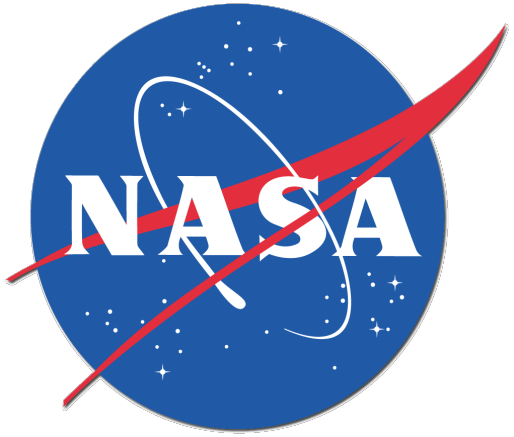
Scoping, tailoring, and abstraction refinement in the hazard assessment process



Dr. Mallory Graydon
Dr. Natasha Neogi
Frank McCormick

m.s.graydon@nasa.gov she | her | hers
NASA Langley Research Center, Hampton, Virginia, USA

Hazard assessment is a rote activity?

- Aircraft development usually begins with hazard assessment
- The usual analyses are defined by, e.g., SAE ARP4761A
  - Aircraft Functional Hazard Assessment (AFHA)
  - Preliminary Aircraft Safety Assessment (PASA)
    - Includes Fault Tree Analysis (FTA)
    - Common cause analysis
      - Zonal hazard analysis (ZHA)
      - Particular risks analyses (PRA)
      - Common mode analysis
    - Etc.
  - System-level FHA (SFHA) and PSA (PSSA)

Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment ARP4761A

ARP4761A and its EUROCAE counterpart, ED-135, present guidelines for performing safety assessments of civil aircraft, systems, and equipment. They may be used when addressing compliance with certification requirements (e.g., 14 CFR/CS Parts 23, 25, 27, and 29 and 14 CFR Parts 33, 35, CS-E, and CS-P). ARP4761A/ED-135 may also be used to assist a company in meeting its own internal safety assessment standards. While the safety assessment processes described are primarily associated with civil aircraft, systems, and equipment, these processes may be used in many other applications. The guidelines herein identify a systematic safety assessment process, but other processes may be equally effective.

Hazard assessment is ^~~not~~ a rote activity~~?~~

- Hazard analyses examine …
  - … a given *scope* of thing
  - … at a given *level of abstraction*
  - … using a given *search path* and *prompts* for what-if questions
  - … so to produce a desired set of *outputs*
- Some analyses bake in specific choices of scope etc.
  - ARP4761A's AFHA and SFHA tailor FHA to meet aviation needs
- *Others require the analyst to define these …*
- *What if you need to identify novel hazards of a novel aircraft?*

Proposed UAM vehicles and operations

- Proposed Urban Aerial Mobility (AAM) missions are inspiring novel technology
  - Battery electric propulsion
  - VTOL capability with wing-borne cruise for efficiency
  - Simplified vehicle operations (SVO) and unified controls
    - One inceptor, two modes
    - Reduced training needs
  - *M*-to-*n* operations
- UAM missions might involve:
  - Flight over dense urban areas
  - UAM traffic management
    - UAM traffic corridors

What is a hazard, anyway?

- There are competing definitions of “hazard”
  - Aviation uses ”hazard” haphazardly, but may mean *intrinsic hazard*: the capacity to cause harm (but perhaps not in this design)
    - High voltage is a hazard (although it might be well contained by design)
  - In systems safety, a *hazardous state* (hazard) is a system state that, under worst-case environmental conditions, will lead to a loss
    - A device with an exposed part carrying high voltage is in a hazardous state
- There is the related aviation concept of *failure conditions*
  - Not quite a hazardous state, but close …
- There is the unrelated aviation concept of “hazardous” severity

The safety engineering process

- Hazard assessment plays a central role in safety engineering
  - Hazardous states are states of the thing being designed that designers must do something about (e.g., eliminate or mitigate)
    - Safety processes during aircraft design, aircraft operation, air traffic control operations, and airspace-related rulemaking concern different "things" …
    - The "state" is a state of a thing over which you have *design authority* (i.e., whether a high-voltage part is exposed, but not where people put hands)
  - Hazardous states must be *identified* and their *severity* assessed
  - Hazardous states must be addressed in accordance with their severity
    - A hazardous state might be eliminated by design changes
    - *Safety requirements* might be defined to forestall entry into a state, or detect entry into the state, or facilitate exit from the state

The SAE ARP4754B/ARP4761A process

- AFHA/SFHA identify failure conditions of an aircraft/system
  - E.g., “unannunciated total loss of oxygenated air to crew or passengers … [during] cruise,” which would be catastrophic
  - These FCs and severities define safety objectives and drive the level of rigor of the remainder of the safety process
- PASA/PSSA look at how the components of a proposed architecture might lead to failure conditions through:
  - Classic failure analyses like fault tree analysis (FTA)
  - Common cause analyses e.g. common mode analysis (CMA), zonal safety analysis (ZSA) and particular risk analyses (PRAs)

The basic form of hazard analysis

- A hazard analysis is a guided human enumeration:
  - Decide on scope & make plan
  - Iterate over a thing, asking *what-if* questions
  - Identify potential losses and the thing's role in them
  - Identify & characterize hazards
  - Capture and communicate results

Public-domain image is from https://commons.wikimedia.org/wiki/File:Search_party_exercise_MPS.jpg

Functional hazard analysis (FHA)

- A hazard analysis is a guided human enumeration:
  - Decide on scope & make plan
  - Iterate over a thing, asking *what-if* questions
  - Identify potential losses and the thing's role in them
  - Identify & characterize hazards
  - Capture and communicate results

- Steps in an FHA:
  - Gather inputs, including a list of aircraft or system functions
  - Consider how each function could fail (in each flight phase)
  - Identify failure conditions
  - Determine effects on aircraft, crew, & other occupants
  - Assign severity classifications
  - Propose mitigations etc.

Hazard and operability studies (HazOp)

- A hazard analysis is a guided human enumeration:
  - Decide on scope & make plan
  - Iterate over a thing, asking *what-if* questions
  - Identify potential losses and the thing's role in them
  - Identify & characterize hazards
  - Capture and communicate results

- Steps in a HazOp:
  - Define scope & pick team
  - Gather design representation
    - Chemical plant schematic
    - Or various software diagrams …
  - Choose guide words
  - For each entity in design, ask and answer the questions formed by the guide words
  - Identify risks and recommend mitigations

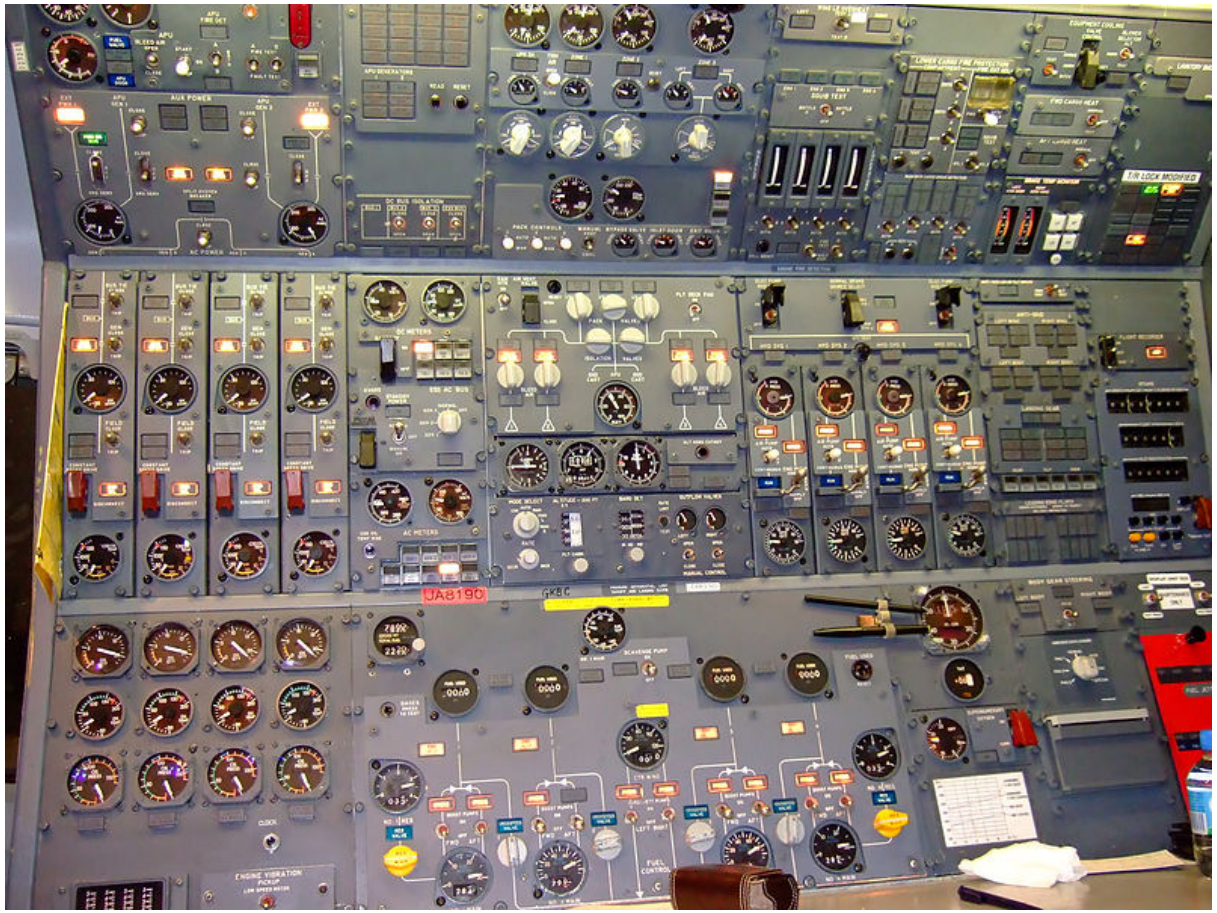
Systems-theoretic process analysis (STPA)

- A hazard analysis is a guided human enumeration:
  - Decide on scope & make plan
  - Iterate over a thing, asking *what-if* questions
  - Identify potential losses and the thing's role in them
  - Identify & characterize hazards
  - Capture and communicate results

- Steps in an STPA:
  - Define purpose & scope
  - Identify losses, hazards, and safety constraints
  - Construct a control structure
  - For each control flow, identify unsafe control actions due to:
    - Providing/not providing control
    - Early/late control
    - Incorrect control duration
  - Describe causal scenarios

Scoping and tailoring hazard analysis

- Analyses can be tailored to a purpose by varying:
  - The *scope* of analysis
  - The *level of abstraction*
  - The *search path and prompts*
  - The *outputs*, including:
    - *Scenarios leading to loss*
    - *Hazardous states*
    - *Degree of contribution to harm*
    - *Assumptions*
    - *Certification documentation*



Public domain image from https://commons.wikimedia.org/wiki/File:B747-200SF_FE_Panel.JPG

Scope

- What thing will be analyzed?
  - An airspace concept?
  - An aircraft conops?
  - An aircraft?
  - An aircraft system?
  - A fleet of aircraft?
- What losses are interesting?
  - Loss of hull?
  - Environmental impact?
  - Loss of confidentiality?
- STPA scope is up to analyst
  - Often starts just above craft
- FHA isn't just AFHA/SFHA
  - FHA has been conducted on aircraft ConOps
  - FHA to explore unique features of an aircraft concept
- Are you examining the things that need to be examined at the right lifecycle stage?

Level of abstraction

- Need to analyze at several levels of abstraction
  - Early analysis is most effective at shaping design
  - Need to examine details not available until late in design
- STPA is tailored by analysts
- ARP4761A's analyses are tailored for lifecycle phases
  - AFHA, SFHA, PASA, PSSA …
- FHA can be done at higher or lower levels of abstraction
  - FHA has been used to analyze a UAS ConOps
- Need to cover the levels where insight is needed
  - If aircraft missions and operating context are novel, those need analysis
  - Insight from abstract views is necessarily limited!

Search paths

- Analysts iterate over certain views of the system
  - FHA iterates over functions during phases of flight
  - HAZOP iterates over a design representation
  - STPA iterates over flows in a control diagram
- Derived from system details but should suit the analysis

- HAZOP analysts might use:
  - A chemical plant schematic
  - A software data flow diagram
- Need to iterate over the right things with the right step size:
  - Different kinds of problems are most obvious in different views
  - Small enough that analysts don’t overlook key insights
  - Big enough for tractability

Prompts

- Analysts use specific prompts to generate what-if questions
  - FHA: failure of function, malfunction
  - HAZOP: properties (e.g., ‘temperature’) and guide words (e.g., ‘high’)
  - STPA: providing, not providing, early/late, incorrect duration
- These can be tailored
  - HAZOP tailored for software
  - STPA tailored for security
- Open-ended ‘what would <*x*> mean for this’ is useful
  - Is there a novel failure mode?
- Knowledge/lists of kinds of failures/deviations/actions are also useful

Outputs

- We want many things from a complete set of analyses:
  - ***Insight*** **into how the thing might lead to harm**
  - A set of *hazardous states*
  - *Severity* of hazardous states
  - *Assumptions* to be checked
  - *Documents required for certification* (e.g., tables of failure conditions)
- Might have to mix & match analyses to provide outputs
- Still working out how to use STPA in commercial aircraft
  - STPA hazards don't neatly align to failure conditions
  - STPA doesn't identify severity
  - Do we present STPA results separately? Add them to our table of failure conditions?

Look where you need to look to find what you need to find

- Hazard analysis is a guided human enumeration
- It can be tailored, e.g.:
  - Scope
  - Level of abstraction
  - Search path and prompts
  - Outputs
- It should be tailored to find what needs to be found

- For traditional aircraft, there is traditional tailoring
- Novel aircraft might need special attention
  - Unique missions
  - New air traffic control schemes
  - Vertical & wing-borne flight
  - Battery electric power
  - Unified flight controls
  - …

Conclusion

- Hazard analyses need to be appropriately scoped & tailored
- Analysts need to think about:
  - What kinds of hazards & contributions to them might exist
  - What aspects of a thing need extra scrutiny
  - What kinds of analyses might best reveal that
  - The capabilities of their teams
  - What outputs are needed
- This ain’t rocket surgery
- But it is, and should be, a careful thinking-through of things

Backup slides

Aviation's poor definition of "hazard"

- In ARP4761A, a "hazard is": "A condition resulting from failures, external events, errors, or a combination thereof where safety is potentially affected."

This definition derives from substantially similar definitions in, e.g., AC 23.1309-1E.

- This definition is flawed:
  - The condition of improving weather potentially affects safety … in a good way
  - The external event of Martians attacking with ray guns would threaten safety … but we don't worry about this in design
- Engineers should focus on states the thing they're designing shouldn't be in