



IAASS Conference

October 21, 2008

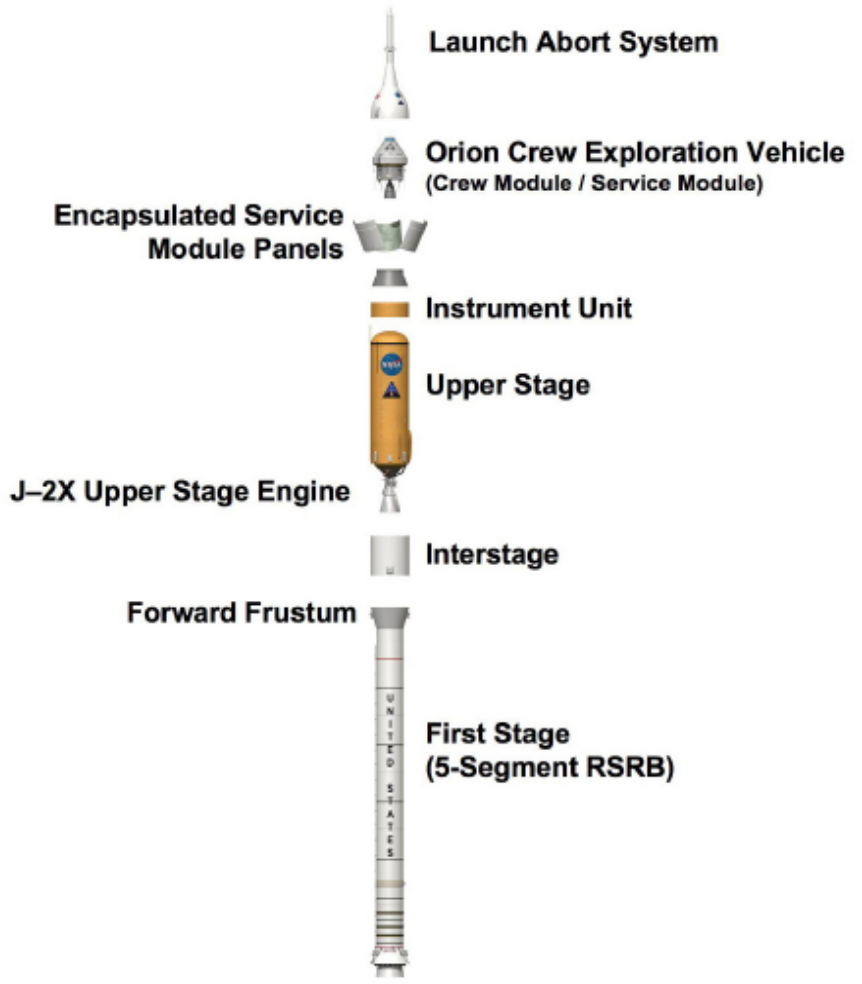


EVOLUTION OF SAFETY ANALYSIS TO SUPPORT NEW EXPLORATION MISSIONS

Chad W. Thrasher
NASA/MSFC/QD34



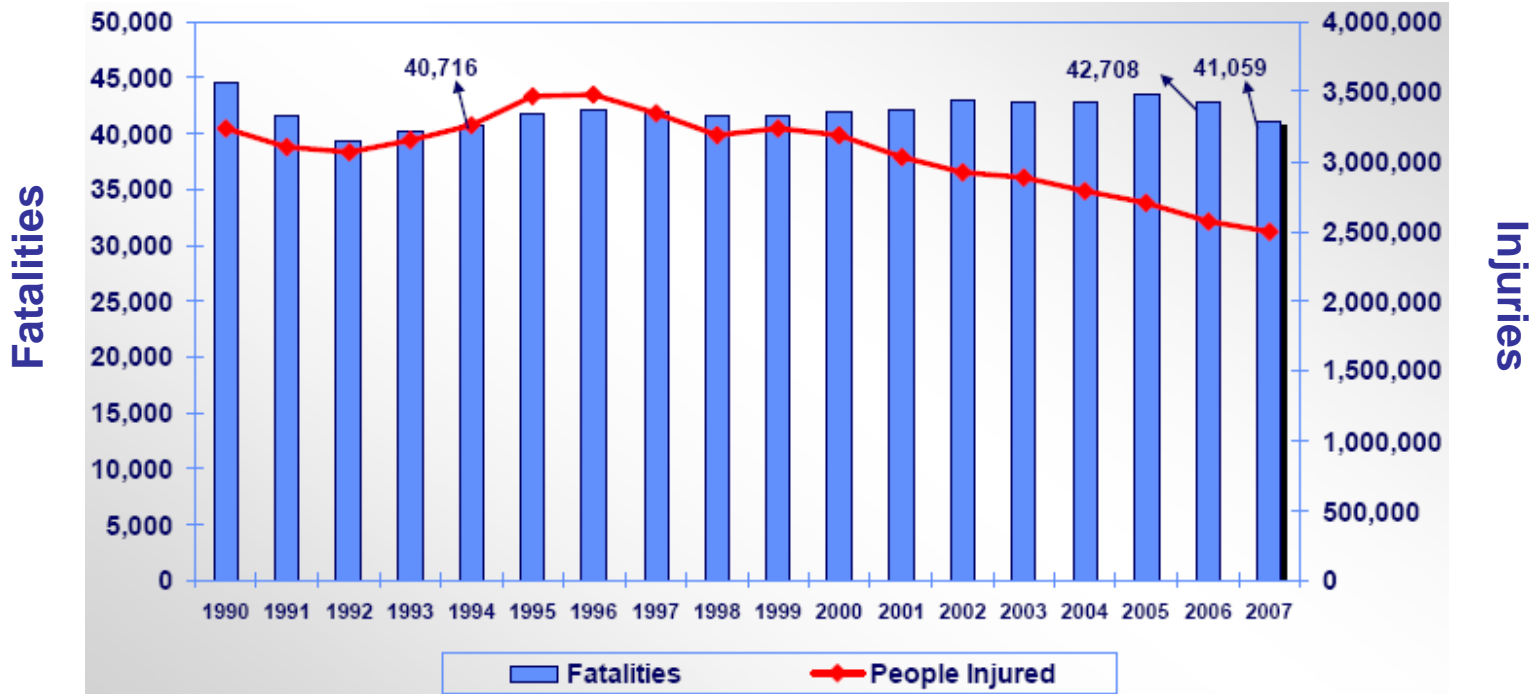
Ares I and Ares V



Concept image of Ares V elements. (NASA MSFC)



People Killed and Injured In Traffic Crashes, by Year



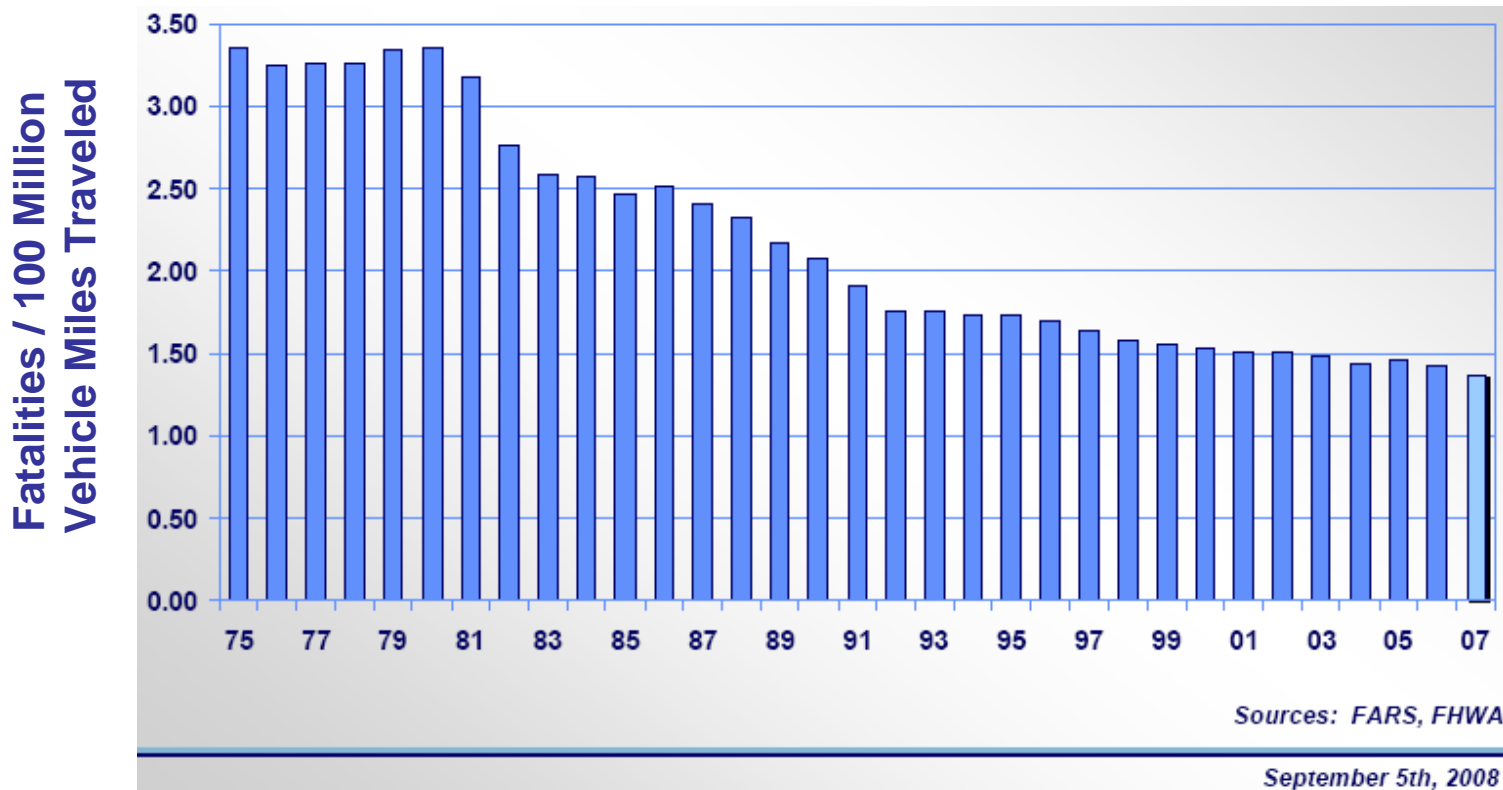
Source: FARS

September 5th, 2008

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



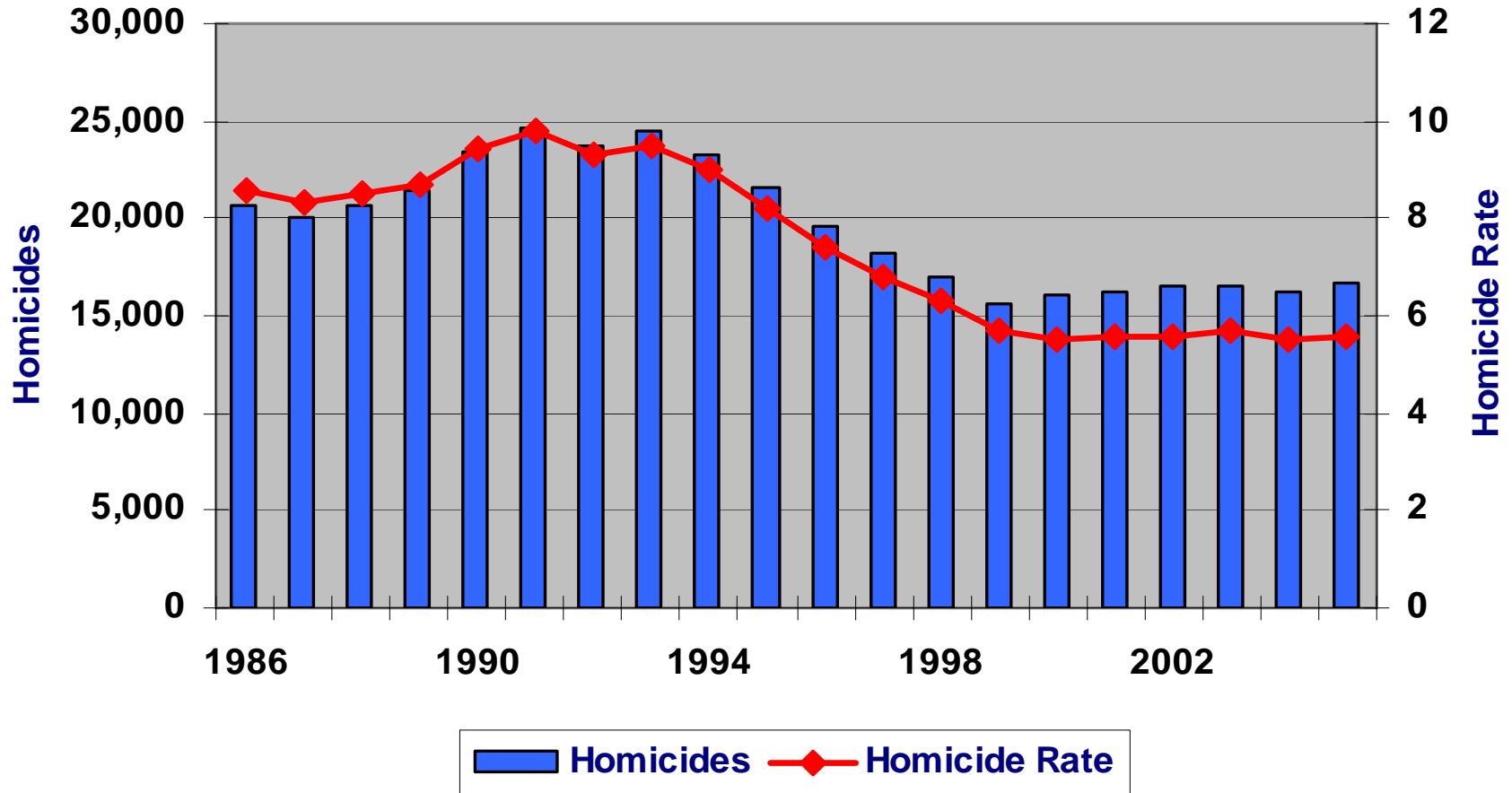
Fatality Rate Per 100 Million VMT, by Year



- ◆ 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



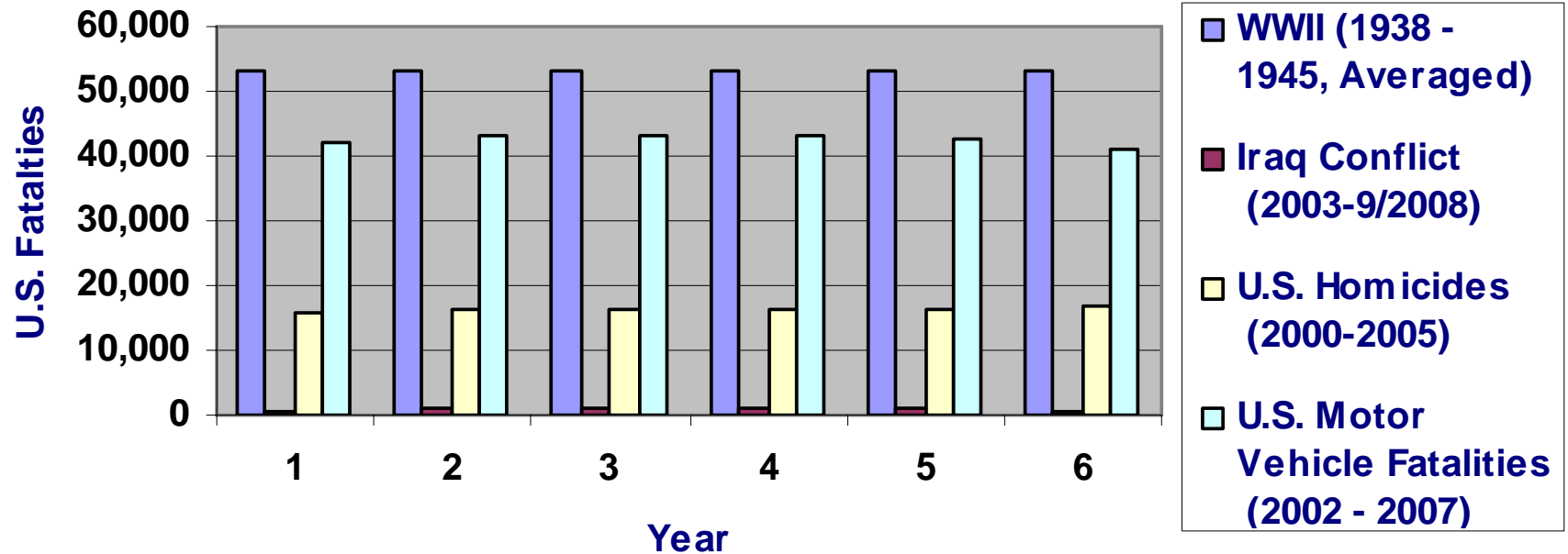
U.S. Homicides and Homicide Rates



- ◆ 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

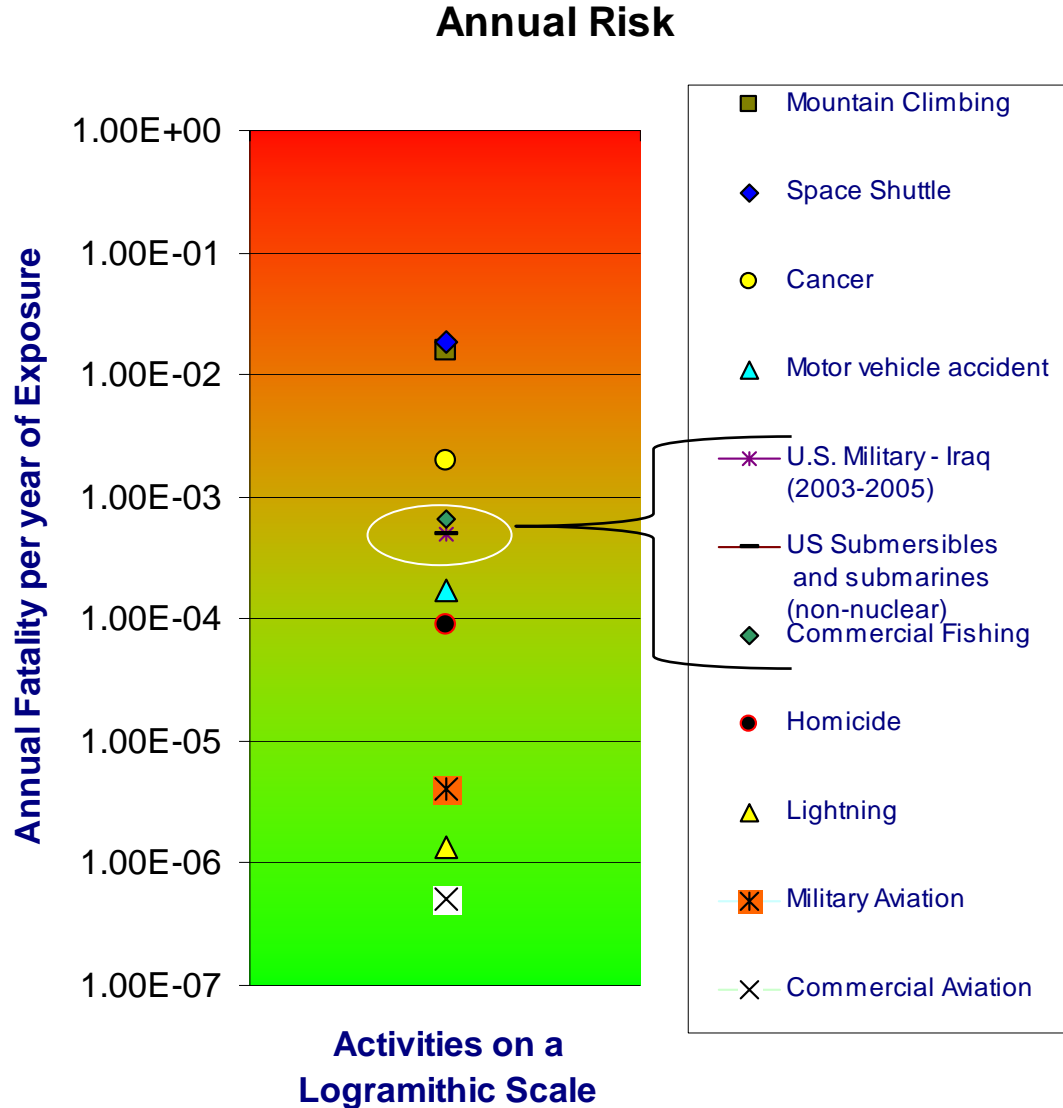
- 1E-03 Threshold
- Generally not accepted

◆ 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





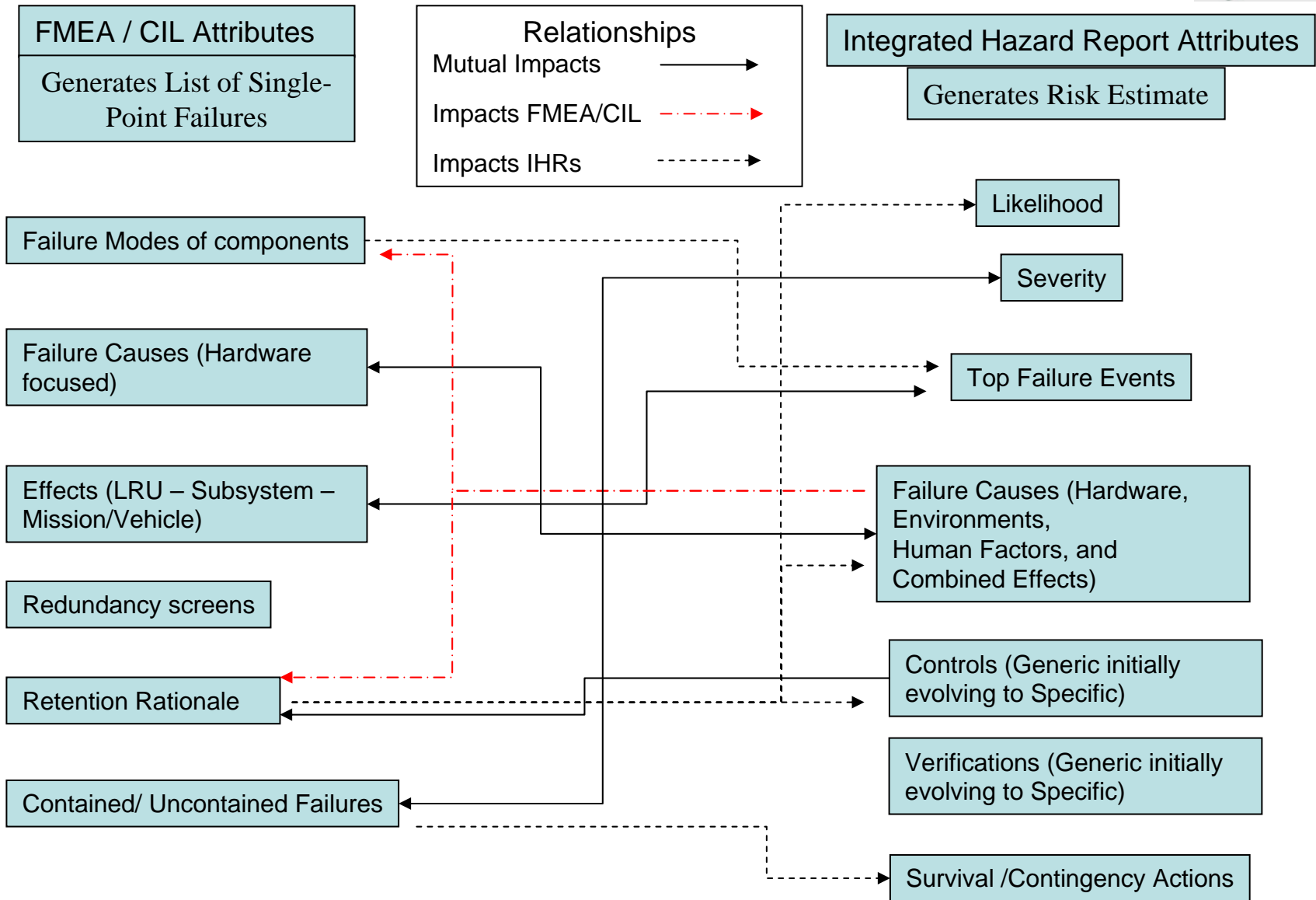
Crew Safety and Reliability Tasks



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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Identify abort conditions, assess which conditions must be monitored
	Ares I Abort Failure Detection and Response System Definition Document	<ul style="list-style-type: none"> • Define abort algorithms • Develop/ document abort architecture and recovery management • Sensor qualification logic
Integrated Aborts	Ares I Integrated Aborts Plan	<ul style="list-style-type: none"> • Outline approach and methods to support aborts
Probabilistic Design Analysis	Abort Risk Assessment Engineering Memorandum	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Identify failure modes and results to the vehicle • Eliminate critical failure modes • Establish risk retention rationale
Safety	Ares I System Safety Analysis Report (SSAR)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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

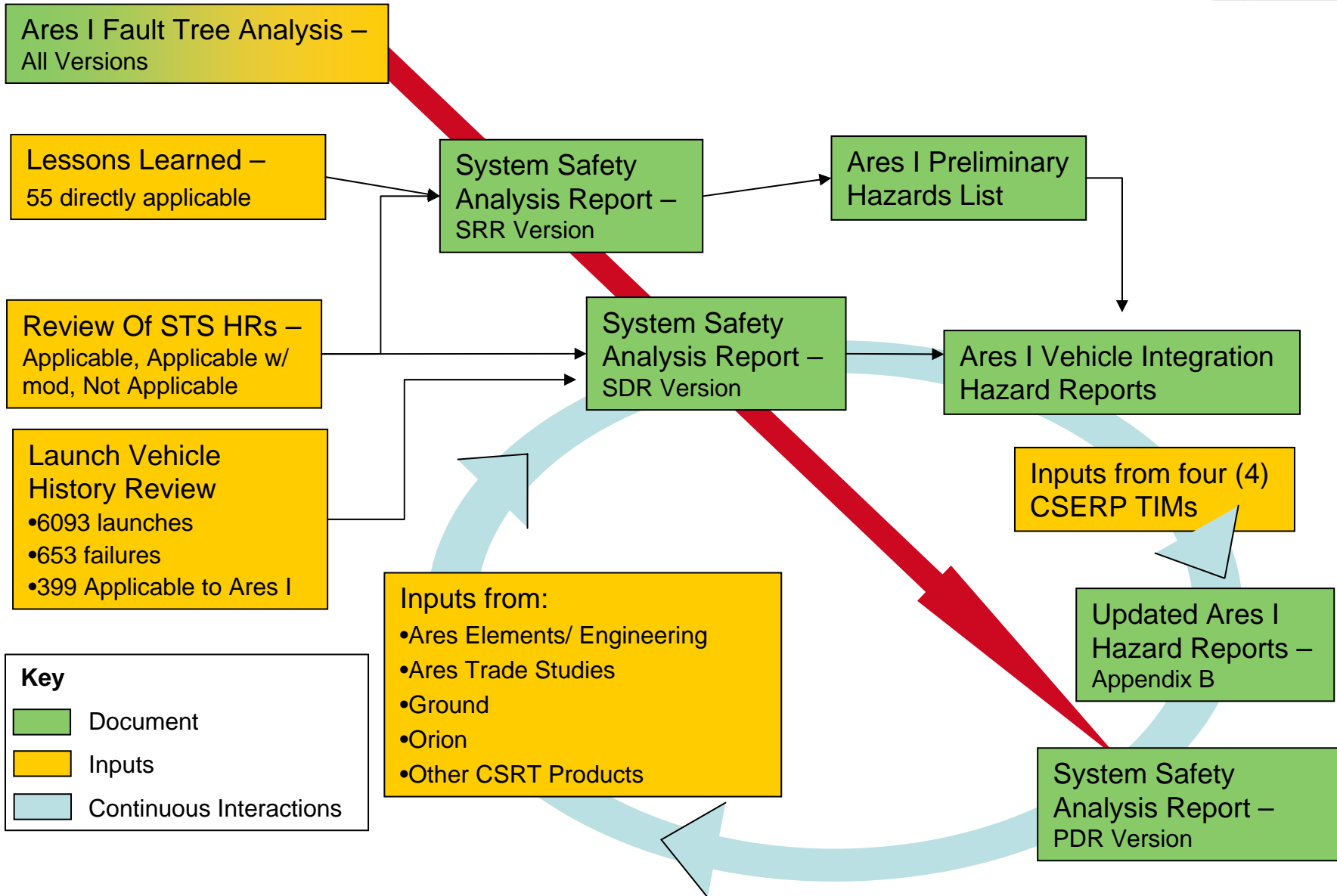


Constellation Program Goals (A partial list)
1.1. Develop a crew launch vehicle to provide transportation to LEO as close to 2010 as possible to minimize the gap with Shuttle retirement
1.2. Provide a substantial increase in safety and reliability in the launch phase compared to present human transportation 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



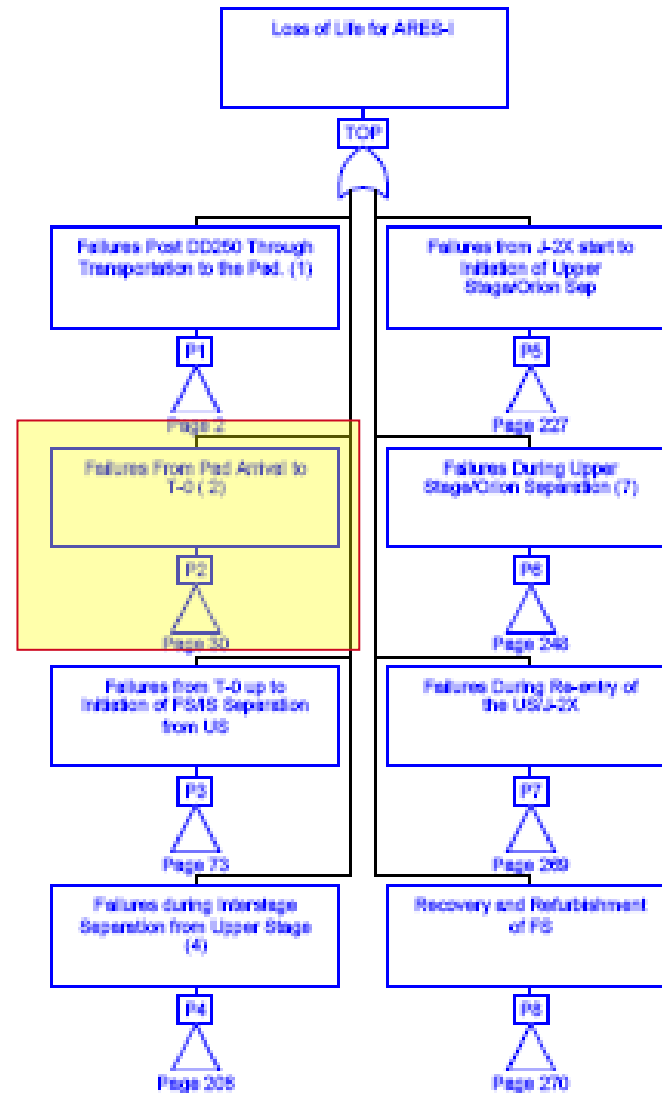
- ◆ **Primary objective was to identify initiating causes which could result in the top undesired event – Loss of Life (Flight crew, ground crew & public)**
- ◆ **The Fault Tree Analysis only addresses integrated vehicle failures – Element failures leading to overall loss of vehicle/mission are addressed 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

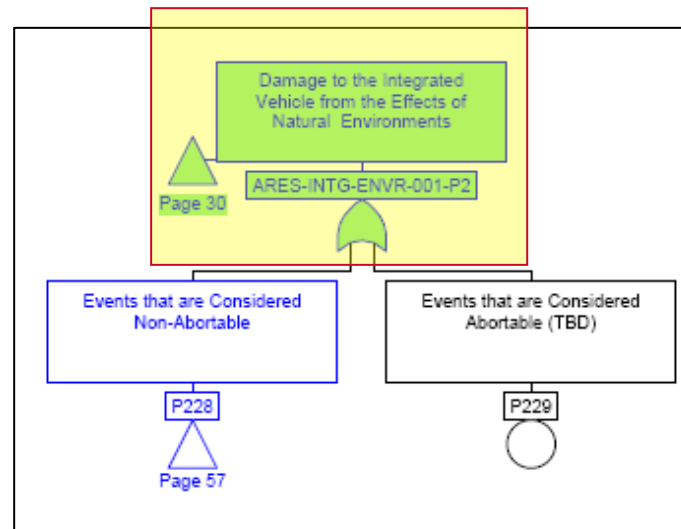
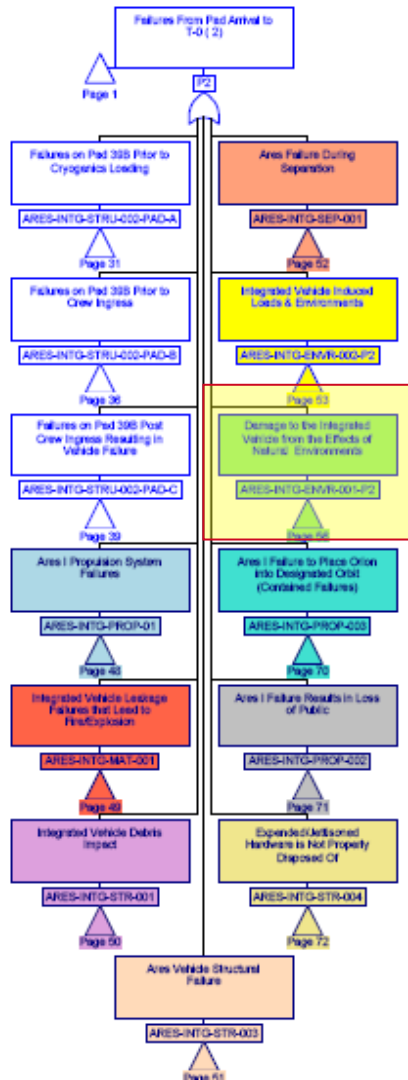


- ◆ Subdivided by VI Hazard Report as necessary

- Hazard Reports are color-coded

- ◆ HR – ARES-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 known 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](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.