



Proposed Definitions for Safety Devices and Survival Devices Related to Human- Rated Spacecraft

3rd International Association for the Advancement of
Space Safety (IAASS) Conference, Rome, Italy
“Building a Safer Space Together”

Day 2 – Wednesday 22 Oct 2008

D. F. Kip Mikula, (562) 209-4748, d.f.mikula@boeing.com

Introduction

- **Issue:**

Survival devices are being defined as Safety devices

- **Result:**

Safety risk is inaccurately being characterized as enhanced, risk is being mis-assessed with unrealistic evaluation of crew/passenger safety

- **Note:**

Crewmembers may survive a mishap through the use of a survival device but be severely, if not permanently, injured in the process, therefore, they survived but were not safe

Basic Definitions

■ Hazard

“Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.”

■ Safety

“Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.”

■ Survival

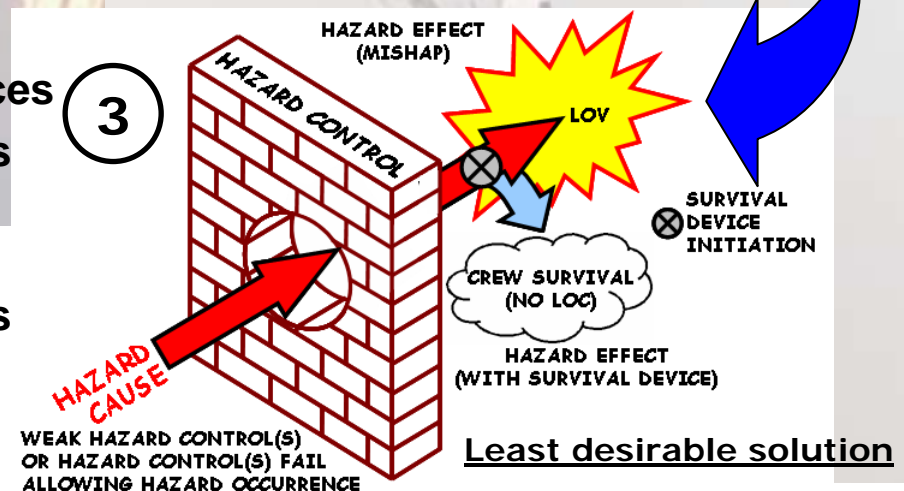
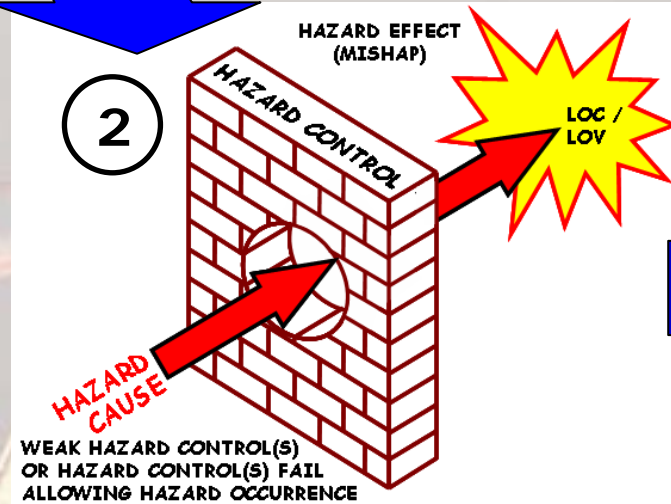
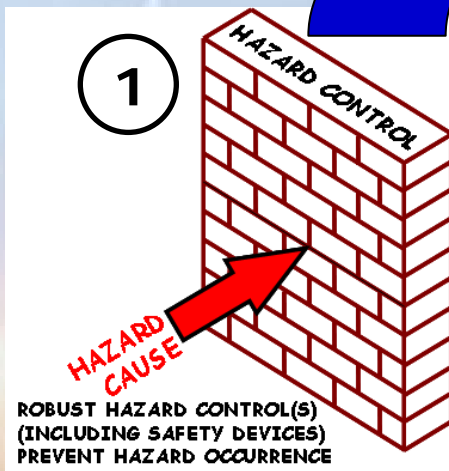
“A state of surviving; remaining alive.”

■ Prevention of hazards

Safety is enhanced by the prevention of hazard initiating events and not by surviving the resulting mishap

Prevention of Hazards

Preferred solution



- 1 Hazard cause is prevented by robust hazard controls including Safety devices
- 2 Weak hazard controls allow hazardous event (mishap with resulting Loss of Crew [LOC]/Loss of Vehicle [LOV])
- 3 Weak hazard controls allow hazardous event (mishap) with LOV (LOC is prevented by Survival Device)

Differentiation Examples

Device	Safety or Survival Device?	Rationale
Active/Dynamic Stability Control Systems	Safety	<u>Prevents</u> the rollover or loss of control of the vehicle during highly dynamic accident avoidance maneuvers.
Anti-Lock Braking Systems	Safety	<u>Prevents</u> the lock-up of aircraft or automotive wheel brakes during hard braking to avoid an accident.
Automotive Active Restraint System (i.e., Airbags)	Survival	Rapidly inflates to protect the driver and passengers only as the accident (mishap) is occurring. They do not prevent the accident.
Cable Tunnels	Safety	<u>Prevents</u> an individual from tripping over cables or wiring that are laid across a walkway.
Chaff and Flare Countermeasures	Safety	Used by military combat aircraft to distract and redirect surface-to-air or air-to-air missiles away from their intended target. Thus, it <u>prevents</u> the missile from striking that target.
Ejection Seat/Launch Abort System	Survival	Do not prevent any hazard initiating events such as fire, engine failures, or loss of structural integrity, are only used after the occurrence of the hazard initiating event, and is used for crew survival of the mishap.
Emergency Lighting	Survival	Provides lighting for dark areas such as stairwells only after the primary power has failed. These lights do not prevent the power failure from occurring.
Emergency Oxygen Systems	Survival	Provides breathing oxygen only after the primary source of oxygen has failed (such as during a commercial aircraft cabin depressurization). Such a system does not prevent the loss of the primary source of oxygen.
Fuel Tank Nitrogen Suppression System	Safety	<u>Prevents</u> the accumulation of hazardous levels of fuel vapors in combination with atmospheric oxygen thus removing one leg of the fire triangle and preventing fuel tank fires.

- **Question to Answer: Does the device prevent a hazard initiating event from occurring?**

Designing for Safety

HAZARD PREVENTION	Eliminate the Hazard
	Reduce the Likelihood of Occurrence of the Hazard
	Provide Safety Devices
	Provide Warning Devices
	Provide Special Procedures/Training
MISHAP SURVIVAL	Nothing Specifically Identified
<p>Preferred Hazard Reduction Sequence (Highest to Lowest) - For maximum safety risk reduction several iterations through the Hazard Reduction Sequence may be required.</p>	

Proposed Redefined Hazard Reduction Precedence Sequence

HAZARD PREVENTION	Eliminate the Hazard
	Reduce the Likelihood of Occurrence of the Hazard
	Provide Safety Devices
	Provide Warning Devices
	Provide Special Procedures/Training
MISHAP SURVIVAL	Incorporate/Provide Survival Devices
<p>Preferred Hazard Reduction Sequence (Highest to Lowest) - For maximum safety risk reduction several iterations through the Hazard Reduction Sequence may be required.</p>	

Current Hazard Reduction Precedence Sequence

Proposed Definitions

■ **Safety Devices:**

These are devices that are incorporated into the design of a human-rated spacecraft that prevent the occurrence of a hazard initiating event and, therefore, prevent a mishap from occurring. Examples of Safety Devices include such items as light grille guards that prevent accidental physical contact and switch guards.

■ **Survival Devices:**

These are devices that are incorporated into the design of a human-rated spacecraft that are used after a hazard has been initiated to separate the crew from the resulting hazard consequences. These devices are only used when hazard controls have failed to prevent the hazard initiating event and crew survival is critical. Examples of Survival Devices include such items as launch abort systems, ejection seats, fire suppression systems, and emergency oxygen systems.

Conclusions

- **There is a difference between Safety Devices and Survival Devices**
 - Confusing one for the other during a safety risk assessment may lead to the incorrect conclusion that the system is safer than it actually is
- **For human-rated space flight this could result in an over-reliance on Survival Devices**
 - Mistaken belief that they prevent catastrophic mishaps from occurring
- **Prevent confusion by (see slides 6 and 7):**
 - Clearly defining where each type of device fits into the Hazard Reduction Precedence Sequence
 - Provide definitions for Safety Devices and Survival Devices that clearly indicate the differences between the two types of devices

