Communicating Safely

Implications of Interpersonal Communication in System Safety Analyses

Presented to: ISSC 2014

By: Jay Naphas, AST-500

Date: August 7, 2014

Federal Aviation Administration

Pick A State

- **Think of a state**
- **Notice how free a decision this seems to be**
  - 50 to choose from
  - Nations count, too
  - Emotional states count, too
  - Software variable values count, too
- **Notice how you felt with each expansion**
  - Implies that you weren't really "free"
- **Correct answer: Colorado**

A Note on Free Will

- **“Free will” is the ability of a conscious entity to author its thoughts independent of all causal chains**
  - Decision space is unbounded, or “free”
  - Actual decisions follow directly from causal chains
  - Actual decisions are not “free” to be anything other than what extraordinarily complex causation dictates
- **Human errors happen for knowable reasons**
  - Punishment often precludes learning because people know their errors aren’t due to malice

Mr. Prosser's Plight

- **Hitchhiker's Guide to the Galaxy**
- **Mr. L. Prosser is a direct descendant of Ghengis Khan**
  - Predilection for little furry hats
  - Likes axes
  - In defeat, thinks of thundering hooves
  - Doesn't know why, makes him nervous
- **Factors beyond our control or awareness can alter our thoughts**
  - Makes our will still less free

Use Your Illusion

- **Free will is an illusion**
  - No combination of determinism and randomness gives us authorship of our thoughts independent of causation
  - Recognizing that fact allows us to address the root causes of mental errors
- **Future decisions are contingent on present actions**
  - Use that awareness to make present actions safer
  - When you know future decisions follow directly from present actions, you choose actions more carefully

Uses of “Contingent” Will

- **Explains patterns in societies**
  - Centers of learning
    - Alexandria, Baghdad, Venice, Oxford, Silicon Valley
  - Centers of religion
    - Athens, Jerusalem, Vatican City, Mecca, Salt Lake City
  - Centers of safety
    - Aviation industry
- **Allows us to predict changes in properties that emerge from social systems**
  - Communication governs emergent properties

Defining Safety

- **Safety is a system property that emerges from the correct derivation and distribution of information about a system**
  - System design is the construction of a mental model
  - Information distribution is a complex socio-technical system in itself
  - Communication is a necessarily broad term:
    - Talking
    - Documentation/illustration
    - Electronic/chemical data transmission
    - Empathy

The General Theory of System Safety

- **All unsafe system behaviors are the result of errors in mental models, whether latent or consciously accepted**
  - Reliability engineering is predicated on understanding the system
  - Risk acceptance is the decision to allow flaws in the final system on the basis of rarity or necessity
  - System safety is deficient to the extent that the mental model is incomplete, inconsistent, or not embodied in the system
  - Disproof: any unsafe action from another source

Implications of the Theory

- **Communication content constrains future decisions**
  - Can no longer think “I’d have known better” without explaining the source of the difference
- **Can now predict the information another person needs to make safe decisions**
  - Look for losses of information or awareness instead of errors in decision logic
  - Gives us a path to engineering empathy
- **System safety’s job is to start and guide safety-increasing conversations**

FMEA

When and where?

Warning signs?

Who's responsible?

Links to test results?

** S – Severity, L – Likelihood, R – Risk

No.	System	Hazard Description	Results	**Risk Before Mitigation Measures			Risk Elimination or Mitigation Measures	**Risk After Mitigation Measures			Verification Evidence
				S	L	R		S	L	R	
1A	Avionics & Guidance	Loss of vehicle's central processor/ navigation systems due to excessive environments or loss of data from one of the following components: GPS, gyro, accelerometer, altitude sensor, antenna, or telemetry system.	The consequence is possible death or serious injury to the public inside or outside the operating area.	I	C	4	- Abort procedures and training for the pilot and ground crew. - Incorporate a Fail-Safe Switch that allows the pilot to manually abort flight by cutting off the main engine. - A warning system will provide the pilot with audible and visual signals when safe operating ranges of safety-critical flight parameters are exceeded.	I	E	12	- The vehicle's central processor and navigation systems will be ground tested at expected (modeled) flight conditions. - The vehicle's central processor and navigation systems will be flight tested during our initial flight test program (prior to permitted tests). - See Appendix E for a description of our verification schedule. - A copy of our training program has been included with this application (Appendix C). - Description of abort rules are included in the following: "BlueSky Checklist and Flight Rules."

- **What does this form really ask us?**
- **What is this form hiding from the reader?**

Key Questions

- **Information density and clarity**
  - What does the form assume that I know?
  - How would I answer a detailed clarification question using this form?
    - Does it link directly to first sources?
  - How would I answer a detailed summary question using this form?
    - Are the major risks and total risk evident?
  - Who else uses this form, what do they know, and what do they need to learn for their tasks?

Key Questions

- **Discussions**
  - Be aware of your own limits
    - 7 ±2 bits of working memory
    - Crew rest for system designers and analysts
    - Plan discussions accordingly
  - Preserve discussions in usable forms
    - Archives of meeting minutes may never be read
    - “Decisions” summaries may be more useful
    - Record what was established as part of the mental model of the system and why
  - Bring awareness to the process of group thinking

Homework

- **Look at hazard reports and system safety process documents**
  - Use this new perspective to see what's being systematically hidden from readers
- **Build your awareness of the content of your communications**
  - Communicate more than your decisions
  - Communicate what others need to be able to make safe decisions
  - Consciously build and correct mental models with every email, phone call, and report

Summary

- **Communication quality drives safety**
  - When errors in design or requirements dominate risk, communication improvements are key mitigations
- **Safety depends inextricably on communication in all phases**
  - Design flaws are artifacts of communication errors
  - Operator errors are caused by communication errors
- **Good communication is no accident**
  - Make communication a conscious, deliberate process
  - Put “talking” on the safety-critical items list

Questions?

- **Contact: Jay Naphas**
  - Email: Jay.Naphas@faa.gov
  - Phone: +1-661-310-8821

- **Reviews, comments, and suggestions are most welcome**