



Safety Data and Risk Analysis Methods

Ewen Denney and **Ganesh Pai**

SGT / NASA Ames Research Center

{[ewen.denney](mailto:ewen.denney@nasa.gov), [ganesh.pai](mailto:ganesh.pai@nasa.gov)}@nasa.gov

UAS in the NAS Annual Meeting, NASA Ames

Terminology



- Hazards
 - 3 notions
- Mishap
- Risk
- Safety
- Incident
- Accident

Categorization of Methods



- A Priori Methods
 - Techniques applied prior to system operation
 - During system conception and development
- A Posteriori methods
 - Analysis of incidents / accidents
 - Applied after system is fielded / in operation
 - Single events rather than a history

A priori Methods



- PHA
- SHA & SSHA
- FHA
- HAZOP
- FMEA
- FTA
- ETA
- STPA & STAMP
- OHA

Accident Causation Models



- James Reason – “Swiss Cheese” model
 - Chain of events

- STAMP
 - System theoretic accident model and process
 - Inadequate control actions
 - Constraints on system operation and design
 - Unsafe interactions between humans, machines and environment

A Posteriori methods



- Root Cause Analysis
 - Work on the chain of events model
 - Events and Causal Factors Analysis
 - Multi-linear Events Sequencing
 - Sequentially Timed Events Plotting
 - Why-Because Analysis
 - AcciMaps

- STAMP
 - Uses the STAMP model

Application to Swift UAS



- Describe how Hazard analysis techniques were applied to Swift UAS
 - Use Infotech slides

Challenges



- What are the relevant methods
- Which methods are applicable in what situation
- What methods must be recommended for UAS context
- Can we combine techniques?