

4.2. Ensure that abort conditions and necessary sensors are identified (3.2)
4.3. Eliminate or control safety hazards and their causes through design (3.2)
Safety Working Group Goals (A partial list)
5.1. No Loss of Life (Public, Flight or Ground Crew) (4.1, 4.2, 4.3)
5.2. No Ares I failures which trigger an abort over the program life (4.1, 4.3)
5.3. No repeat "Lesson Learned"(4.2, 4.3)
5.4. Impact the design based on hazard analyses (4.1, 4.2, 4.3)
5.5. Pass all Constellation Safety and Engineering Review Panel (CSERP) reviews (4.2, 4.3)

Table 2. Example of the Flow-down of Safety Goals

Under the goal 5.2: "No Ares I failures which trigger an abort over the program life" are a number of sub-goals /functions which must be accomplished to be successful. While the list of goals is not complete here it is easy to see how individual engineers can use one or more as guidance on where to focus their efforts. It allows the engineer to communicate goals and prioritize task related to the hazards that they are assigned.

3.2 Expectations of the Ares I Safety Organization

The Ares I management expects the safety organization to identify any safety issues, communicate those issues to the engineering community, and elevate to management's attention any high risk or one which an acceptable solution can not be agreed upon. Besides generating hazard reports with causes, controls, and verification; formally identifying and elevating risk items, generating Review Item Discrepancies, and presentations at meetings are also used to highlight high-risk areas. Management also expects the safety organization to successfully pass all Constellation Safety and Engineering Review Panel (CSERP) reviews. The CSERP is a group of engineering experts that are funded by the Constellation Program and are not funded or accountable to the Level III projects, such as Ares or Orion. They function as an independent review board concerned primarily with the safety aspects of the system. The CSERP has a phased review approach similar to that which has been successfully applied to the Payload Safety Review Panel (PSRP). Unfortunately, a phased safety review process for a developmental project is new and untried process. The safety organization must coordinate inputs and support from the engineering community and other projects as necessary to support reviews. Action Items and agreements must be answered and a number of meetings scheduled to be effective.

A key expectation within the Ares I safety organization is ownership of hazard reports. Ownership requires that the safety engineer identify tasks to be accomplished to support the delivery schedule, identify key points of contact, participate in meetings regularly, plan to hazard report development (inputs needed, key dates, analysis methods, needed support), discuss plan with the right design teams, and finally document. Ownership of hazard reports will encourage engineers to communicate issues and concerns sooner rather than later. Both management and designers need regular analysis updates and results, identification of requirement gaps, and an explanation of what assumptions and documents were used as inputs. Overall the expectation is to deliver high-quality products, not just hazard reports, in time to influence the design.

3.3 Planning for Success

Strategic planning is one of the keys to being effective by providing timely technical assessments. One must first know the major program and project milestones. The next critical step is to determine the goals of the safety analysis team. A goal such as: "No Ares I failures which trigger an abort over the program life" or "Pass all CSERP reviews" are clear and defined. These must be further divided into deliverables and tasks which can be completed. After the content of deliverables, their inputs, and due dates have been identified the relationship with other groups can be defined. Remember that the more your products are used the greater value you have to the project. The amount of involvement and communication with other groups will partially be based upon the deliverables and expectations of management and any reporting requirements. However, more information in reports, official documents, or in briefing formats may also be required to communicate the issues effectively.

Always ensure enough resources are available to communicate concerns and participate in trade studies or analyses which will not be scheduled in the original planning. Resource planning must also include vacations and training of personnel. Engineers that are asked to continually work at stressful levels without any vacations or lulls in the level of activity will either burn-out or leave to pursue other opportunities. Training is necessary to prevent the engineer from developing tunnel-vision when examining their assigned system.

4. CONCLUSION

If space exploration is to continue, safety must increase and the overall cost must continue to be reduced. Safety

can only increase through incorporating the right safety requirements into the program and the necessary hardware controls earlier in the design cycles than the majority of prior major NASA systems. The safety risks must be clearly communicated to the public along with the benefits of technology development and scientific discovery. The public must perceive that the economic benefits of space exploration outweigh any potential shared financial risk –which was accomplished on ISS by sharing the cost and risk. The hazard analysis, along with a number of supporting analyses must be fully integrated from the beginning of the design concept phase to reduce development and long-term operational costs.

5. REFERENCES

1. NASA (2002). A Walk Around the Space Shuttle, FS-2002-08-133-MSFC. *NASA Facts*, Pub 8-40062

2. NASA (2002). NASA Facts: Shuttle Propulsion Trivia, FS-2002-08-134-MSFC. *NASA Facts,* Pub 8-40061

3. icasualties.org (2008). Iraq Coalition Causality Count, http://icasualties.org/oif/

4. The Chicago Council on Global Affairs, (2008). *Global Views 2008: Troubled by Loss of Standing in the World, Americans Support Major Foreign Policy Changes*, The Chicago Council on Global Affairs, Chicago, IL, pg. 6. http://www.thechicagocouncil.org/UserFiles/File/POS_Topline%20Reports/POS%202008/2008%20Public%20Opinion_Foreign%20Policy.pdf

5. U.S. Department of Justice Federal Bureau of Investigation, (2008). U.S. 2007 Homicide statistics, http://www.fbi.gov/ucr/05cius/offenses/violent_crime/murder_homicide.html

6. National Highway Traffic Safety Administration, (2008). Motor Vehicle Traffic Crash fatality counts & Estimates of People Injured for 2007. *DOT HS 811 034*, www.nhtsa.gov

7. NASA (2008). Kennedy Space Center: Frequently Asked Questions, http://www.nasa.gov/centers/kennedy/about/information/shuttle_faq.html#10

8. United States Air Force, (2008). FY2009 Budget Estimates, p. 1-13.

9. Stiglitz, Joseph E., Bilmes, Linda J., (2008). *The Three Trillion Dollar War: The True Cost of the Iraq*, W.W. Norton, NY, NY, pp 100-101.

National Aeronautics and Space Administration

IAASS Conference

October 21, 2008

EVOLUTION OF SAFETY ANALYSIS TO SUPPORT NEW EXPLORATION MISSIONS

Chad W. Thrasher
NASA/MSFC/QD34

Ares I and Ares V

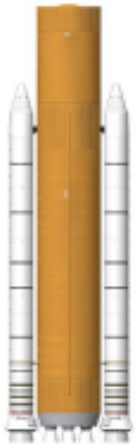
Composite Payload Shroud

Altair Lunar Lander

Earth Departure Stage
LOx/LH_2
1 J-2X Engine
Al-Li Tanks
Composite Structures

Loiter Skirt

Composite Interstage



Core Stage
LOx/LH_2
6 RS-68B Engines
Al-Li Tanks
Composite Structures

2 5.5-Segment RSRBs

Launch Abort System

Orion Crew Exploration Vehicle
(Crew Module / Service Module)

Encapsulated Service Module Panels

Instrument Unit

Upper Stage

J–2X Upper Stage Engine

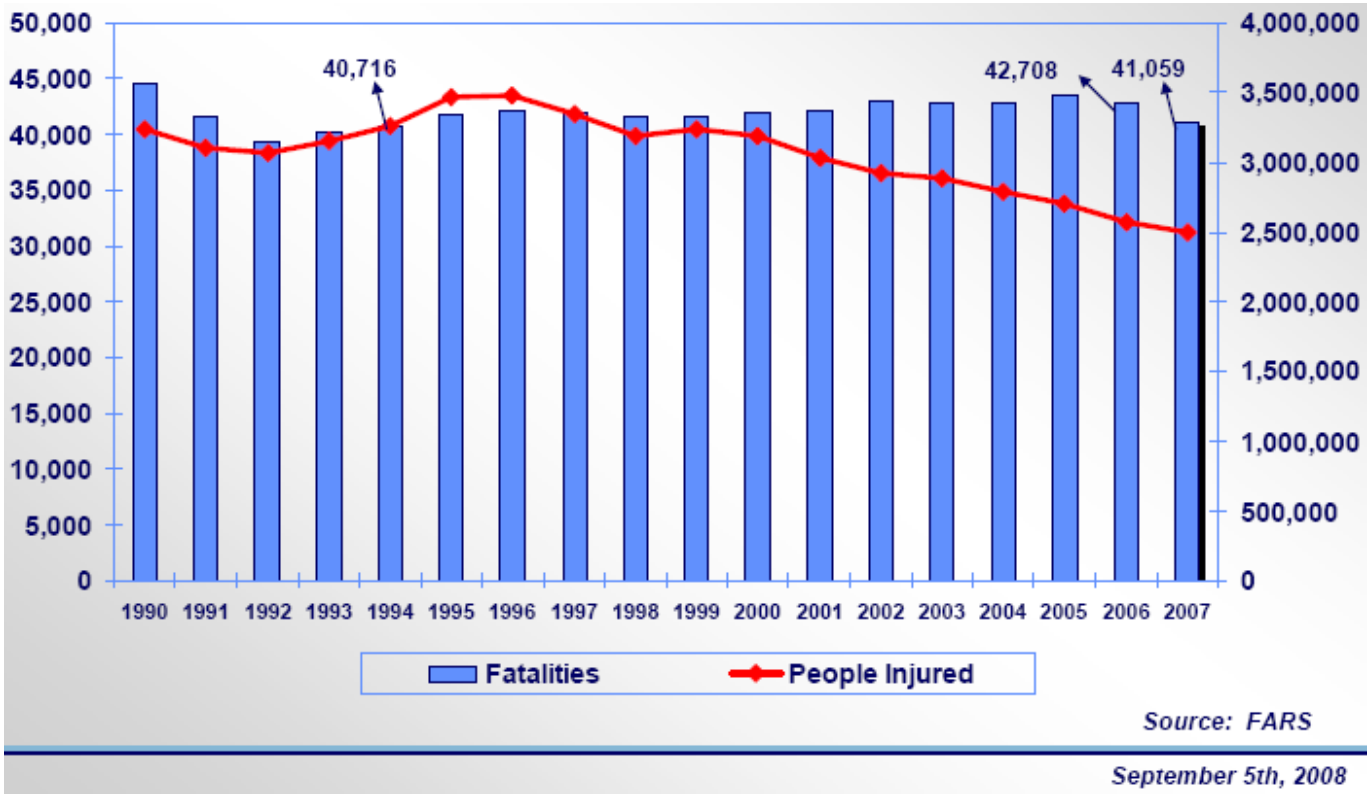
Interstage

Forward Frustum

First Stage
(5-Segment RSRB)

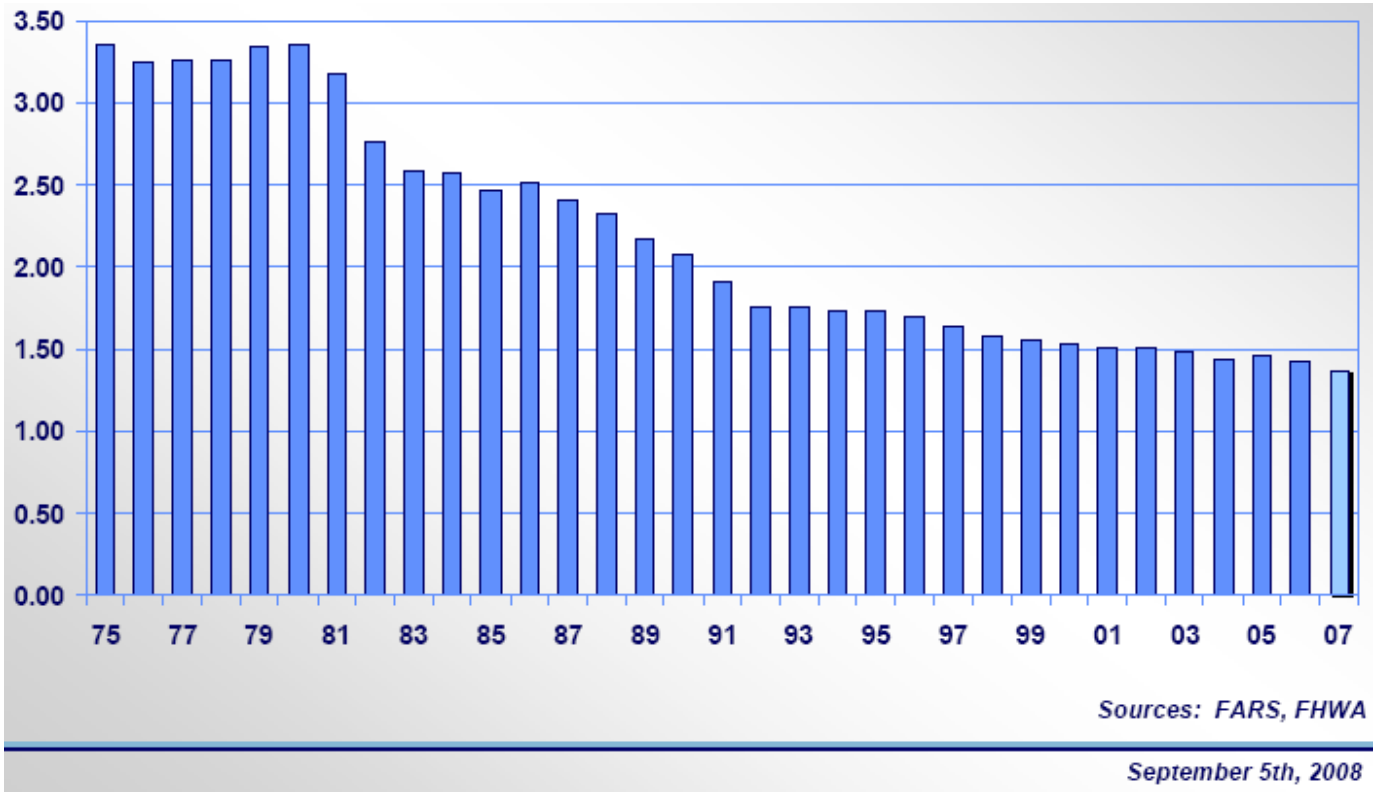
Concept image of Ares V elements. (NASA MSFC)

People Killed and Injured In Traffic Crashes, by Year



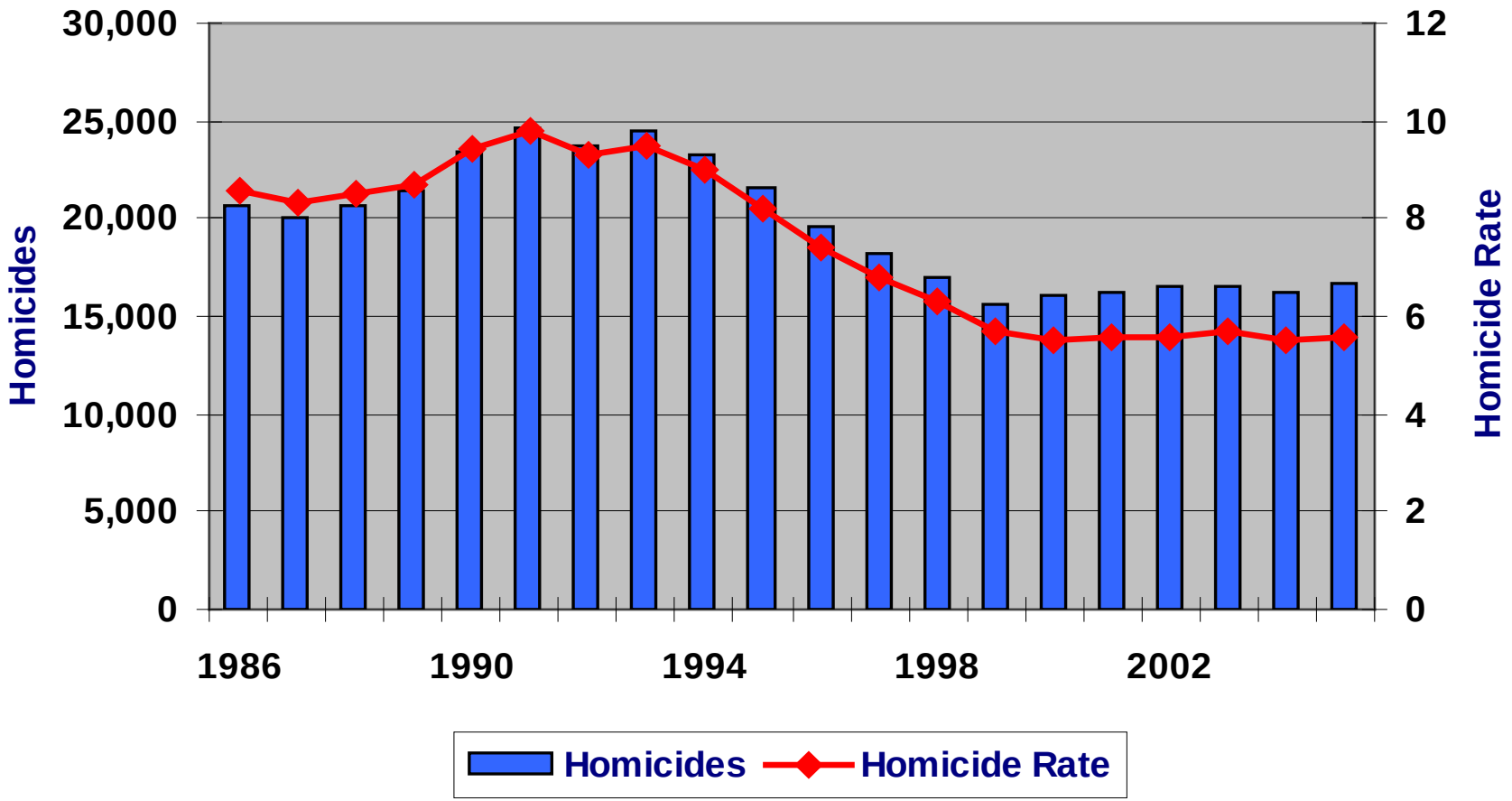
- Number of Fatalities is relatively stable
- Injuries have been decreasing since 1995

Fatality Rate
Per 100 Million VMT, by Year



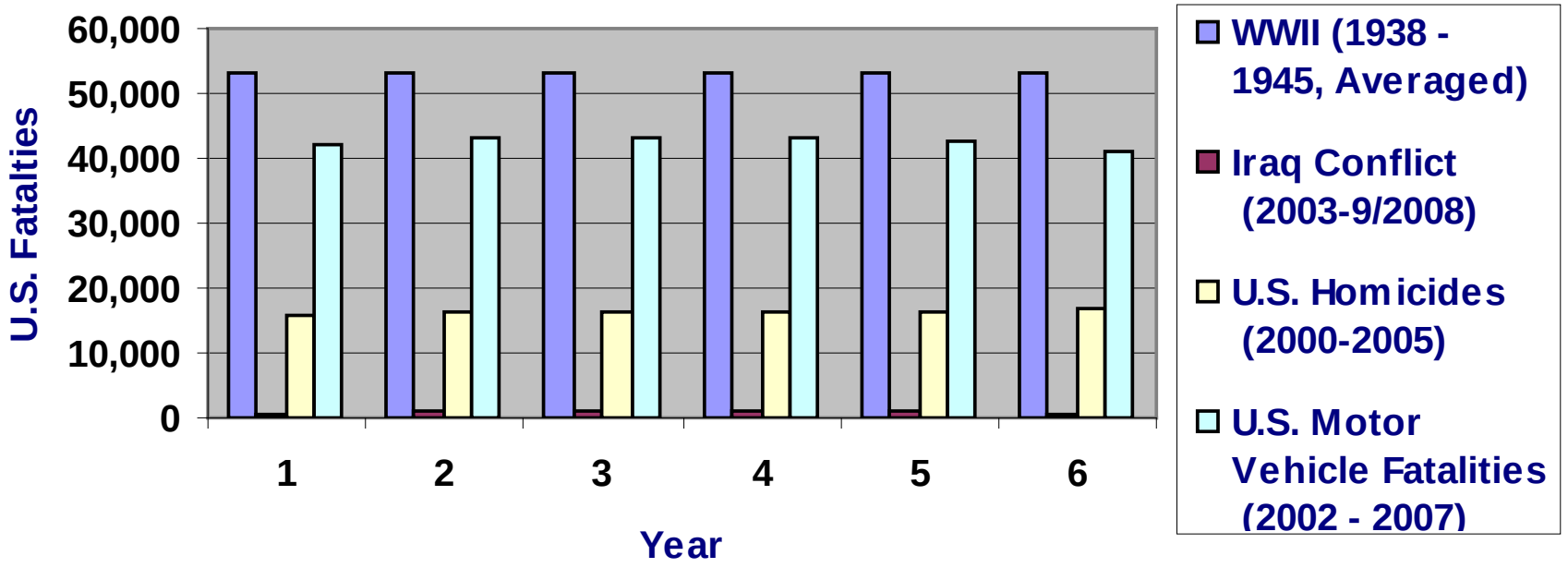
- **Increase in exposure time**
  - **Increasing number of drivers**
  - **Increasing commute times**
- **Lower risk because the number of fatalities is not increasing with additional drivers or increase commute times**

U.S. Homicides and Homicide Rates



- **Population is increasing faster than the number of U.S. homicides**
  - **Number of homicides is relatively stable since 1998**
  - **Slight decrease points to continued population growth**

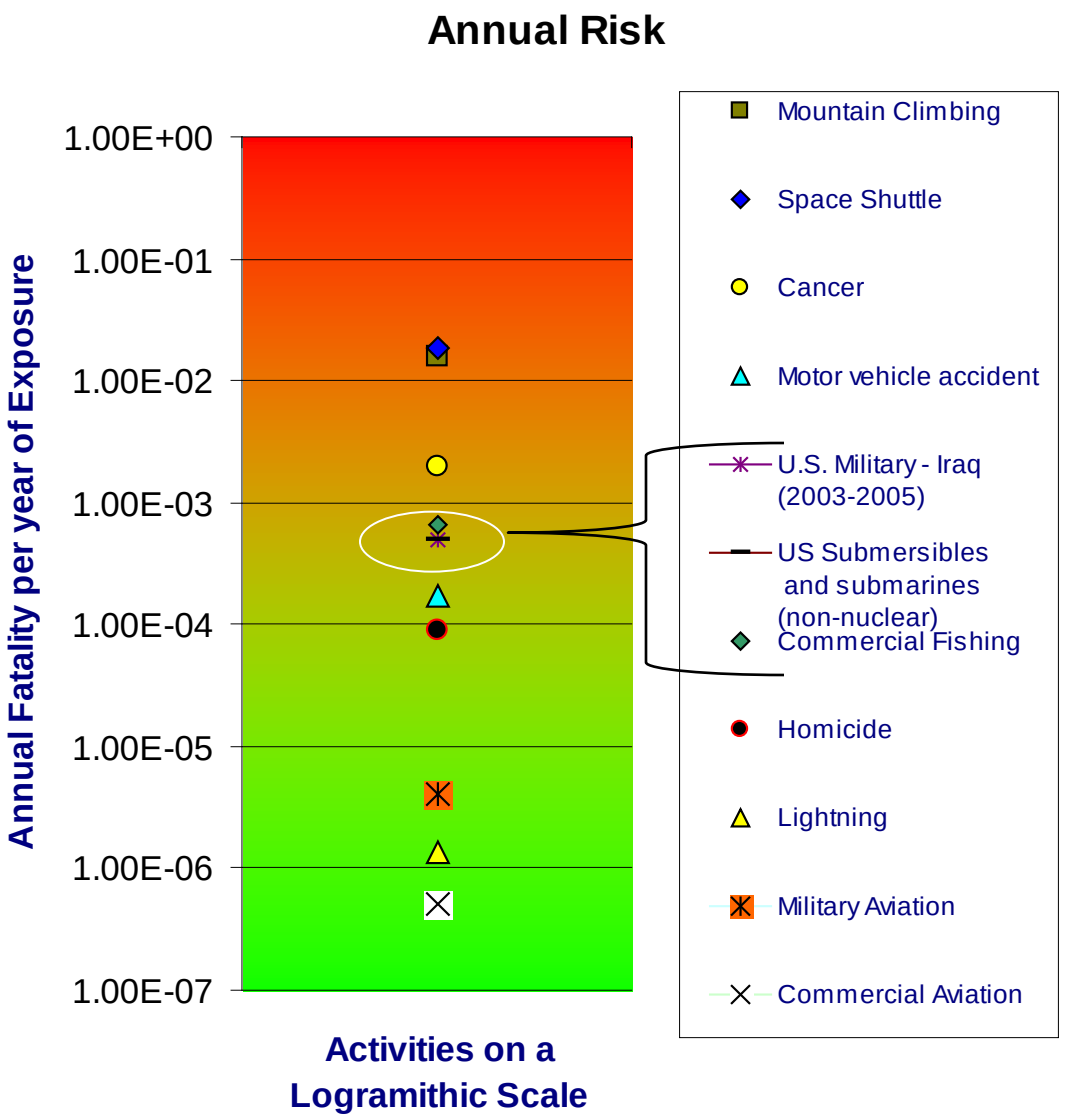
Comparison of Fatality Statistics



- **Significant differences in exposed individuals**
  - **WWII losses are an order of magnitude higher after considering exposure rates**
  - **Homicides considers entire U.S. population – increasing over time**
  - **Motor vehicle fatalities considers all drivers – increasing over time**

Annual Relative Risks Comparisons

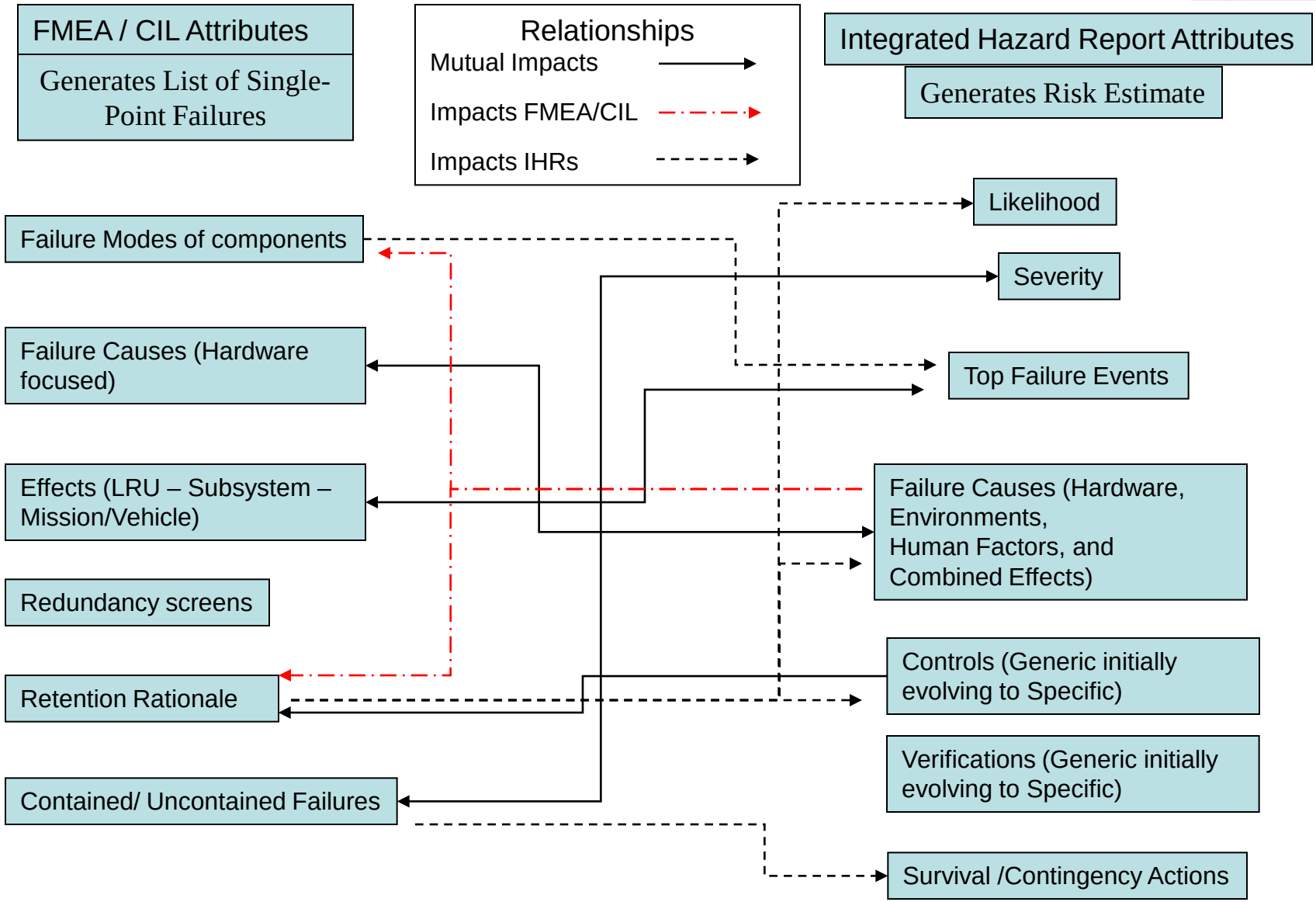
- **Unacceptable Risk**
  - 1E-03 Threshold
  - Generally not accepted
- **Marginal Risk**
  - 1E-06 to 1E-03
  - Accepted but considered a high-risk by the public
- **Acceptable Risk**
  - 1E-06 Threshold
  - No additional mitigations necessary



Crew Safety and Reliability Tasks

WBS 5.2.7 - Crew Safety and Reliability		
Working Group	**Deliverables**	**Assigned Tasks**
Ascent Risk Analysis	Ares I Crew Safety and Reliability Ascent Risk Analysis Report	• Provide integrated vehicle level PRA estimate • Identify key risk drivers and potential areas of improvement • Document ground rules and assumptions
Fault Detection, Diagnostics, and Response	Ares I Abort Conditions Report	• Identify abort conditions, assess which conditions must be monitored
	Ares I Abort Failure Detection and Response System Definition Document	• Define abort algorithms • Develop/ document abort architecture and recovery management • Sensor qualification logic
Integrated Aborts	Ares I Integrated Aborts Plan	• Outline approach and methods to support aborts
Probabilistic Design Analysis	Abort Risk Assessment Engineering Memorandum	• Physics-based analyses to assess severity of failure environments • Monte Carlo simulations of failure environments • Input to loss-of-crew estimate • Document modeling ground rules and assumptions
Reliability	Ares I Integrated failure Mode and Effects Analysis and Critical Items List	• Identify failure modes and results to the vehicle • Eliminate critical failure modes • Establish risk retention rationale
Safety	Ares I System Safety Analysis Report (SSAR)	• Provide recommend actions with regard to safety risks • Document hazard reports and FTA findings • Summarize critical/high-risk events
	Ares I Fault Tree Analysis Report (FTA)	• Identify initiating failure causes including non-hardware causes

Relationships Between CSR Groups



Example of FMEA/CIL and Hazards Interactions

Mutual Impacts

- Compare FMEA – Failure Causes and HR – Failure Causes which provides additional information to both analyses
- Compare FMEA – Effects (Mission/Vehicle) and HR – Top Failure Events and all HRs to confirm end effects and effects are captured which may result in modification of FMEA Retention Rationale or additional HRs.
- Comparison of the FMEA – Contained/Uncontained Failures and HR – Severity, Survival methods is used to confirm separate conclusions and the HR will also define any contingency actions which may be used to prevent harm to the vehicle or crew.

Impacts FMEA/CIL

- HR – Failure Causes may result in additional FMEA - Failure modes
- HR – Failure Causes may result in updating the FMEA/CIL - Retention Rationale based on new information.

Impacts IHRs

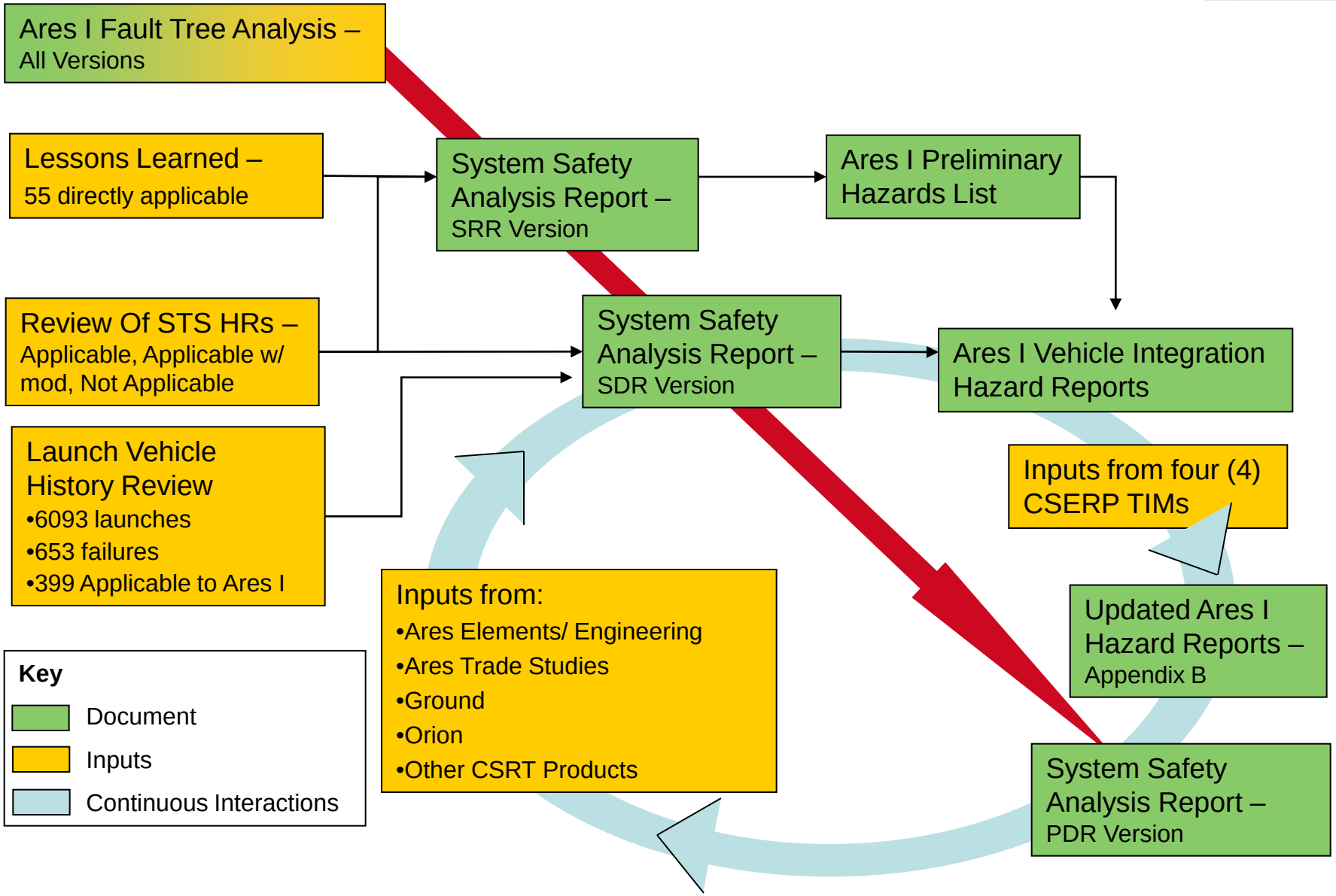
- FMEA – Failure Modes could result in additional Top Level Failures or a change in scope of specific HRs.
- FMEA – Retention Rationale can result in both adding/deleting failure causes of a particular hazard
- FMEA – Retention Rationale may be used to justify or update HR – Likelihood and/or add failure causes based on information in the Retention Rationale.
- FMEA – Retention Rationale may be used to justify or update HR – Controls based on information in the Retention Rationale.
- FMEA – Contained/Uncontained Failure field would impact which survival or contingency actions that would be effective given the failure mode.

Goals Flow-Down

Constellation Program Goals (A partial list)
1.1. Develop a crew launch vehicle to provide transportation to LEO as close to 2010 as possible to minimize the gap with Shuttle retirement
1.2. Provide a substantial increase in safety and reliability in the launch phase compared to present human transportation systems.
1.3. Provide a launch vehicle system that supports a substantial reduction in total mission operation costs compared to present human transportation systems.
Ares Project Goals (A partial list)
2.1. Ensure flight/ground safety, while meeting system performance requirements and achieving mission objectives. (1.1,1.2)
2.2. Utilize current, proven technology in the designs of the Ares I and Ares V. (1.2, 1.3)
2.3. Implement the Integrated Logistics Support approach and methodologies at the earliest stages to achieve the lowest ownership costs. (1.3)
Vehicle Integration Goals (Technical Performance Metrics)
3.1. Mass to Orbit (2.1)
3.2. Loss of Mission (2.1)
3.3. Launch pad processing time. (2.3, 2.3)

Vehicle Integration Goals (Technical Performance Metrics)
3.1. Mass to Orbit (2.1)
3.2. Loss of Mission (2.1)
3.3. Launch pad processing time. (2.3, 2.3)
Crew Safety and Reliability Goals (A partial list)
4.1. Generate a integrated vehicle level PRA estimate (Loss of Mission / Loss of Crew) (3.2)
4.2. Ensure that abort conditions and necessary sensors are identified (3.2)
4.3. Eliminate or control safety hazards and their causes through design (3.2)
Safety Working Group Goals (A partial list)
5.1. No Loss of Life (Public, Flight or Ground Crew) (4.1, 4.2, 4.3)
5.2. No Ares I failures which trigger an abort over the program life (4.1, 4.3)
5.3. No repeat “Lesson Learned”(4.2, 4.3)
5.4. Impact the design based on hazard analyses (4.1, 4.2, 4.3)
5.5. Pass all Constellation Safety and Engineering Review Panel (CSERP) reviews (4.2, 4.3)

System Safety Analysis Report Maturation Process



Ares I Shared Attributes

- **Development History**
  - **Pre-SRR and Pre-SDR review of STS HRs.**
  - **Pre-SRR Lessons Learned review produced 55 directly applicable items, 35 from manned missions and 20 from ELVs.**
  - **Reviewed over 6093 launches including 653 failures or which 399 (appx. 61%) were judged as applicable to Ares I.**
  - **The IFTA and SSAR will be formally base-lined after CDR at which point it will be under configuration control**
  - **The IFTA and SSAR is a "living documents" that will be updated throughout the life of the Constellation Program**
- **The Ares I IFTA and SSAR serves as input data to multiple related analyses (e.g., FDDR, Abort Conditions Report, Ascent Risk Analysis, Logistics Support Analysis, etc.)**

Ares I Safety Generated Documents

- **Ares I Fault Tree Analysis Report (FTA)**
- **Purpose:**
  - Primary objective was to identify initiating causes which could result in the top undesired event – Loss of Life (Flight crew, ground crew & public)
  - The analysis logic is structured such that mission phase (time), system failures of any element or interface, and all environments are considered

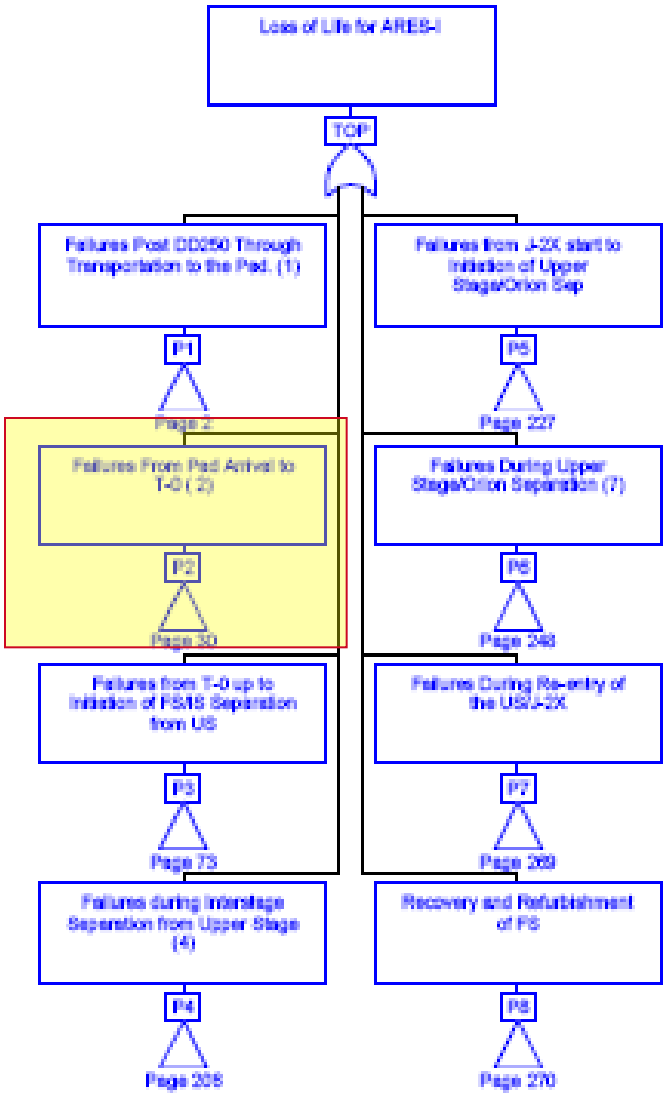
- **Ares I System Safety Analysis Report (SSAR)**
- **Purpose:**
  - Provide an overview of the results of the FTA and all integrated vehicle Hazard reports
  - Provides summaries of the vehicle, operations, and timeline of critical/ high-risk events to assist reader to understand the analysis
  - Provides critical recommendations to management to address identified areas of high safety/mission risks

FTA Overview

- Primary objective was to identify initiating causes which could result in the top undesired event – Loss of Life (Flight crew, ground crew & public)
- The Fault Tree Analysis only addresses integrated vehicle failures – Element failures leading to overall loss of vehicle/mission are addressed in Element FTAs. Integrated failures due to Element specific causes are captured through transfers.
- FTA is a “living document” that will undergo numerous updates prior to CDR
- Ground rules and Assumptions are included in the document

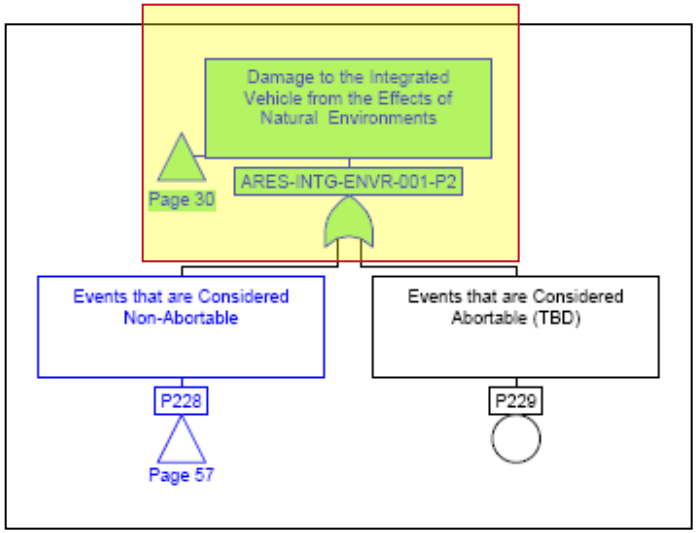
FTA Snapshot - Example

- **Example:** Top block Loss of Life (Flight crew, ground crew & public)
- **Divided by Mission Phase**
  - Failures From Pad Arrival to T-0
  - Non-traditional but assisted in evaluating functions at different times and conditions
- **Ares Internal (VI) Transfer**
  - Triangle to page within VI



FTA Snapshot - Example

- **Subdivided by VI Hazard Report as necessary**
  - Hazard Reports are color-coded
- **HR – ARESI-INTG-ENVR-001 highlighted**
  - “Events that are Considered Abortable (TBD)” is undeveloped in lower right diagram
  - Triangle transfer indicates branch is further developed elsewhere



FTA Analysis Results

- **The analysis logic reflects the physical failure methods by including all environments, Element specific causes, and possible combinations from multiple sources**
- **The report documents all known failure causes and tracks those relationships through transfers with Ares Elements (FS, US, and USE) and other Constellation projects (Orion, Ground, etc.)**
- **The FTA feeds into the System Safety Analysis Report through the multiple hazard reports**
- **FTA contains a high level of detail for an integrated system at this design phase**
  - All mission phases
  - Consistent with division of hazard report and content
  - Many levels in depth to capture critical interactions at the integrated level

SSAR Overview

- **The System Safety Analysis Report is the combined results of the FTA, lessons learned, applicable STS hazard reports, and independent analyses**

- **The report documents all know failure causes and tracks those relationships through transfers with Ares Elements (FS, US, and USE) and other Constellation projects (Orion, Ground, etc.)**
  - Executive summary section
  - Provides nine (9) specific areas/issues identified during the analysis
  - Section with summaries of all VI hazard reports
  - Individual Hazard Reports and supporting sections of the FTA are located in Appendices

Expectations

- **Communicate issues and concerns sooner rather than later.**
- **Support milestone project reviews of both the VI and Elements – plan to develop HR (inputs needed, key dates, analysis methods, needed support) discuss plan with the right design teams, - document.**
  - Deliver high-quality products on time. Includes information that the designers and management needs to understand, regularly update analysis and results, document inputs and assumptions, address gaps and requirements as analysis identifies them.
- **Support the Constellation Safety and Engineering Review Panel**
- **Ownership of Hazard reports, agreement that identified work can be accomplished to support the**
  - Delivery schedule,
  - Identify key points of contact
  - Participate in meetings regularly
  - Identify tasks,

Planning and Communication

- **Strategic planning is one of the keys to being effective**
  - Support program and project milestones
  - Define deliverables or tasks to be completed
  - Set goals of the safety analysis team - such as: “No Ares I failures which trigger an abort over the program life”
  - Timely technical assessments

- **Communicate with other groups and organizations - Remember that the more your products are used the greater value you have to the project!**
  - Deliverables including content and limitations
  - Input needed for analysis
  - Identify due dates
  - Define relationship with other groups
  - Effectively communicate in multiple forums: reports, official documents, or briefing

Conclusion

If space exploration is to continue, safety must increase and the overall cost must continue to be reduced.

- **Early involvement**
- **Increase safety through incorporating the right safety requirements into the program and the necessary hardware controls earlier**
- **Participated in all design cycles**
- **The hazard analysis, along with a number of supporting analyses must be fully integrated from the beginning of the design concept phase**
- **Reduce the number of design cycles, development costs, and long-term operational costs by coordinating work across multiple disciplines**

References

1. NASA (2002). A Walk Around the Space Shuttle, FS-2002-08-133-MSFC. *NASA Facts,* Pub 8-40062
2. NASA (2002). NASA Facts: Shuttle Propulsion Trivia, FS-2002-08-134-MSFC. *NASA Facts,* Pub 8-40061
3. icasualties.org (2008). Iraq Coalition Causality Count,
4. The Chicago Council on Global Affairs, (2008). *Global Views 2008: Troubled by Loss of Standing in the World, Americans Support Major Foreign Policy Changes*, The Chicago Council on Global Affairs, Chicago, IL, pg. 6. http://www.thechicagocouncil.org/UserFiles/File/POS_Topline%20Reports/POS%202008/2008%20Public%20Opinion_Foreign%20Policy.pdf
5. U.S. Department of Justice Federal Bureau of Investigation, (2008). U.S. 2007 Homicide statistics,
6. National Highway Traffic Safety Administration, (2008). Motor Vehicle Traffic Crash fatality counts & Estimates of People Injured for 2007. *DOT HS 811 034*,
7. NASA (2008). Kennedy Space Center: Frequently Asked Questions, http://www.nasa.gov/centers/kennedy/ about/information/shuttle_faq.html#10
8. United States Air Force, (2008). FY2009 Budget Estimates, p. 1-13.
9. Stiglitz, Joseph E., Bilmes, Linda J., (2008). *The Three Trillion Dollar War: The True Cost of the Iraq*, W.W. Norton, NY, NY, pp 100-101.