Safety: Areas of concern

(More things to think about?)

David Schultz QinetiQ-NA

TVC SSS 19 February 2014

Terminology and Definitions

Jargon

- **Jargon:**
- Terms used to provide shorthand communication between members of a cohort group.
- **Purposes of Jargon:**
- a. Accuracy and precision between experts
- b. Brevity
- c. Clarity
- d. Concision
- e. Obfuscation - Used to exclude non-members of the in group.

Terms Continued

- Can we agree to NOT use the jargon of the field for obsfucation?
- OR
- Let's define some safety terms to avoid obsfuction!

Safe

- A condition of health and well being.
- A place where health and well being is not threatened
- Freedom from risk, threat of injury or damage
- A baby in mothers arms. (context and scenario matter).

Safety:

- Safety. Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. 882E 3.2.30

Safety Goals

- Limit accident risk and liability (ISSS)
- Protect against financial disaster by compliance with accepted standards (corporations).

System

A collection of elements that works together to accomplish a purpose / function

System. The organization of hardware, software, material, facilities, personnel, data and services needed to perform a designated function within a stated environment with specified results. Per 882E 3.2.41

System Safety

- System safety. The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life-cycle. per 882E 3.2.43

System Safety Engineering

An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated.

Per 882E 3.2.44

Hazard

- A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. per 882E 3.2.14

Risk

The product of probability and severity

Severity

- The magnitude of potential consequences of a mishap to include: death, injury, occupational illness, damage to or loss of equipment or property, damage to the environment, or monetary loss. Per 882E 3.2.36
- How bad is it?
- How bad it is!

Probability of Failure:

- An estimate of the probability that the unit will fail in any specified time period, (day, year, hour).
- The estimate can be generated by analytic projections based on historical estimates of component failure rates.
- The estimate can be based on actual field failures of the unit under consideration, or a similar unit, for new versions of a product.

Use of Probability And Statistics

- The process of performing Safety engineering is vitally linked to the development of reliable, meaningful probabilities of failure.

- If statistics are not appropriately formed and evaluated, poor management decisions follow.

Mitigation Defined

Action required to eliminate the hazard

or

when a hazard cannot be eliminated,

reduce the associated risk by lessening the severity of the resulting mishap,

or lowering the likelihood that a mishap will occur.

Mitigation Methods

use redundancy to reduce probability of hazard (loss or malfunction).

use procedure changes (i.e. work-arounds) to reduce severity or probability.

use other functions to reduce effect of mishap (occupant restraint {seat belt}, crushable seat base). (How is this different from redundancy? It doesn't prevent mishap)

Fault Independence:

- absence of common elements
- foundation model: parts of a castle wall stand on a common foundation. If foundation fails all above collapse. A separate building on separate foundation is independent.
- If “redundant” items are not fault independent, you don’t have redundancy

Redumbdancy

- Putting a whole bunch of the same thing on a platform in the vague hope that it may provide greater availability, reliability and safety.
- Having four of the same thing, where a single common item will render them all useless, is not redundant.

Redundancy

- Adding materiel support to provide acceptable alternatives in the event of a failure.
- ATC communications are safety critical, so the FAA specifies that aircraft carry at least two radios capable of maintaining contact. And that you have alternative power available, in the event of engine generator failure.
- e.g. compass

Systems Safety Engineering

Characteristics of Systems

- Structure: parts (or components) directly or indirectly related to each other;
- Behavior: processes transform inputs into outputs (material, energy or data);
- Interconnectivity: parts and processes are connected by structural and/or behavioral relationships.
- Structure and behavior may be decomposed via subsystems and sub-processes to elementary parts and process steps.

System Conceptualization

- Systems must be conceptualized (simplified) for analysis and assessment
- Tools available are:
  - Models
  - Colored boxes
  - Functions

Application of Systems Models

- “All models are wrong, some are useful” (George Box).
- "Remember that all models are wrong; the practical question is how wrong do they have to be to not be useful?"

Colored Box Theory

- **Black Box Theory**
  - Inputs/outputs are visible, internal works are not.

- **White Box Theory:**
  - Inputs, outputs & everything inside is known.
- Black Box is a good place to start
- Move on to White Box when you have explored Black Box inputs/outputs and their hazards

Function Defined

- **A function is determined in terms of its inputs and outputs (Black Box concept)**
- Functional safety analysis doesn't care how the function is performed, whether it has electronics, electrics, wires, chains, hydraulics or levers inside so long as it meets specifications

A function is a toaster

- Inputs > Function> Output

- Bread &)
- > Toaster > Toast
- Electricity)

Function vs Implementation

- Implementation is the How part of a function.
- Early jet engines used a mechanical 3D cam to adjust the fuel flow
- Modern jet engines use digital systems to adjust the fuel flow
- Both work
- Safety shouldn't care if the implementation is mechanical, hydraulic, electronic, or any other mechanism so long as it meets requirements. [Black Box]

Example System Safety Techniques/Methods

- Used to set safety requirements and residual risk
  - Functional Hazard Assessment (conceptual models of failure mechanisms, sets safety requirements)
  - SSHA determines hazards, mitigations and residual risk
  - Root Cause analysis (stops when blame is firmly fixed)
  - FMEA (determines effects of component failures: Hardware and Software)
- Drives safety triage

Medical Triage Concept

When resources are inadequate, medical providers sort patients by prognosis:

a. No hope of survival / success

b. Probable survival with immediate treatment and resource allocation

c. Probable survival without intervention

In Medical Triage, a and c get minimal treatment]

Medical Triage Cost Benefit Trade

- The cost benefit ratio is a valid trade study, even when human lives are figured into the equation.
- The cold blooded nature of the exercise is seen by some as repugnant, but, as is well known to hospital personnel, it must be done.

Safety Triage
(Heart of System Safety Engineering)

What are the Systems Safety Equivalent of the Triage categories?

a. Hazard severity is not currently acceptable, but mitigation would take up all program resources

b. Hazard severity is not currently acceptable but mitigation is within system safety resource budget

c. Hazard severity is currently acceptable, but could be lowered

In Safety Triage, a and c get minimal resources

Safety Engineering Process Examples

- FAA defines risk requirements, demands actual achieved risk, if below Requirement, you don't fly.
- DoD program determines system hazards, estimates risks, refines systems requirements, determines actual risks, then accepts residual risks.
- SAE defines acceptable system risk levels, system hazards, estimates risk, refines systems to reduce risk to acceptable level.

Mitigation By Mitigation

- A company contracts to provide a box to produce function “A” and determines that a hazard caused by a function “A” failure
- Design is changed to reduce the severity of the hazard and/or reduce the probability of the hazard

Mitigation By Hand Waving

- A company contracts to provide a box to produce function “A” and determine that a hazard caused by a function “A” failure
- So, they go to the customer, and say, look, the function “A” box has a hazard but it will take resources to mitigate. So let’s just use the box to hold up a placard that tells the pilot to perform workaround “X, Y &Z” and we can complete our project on time and on budget.