System Safety Challenges in Rapid Collaborative Development

Lynece Pfledderer

Panel: G-48 Most Pressing Issues Facing System Safety

34th International System Safety Conference, Orlando, FL

AGENDA

- Defense Acquisition Environment
- Rapid Collaborative Development
- Challenges to System Safety
- Lessons Learned
- Discussion

DEFENSE ACQUISITION ENVIRONMENT

- Some Acquisitions are Becoming More Like Commercial
- Less Funding Available, More Competition
- More Affordability, Sustainability Focused
- Many Adopting Agile Design and Operations Lifecycles
- Driving More IRAD Before RFP
- More Foreign Military R&D
- Urgent Need Procurements

Investment requirements are increasing

Rapid Collaborative Development Programs Becoming More Common

RAPID COLLABORATIVE DEVELOPMENT MAY INCLUDE:

- **Repurpose, reuse of products**
- **Combining parts of two or more products to make a different product**
- **New technologies**
- **Often complex**
- **Urgent need**
- **Little to no government specs**

Initial development often without formal Customer requirements

May be specialized products being used in new ways, different combinations, new capabilities, or by different users

CHALLENGES SYSTEM SAFETY MAY ENCOUNTER:

- Same Challenges as With Agile Lifecycle
- Too Little Time, and Lifecycle Not Waterfall
- New Technology/COTS/Unknown Legacy Hazards = Don't Know What You Don't Know
- First to Market, Affordability = Only Do What Have To Do Now, Nothing More
- Unrealistic Customer, Business and Management Expectations
- IRADs = "Not Enough Money for Safety"
- Safety Not Included in Specs or SOW
  - No/Low Budget
  - Must Decide Standards, Tasks, Level of Safety, etc.
- Product Liability

Change can be uncomfortable

CHALLENGES SYSTEM SAFETY MAY ENCOUNTER:

- Safety requirements harder to identify, estimate and prioritize. Frequently reassess and change
- Government Safety Boards Not Included
- Often Fluid Staffing and Geographically Dispersed Team of Teams With Multiple Contractors and Unknown Suppliers. SSE often part-time
- Operational Scenarios, Functions, Test Approach May Not Be Well Thought Out
- Intended Use, Operational Environment and User May Not Be Defined
- Inadequate Subsystem and Integration Tests
- Operational Test Hazards
- R&D Safety Culture, Often Inexperienced in System Safety
- Lack of Qualified Staffing

… How do we meet the safety challenges?

SYSTEM SAFETY LESSONS LEARNED

- Same lessons learned and guidelines as Agile, plus…
- Must manage expectations of Customer, Management, Business Development and Design Engineering
- System Safety planning, initial analysis of known functions and high level requirements should be early as possible before RFP
- System Safety must be design partner - close teamwork and matching tempo is essential. Also results in stronger working relationships
- Limit to priorities and things needed now, and determine what can be delayed until next phase

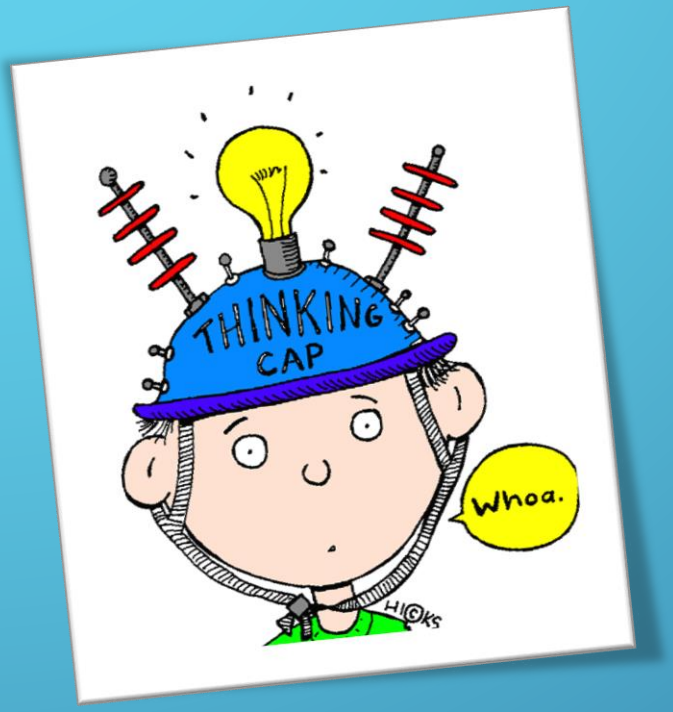
SYSTEM SAFETY LESSONS LEARNED

- Scale, streamline and tailor System Safety and Software Safety program and processes
- Match safety data submittals to development cycles, and shape customer expectations to process outputs
- If possible, obtain pre-program agreement on how much analysis/modeling/testing is enough for “acceptable” risk
- Constant communication with customer so they understand what is being done, concerns and why changes were implemented
- Work early and often with safety boards whether required this phase or not

SYSTEM SAFETY LESSONS LEARNED

- If using Agile, the multiple reviews provide better understanding of implementation details
- Usually requires highly experience System Safety Engineers.
  - Fast pace, must be able to provide quick and detailed understanding, and prioritize. And if Agile is used must be able to handle constant change and multiple activities occurring at once.
- Traceability and documentation is very important
- Must training SSE professionals how to apply System Safety to rapid development efforts
- Expect constant change

AGILE AND RAPID COLLABORATIVE DEVELOPMENT IS CHANGING THE SYSTEM ENGINEERING PROCESS



How do we ensure safety of rapid development systems?

How will we adapt, change and scale System Safety processes?

How do we equip System Safety Engineers to be effective in these environments?

Can we influence the R&D and acquisition process to ensure safety is included in specifications?

Other?

Discussion