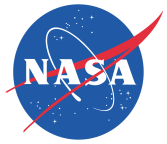


Goddard Space Flight Center

Balanced risk – hardware safety for robotic spacecraft

Dr. Jesse Leitner

Chief Safety and Mission Assurance Engineer

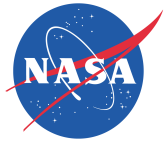
NASA GSFC

Agenda

- Hazard categories and risk
- Risk definitions at GSFC
- Risk handling
- Hazard analysis and credible risk
- Safety in the launch vehicle fairing
- Prompting change in NASA's requirements

Introduction

- The system safety function at NASA has considered all levels of protection
  - Personnel/range
  - Flight hardware
  - Facilities
- For a manned mission, there is little distinction
- For a robotic mission, the risk tolerance is substantially different for each situation
- Traditionally, hazards identified during system safety analyses have all been treated as safety risks
- This has led to an unbalanced approach at risk mitigation



Safety engrained in NASA

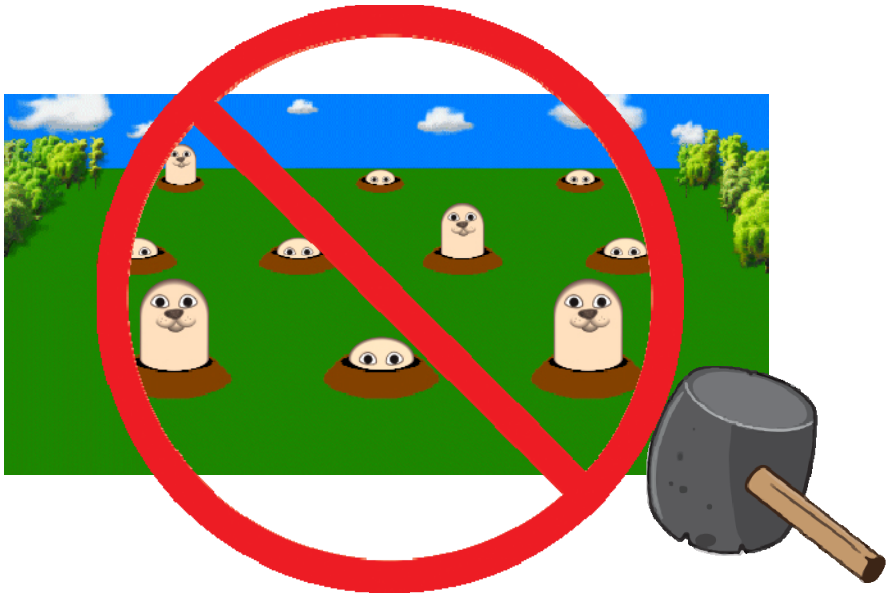
Goddard Space Flight Center

- Safety is an element of everything that NASA does
- So much so that even implementing practices to ensure safety may inadvertently cause safety risks
- There is a constant trade among safety, technical and programmatic risks
- Finding a balanced approach at managing risk in NASA can be a major challenge
  - Avoiding putting too much emphasis in one area and causing problems in others.

Balanced Risk (Whack-A-Mole)

Goddard Space Flight Center

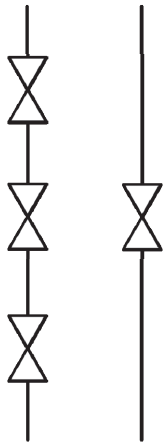
- A systems approach of looking across all options to ensure that mitigating or eliminating a particular risk does not cause much greater risk somewhere in the system



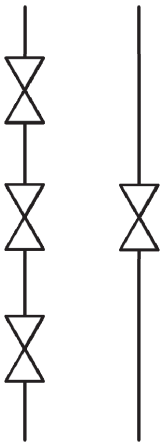
Unbalanced Risk Example

- General safety requirements dictate that anything considered "safety" requires 3 inhibits.
- Unfortunately, many elements prior to launch vehicle separation that are tied solely to mission success are put under the safety umbrella.
- This means that by default, many items such as premature deployment of solar arrays or other appendages are considered a safety issue for the on-orbit portion, even if they have no range safety effect, and they prompt a decision that it is always better to have more inhibits even if such a design prompts an even greater risk of mission failure due to one of the inhibits not releasing.
- Ultimately, under the guise of “safety” we may end up with a less reliable system that is not more safe if we are not diligent with system-level thinking

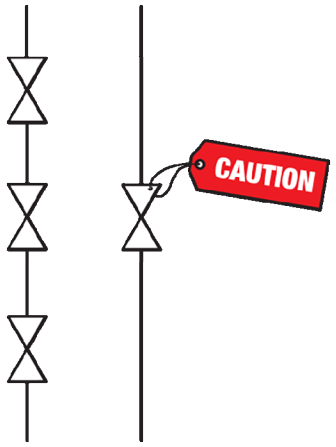
Which is Safer?



Which is More Reliable?



Which is Safer and More Reliable?



Hazard categorization

- Hazard analysis will lead to identification of threats to personnel, facilities, and the hardware itself
- Threats to personnel, the public, facilities, “collateral damage” must be handled at the lowest possible risk tolerance
- Threats to mission hardware may be programmatic or technical
  - Prior to launch, threats are programmatic
    - Because they can be mitigated, with the threat being cost/schedule impact
  - A post-launch threat is technical
    - Because it may not be mitigated by modifying or replacing hardware, and impacts mission success (only option is for operational/software mitigation)

Risks associated with hazards

- Given a particular configuration, an event may occur, resulting in injury to a person or the public (safety risk)
- Given a particular configuration, an event may occur, resulting in severe damage to hardware prior to launch (programmatic risk)
- Given a particular configuration, an event may occur, resulting in damage during launch or on-orbit (technical risk)

Risk levels per GPR 7120.4D

Likelihood	Safety Estimated likelihood of Safety event occurrence	Technical Estimated likelihood of not meeting performance requirements	Cost Schedule Estimated likelihood of not meeting cost or schedule commitment
5 Very High	$(P_{SE} > 10^{-1})$	$(P_T > 50\%)$	$(P_{CS} > 75\%)$
4 High	$(10^{-2} < P_{SE} \leq 10^{-1})$	$(25\% < P_T \leq 50\%)$	$(50\% < P_{CS} \leq 75\%)$
3 Moderate	$(10^{-3} < P_{SE} \leq 10^{-2})$	$(15\% < P_T \leq 25\%)$	$(25\% < P_{CS} \leq 50\%)$
2 Low	$(10^{-5} < P_{SE} \leq 10^{-3})$	$(2\% < P_T \leq 15\%)$	$(10\% < P_{CS} \leq 25\%)$
1 Very Low	$(10^{-6} < P_{SE} \leq 10^{-5})$	$(0.1\% < P_T \leq 2\%)$	$(2\% < P_{CS} \leq 10\%)$

Risk Handling from Hazards

- In order to handle risks consistently, they must be treated consistently with the type of consequence
  - Balanced approach of risk across a project
    - Treating a mission success risk as safety results in some mission success risks treated with orders of magnitude less risk tolerance than others with the same ultimate consequence
  - Avoids overtreating a programmatic risk at the expense of an on-orbit technical risk
- The fact that a concern, threat, or risk arises from a hazard does not define it as a safety risk
- Systems safety engineers will regularly deal with programmatic, technical, and safety risks but safety requirements apply only to safety risks

Hazard Analyses

- Perform based on a review of the particular architecture and layout
- A developer must prove a configuration is safe or reliable (as applicable) when a hazard is identified based on the specific configuration
- Note that some hazards may be “possible” occurrences, but not credible occurrences.
  - The risk likelihood scale may be used if practical
  - Subjective determinations may be made to establish the risk as “off the scale” based on redundancy, ruggedness, stored energy, mass ratios, etc to establish a risk as noncredible.

GSFC's implementation of NASA safety requirements (NPR 8715.3, NPR 8715.7, NASA-STD-8719.24)

- Safety engineers will perform the hazard analysis based on the known configurations and will identify risks to hardware, personnel, and property
- Hazards will be aligned with associated risk type (safety, technical, programmatic)
  - Hazard reports will include language to identify risks as credible or noncredible
  - Credible risks will be dispositioned in accordance with the risk type
- Only safety risks will be used to specify requirements for inhibits.
- Programmatic and technical risks will be provided to the project for disposition in the risk board, or to the CSO or reliability for handling of concerns not yet formulated as risks.
- We are currently negotiating a requirements change to eliminate the default use of inhibits (single point failures) to mitigate mission success risks

Conclusions

- There is a long history of system safety hazard analyses covering safety and mission success concerns
  - This traces to human-rated missions
- The philosophy led to appropriate thoughts and culture for hardware safety
- There was a side effect of causing unbalanced risk by treating mission success risks at much lower tolerance than others