

ARES
CORPORATION



Constellation Integrated Hazard Analyses – Overcoming the Challenges

Michael J Massie
NASA SE&I Constellation IHA LEAD

Presented by
Dr. J. Steven Newman
ARES Corporation



Constellation Integrated Hazard Analysis - AGENDA

- ◆ **The 4 Keys to Generating a Large Scale Integrated Hazard Analysis**
 - **Key 1: IHA must have a Methodological Structure**
 - **Key 2: IHA program needs a good plan of attack and execution**
 - **Key 3: IHA Must have Good Reliable Communication Paths**
 - **Key 4: IHA Must have Right People doing the Job**
- ◆ **Avoiding Some of the Pitfalls**
- ◆ **Conclusion and Summary**

Key-1: Structure and Method

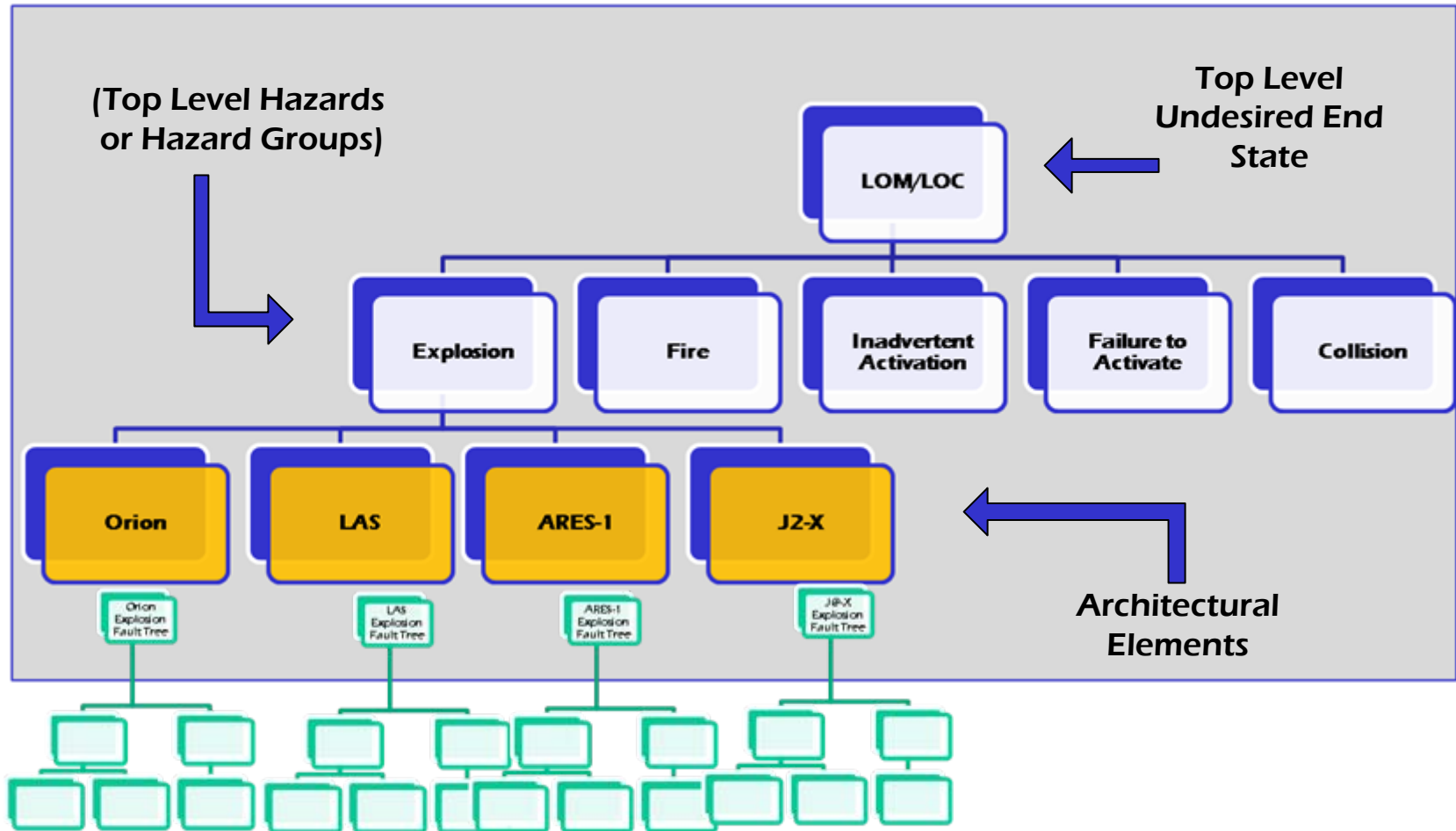
- ◆ Large Scale Hazard Analyses must be Top Down and Organized to be manageable and Effective

- ◆ Bottoms Up Approach Untenable - Integration at the Top Level has some similarities to a payload safety analysis but due to level of complexity and sheer volume of information it is not possible to approach it the same way.
 - Integrated Analysis of a small payload can be built from separate analyses of each set of components
 - Each box can have a separate analyses then an analysis of the boxes working together can be performed.
 - To simply escalate this approach for massive programs is cost prohibitive
 - » Example: ISS US Lab has 400,000 parts, if each of 44 major elements of ISS had same number and 1 assessment for each we would quickly require over 17 million assessments plus the integrated assessments from each developer plus the overall integrated assessment.
 - 8 hrs per assessment is 153 million man-hours
 - » Even elevating to starting at the box level is prohibitive

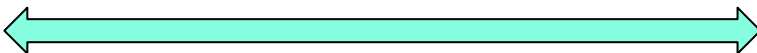
KEY 1a: Organizing Around the Hazard Tree

- ◆ **IHA Hazard Tree Structure Built to House Constellation Fault Trees**
 - **To build a true fault tree from Loss Of Crew down would result in the primary undesired events/conditions (ie: Hazards) scattered throughout the tree and a repeated frequently as many different systems can create common hazards**
 - **Tree is 1st built from Hazard Point of View**
 - **Top of Tree then Organizes the credible hazards or hazard groups in accordance with hazards that can credibly arise from architecture**
 - **Each hazard arises from potential hazard causes**
 - **Each hazard cause arises from Failure of the Hazard Controls**
 - » **Development of the “Loss of Controls Trees” is the actual traditional fault trees built around vehicle failures**
- ◆ **Thus, Major Large Scale IHA is built from Organizing Hazards around architecture and then Hanging true Fault trees from the hazard causes.**

Notional Integrated HA Structure



Seek Grouping Opportunities, Identify Common Solutions, Identify Gaps in Element Analysis



Key 1b: Hazard Groups versus Hazards versus Hazard Cause

- ◆ **Hazard Report Building also Must Consider Reorganization from Traditional Payload Safety Approaches**
 - **Building separate HRs for each true Hazard results in thousands of hazard reports**
 - **Difficult to track, manage and keep your head around**
 - **Where appropriate Top Level IHA Slightly Redefines Hazards and Hazard Causes**
 - **Many Top Level IHA Reports are Collections of Lower Level Hazards or Hazard Contributors**
 - » **Thus each report is often really a Hazard Group**
 - » **Each Hazard Cause is a traditional Hazard Report of Its own**
 - **Sub causes sometimes are needed but it turns out these are rare**
 - **Occasionally IHA turns the concept upside down as well to manage the data**
 - » **A single hazard Cause can sometimes be a Program Level mitigation that is common to numerous true hazard causes**
 - **This is effectively Documenting a Single Hazard Control on a Hazard Cause form and having the remaining controls in the individual hazard causes**

IHA Structure – Tools

- ◆ **Hazard Tree is Organized Like Traditional Fault Tree but Divides program by hazards 1st then supports each Hazard Cause with traditional Tree**
 - **Any Software Tool that Displays the Tree Structure is Acceptable**
- ◆ **Linking together the Lower Level Data to the upper Level Data Require a Massive Scale Mapping Effort**
 - **Tables are Built which identify which hazard Causes are linked to which and who needs what data from who**
- ◆ **Managing the ability to link analyses is Next Major Step**
 - **All elements building their own their own way**
 - **Near PDR Standards need set that make all the analyses linkable**
 - **Common definitions for Hazard Groups**
 - **Common Numbering System**
 - **Common Ground rules for Hazard Cause documentation**

IHA Master Matrix Example

| | A | B | AK | AL | AM | AN | AO | AP | AQ | AF |
|----|----------------------|----------------------|-------------------------|------|-------|-----|------------|-------------|-----|----|
| 1 | | | Hazard Cause Management | | | | | | | |
| 2 | Hazard Report Number | Hazard Report Cause | SE&I | Ares | Orion | EVA | Ground Ops | Mission Ops | ISS | PO |
| 3 | CEV-CM-AVN-001 | HR #1 Title | S | S | P | S | S | S | S | |
| 4 | CEV-CM-AVN-001 | HR #1 Cause 1 Title | | | | | | | | |
| 5 | CEV-CM-AVN-001 | HR #1 Cause 2 Title | | | | | | | | |
| 6 | CEV-CM-AVN-001 | HR #1 Cause 3 Title | | | | | | | | |
| 7 | CEV-CM-AVN-001 | HR #1 Cause 4 Title | | | | | | | | |
| 8 | CEV-CM-AVN-001 | HR #1 Cause 5 Title | | | | | | | | |
| 9 | CEV-CM-AVN-001 | HR #1 Cause 6 Title | | | | | | | | |
| 10 | CEV-CM-AVN-001 | HR #1 Cause 7 Title | | | | | | | | |
| 11 | CEV-CM-AVN-001 | HR #1 Cause 8 Title | | | | | | | | |
| 12 | CEV-CM-AVN-001 | HR #1 Cause 9 Title | | | | | | | | |
| 13 | CEV-CM-AVN-001 | HR #1 Cause 10 Title | | | | | | | | |
| 14 | CEV-CM-AVN-001 | HR #1 Cause 11 Title | | | | | | | | |
| 15 | CEV-CM-AVN-001 | HR #1 Cause 12 Title | | | | | | | | |
| 16 | CEV-CM-AVN-001 | HR #1 Cause 13 Title | | | | | | | | |
| 17 | CEV-CM-AVN-001 | HR #1 Cause 14 Title | | | | | | | | |
| 18 | CEV-CM-AVN-002 | HR#2 Title | S | S | P | S | S | S | S | |
| 19 | CEV-CM-AVN-002 | HR #2 Cause 1 Title | | | | | | | | |
| 20 | CEV-CM-AVN-002 | HR #2 Cause 2 Title | | | | | | | | |
| 21 | CEV-CM-AVN-003 | HR#3 Title | S | | P | | | S | S | |
| 22 | CEV-CM-AVN-003 | HR #3 Cause 1 Title | | | | | | | | |
| 23 | CEV-CM-AVN-003 | HR #3 Cause 2 Title | | | | | | | | |
| 24 | CEV-CM-AVN-003 | HR #3 Cause 3 Title | | | | | | | | |
| 25 | CEV-CM-AVN-003 | HR #3 Cause 4 Title | | | | | | | | |
| 26 | CEV-CM-AVN-003 | HR #3 Cause 5 Title | | | | | | | | |

Notes \ Master / Orion Mods / ARES Mods / EVA Mods / HRMapping / HSIR / Causes / |

Ready

IHA - Plan

◆ A Good Plan is Required

- Address how the lower level analyses will be fit with Integrator
- Address Schedule on doing this
- Document How this is accomplished
- Document Ground rules
 - Who Covers What
 - How to resolve areas of overlap and gaps
 - How data will be exchanged and when
 - How issues and concerns are identified tracked and elevated through program
 - » Ground Rules on which ones get elevated
 - How changes will be address
 - Expected Interteam Support at Reviews and Coordination Meetings and TIMS
 - etc

IHA- Communications

- ◆ **Reliable communications paths must be established**
 - **Between Integrator and Developers**
 - **Between Developers**
- ◆ **A consistent set of Meetings**
 - **Eg: IHA Working Group (IHA WG) meets every other Wed on Constellation**
 - **SRQA and/or SEI Reps from Every provider are Required to Attend**
- ◆ **Accurate phone and Email lists available to all participants**
- ◆ **Commitment to be responsive to each other**
- ◆ **Common Websites where all data can be shared**

IHA - Personnel

- ◆ **Leadership**
 - Many features are needed in a good leader one of the most critical is the ability to think at all levels and seamlessly shift between them
 - Central Organization and Leader to Resolve Issues and Have Ownership and Responsibility for Overall IHA Project
 - Adequate number of Lead personnel to handle major program Segments
 - Constellation uses 1 for Projects and 1 for Level 2 Internal Activities
 - Each Project/Element must have Identified Reliable Leader who is Responsive
- ◆ **Shared Effort Between Design and SRQA**
 - Early initiation usually works best by having the HA experts (SRQA) start the Analysis
 - » Know how to think about IHA
 - Most Effective Content However Comes from Design Organization
 - » Must Own HRs throughout Analysis
 - » Should take them over once well developed

SUCCESS CHECKLIST -1

◆ Maintain Top Down Discipline

- Work through Each Hazard/Cause one at a time and tell 1 story at a time
 - » Start at top undesired event

◆ Leverage FMEA – Leverage Functional & Ops Haz Analysis

- FMEA works from Bottom up
 - » Allow it to be source data
 - » Allow where it picks up to be your stopping point
- Functional Hazard Analysis and Operating and Support Hazard Analysis provide excellent Operational Looks at program hazards
 - » Use them to augment the IHA and identify any gaps

◆ Implement Stopping-Point Rules

- look for commonality to give you a stopping point
- Look at reasonable span of control

◆ Critically Examine Control Profile

- If you find yourself documenting 12 controls to a single hazard cause there is often something wrong in the approach to the hazard analysis
 - » Are you really trying to cover multiple causes in one cause
 - » Controls really aren't controls

SUCCESS CHECKLIST -2

◆ The Right People

- **Assure they are trained in what you are looking for**
- **Assure they are able to understand the HA way of thinking**
- **Why things won't work versus why they will work**
- **Able to repackage the program in Safety Language**
- **Able to communicate in Safety Language**
- **Able to Derive specific Hazard and Causes from initially nebulous Safety Requirements**
- **Good Technical Knowledge of the Systems under Review and can use that knowledge**
- **Experienced in Program Analysis and able to debate with Senior Technical Personnel**
 - **A College New hire has almost no chance against a 25 year Electrical Design veteran with an attitude**

SUCCESS CHECKLIST -3

◆ “Document All Assumptions” Discipline

- Unwritten and unexamined assumptions have lead to mistakes and errors in every HA**
 - On-orbit or In-Flight and Ground incidents have occurred that were not picked up by HA because of Ground rules that either were forgotten or lost their applicability**
 - » Eg: Orbiter wiring was assumed to be structure in Original Hazard Analysis**
 - Essentially valid assumption 25 years ago**
 - Aging eroded this assumptions validity and massive wiring reassessments and reworks were required AFTER failures started occurring**
 - Revisit assumptions periodically**



Constellation – IHA Conclusion

- ◆ **A good large scale Integrated hazard analysis will have an infrastructure at it's foundation that allows for a good well integrated analysis to be built**
 - **Analysis Structure**
 - **Good Plan**
 - **Good Reliable Communication Paths**
 - **Right Personnel for the Job**