SYSTEM SAFETY ENGINEERING AND MANAGEMENT

An Overview

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
SYSTEM SAFETY

Video

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
SYSTEM SAFETY
McDonnell-Douglas DC-10

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
SYSTEM SAFETY

DeHavilland Comet
SYSTEM SAFETY

DeHavilland Comet
SYSTEM SAFETY
DeHavilland Comet

FIG. 6. AERIAL VIEW OF COMET G-ALYU IN TESTING TANK.
SYSTEM SAFETY

History

1940s
- Trial and Error
- Fly-Fix-Fly
- Nuclear Weapons
- Jet Aircraft
- Aircraft Accidents

1950s
- Trial and Error
- Fly-Fix-Fly
- Jet Aircraft (HA Flight)
- Nuclear Power
- Aircraft Accidents

1960s
- Nuclear Weapons
- Jet Aircraft (NASA, DOD, 882)
- MIL-S-38130
- MIL-S-380130
- MIL-STD-882 (DOD)
- Space Systems
- Aircraft Accidents

1970s
- 1970s (MORT)
- MIL-STD-882A (DOD)
- NASA NHB 1700.1
- AEC Pub/Tn MORT
- MIL-STD-882B (DOD)
- Air/Spacecraft Accidents

1980s
- 1980s (Facility System Safety)
- NAVFAC SS Training
- OSHA Process Safety
- USACE SS Workshop
- MIL-STD-882C (DOD)
- Air/Spacecraft Accidents

1990s
- 1990s (Risk-Based Process System Safety)
- QA interface
- MIL-STD-882D / 882E (DOD)
- Human Factors

2000s
- 2000s (Facility System Safety)
- Software System Safety
- Air/Spacecraft Accidents

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
What is System Safety?

System Safety is defined as the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.
SYSTEM SAFETY

What do we do?

• **Influence design selection** through a structured hazard identification and risk mitigation process

• Promote safety **lessons learned**

How do we do it?

• Engaged in development programs **reporting to Chief System Engineer**
  - Co-located with design team
  - Closely aligned with Reliability Engineering

• Generic requirements defined in Standard Work

• Program specific deliverables defined in **System Safety Program Plan**

• Oversight and progress monitored thru:
  - Peer review of deliverable CDRL safety analyses
  - Customer / Regulatory Authority approval
  - Periodic System Safety Working Group meetings
When do we do it?

Throughout the entire program starting at the beginning!
SYSTEM SAFETY – USG PROGRAMS

Integrated with System Engineering (SE) Process

- Requirements Definition
- Detailed Design
- Component Build
- System Integration
- Test

Proposal / Specification Input

Risk Resolution / Hazard Tracking / System Safety Working Group Activities

MIL-STD-882E Process

Aircraft

- Concept of Operation
- Customer Validation
- Flight Test

System

- System Integration

Sub-System

- Preliminary Design
- Subsystem Testing
- Module / Component Test

Development

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
DOD SYSTEM SAFETY PROCESS
MIL-STD-882E System Safety Process

System Safety Tasks:
- Provide guidance for safe designs
- Identify potential safety hazards
- Conduct risk assessments
- Track safety hazards
- Verify risk elimination and/or mitigation

Element 1
Document the System Safety Approach
- Tasks Schedule
- Team Tools

Element 2
Identify and Document Hazards
- Life-Cycle Monitoring
- Maturing Design

Element 3
Assess and Document Risk
- Understand Hazards

Element 4
Identify and Document Risk Mitigation Measures

Element 5
Reduce Risk
- Understand Risk Reduction

Element 6
Verify, Validate, and Document Risk Reduction
- Understand Risk Acceptance

Element 7
Accept Risk and Document

Element 8
Manage Life-Cycle Risks
- Continuous
- Iterative

Team Tools
- Maturing Design

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
RISK MANAGEMENT PROCESS

- Identify Hazards
- Assess Hazards
- Develop Controls
- Implement Controls
- Monitor

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
IDENTIFY HAZARDS

- Accident and incident reporting databases
- Deficiency reporting databases
- Safety alerts and safety messages
- Hazard tracking databases for legacy and similar systems
- System/subsystem functions and analysis (hardware and software)
- System design documents (hardware and software)
“THOSE WHO DO NOT REMEMBER THE PAST ARE CONDEMNED TO REPEAT IT.”

George Santayana
US (Spanish-born)
Philosopher
1863-1952
# HAZARD ASSESSMENT

## Risk Assessment Matrix

<table>
<thead>
<tr>
<th>PROBABILITY</th>
<th>SEVERITY</th>
<th>Catastrophic (1)</th>
<th>Critical (2)</th>
<th>Marginal (3)</th>
<th>Negligible (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>High</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Probable</td>
<td>High</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td>Serious</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Eliminated</td>
<td>Eliminated</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.**
## SEVERITY CATEGORIES

<table>
<thead>
<tr>
<th>Description</th>
<th>Severity Category</th>
<th>Mishap Result Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>1</td>
<td>Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.</td>
</tr>
<tr>
<td>Critical</td>
<td>2</td>
<td>Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1 M but less than $10M.</td>
</tr>
<tr>
<td>Marginal</td>
<td>3</td>
<td>Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $1 00K but less than $1 M.</td>
</tr>
<tr>
<td>Negligible</td>
<td>4</td>
<td>Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $1 00K.</td>
</tr>
</tbody>
</table>
# HAZARD ASSESSMENT

Risk Assessment Matrix - Hazard Probabilities

<table>
<thead>
<tr>
<th>Description</th>
<th>Level</th>
<th>Specific Individual Item</th>
<th>Fleet or Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>A</td>
<td>Likely to occur often in the life of an item.</td>
<td>Continuously experienced.</td>
</tr>
<tr>
<td>Probable</td>
<td>B</td>
<td>Will occur several times in the life of an item.</td>
<td>Will occur frequently.</td>
</tr>
<tr>
<td>Occasional</td>
<td>C</td>
<td>Likely to occur sometime in the life of an item.</td>
<td>Will occur several times.</td>
</tr>
<tr>
<td>Remote</td>
<td>D</td>
<td>Unlikely, but possible to occur in the life of an item.</td>
<td>Unlikely, but can reasonably be expected to occur.</td>
</tr>
<tr>
<td>Improbable</td>
<td>E</td>
<td>So unlikely, it can be assumed occurrence may not be experienced in the life of an item.</td>
<td>Unlikely to occur, but possible.</td>
</tr>
<tr>
<td>Eliminated</td>
<td>F</td>
<td>Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.</td>
<td>Incapable of occurrence. (This level is used when potential hazards are identified and later eliminated.)</td>
</tr>
</tbody>
</table>
## HAZARD ASSESSMENT

### Risk Assessment Matrix

<table>
<thead>
<tr>
<th></th>
<th>Frequent (A)</th>
<th>Probable (B)</th>
<th>Occasional (C)</th>
<th>Remote (D)</th>
<th>Improbable (E)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Catastrophic</strong></td>
<td><strong>1</strong></td>
<td><strong>2</strong></td>
<td><strong>4</strong></td>
<td><strong>8</strong></td>
<td><strong>12</strong></td>
</tr>
<tr>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Critical</strong></td>
<td><strong>3</strong></td>
<td><strong>5</strong></td>
<td><strong>6</strong></td>
<td><strong>10</strong></td>
<td><strong>15</strong></td>
</tr>
<tr>
<td>(II)</td>
<td></td>
<td></td>
<td><strong>6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Marginal</strong></td>
<td><strong>7</strong></td>
<td><strong>9</strong></td>
<td><strong>11</strong></td>
<td><strong>14</strong></td>
<td><strong>17</strong></td>
</tr>
<tr>
<td>(III)</td>
<td></td>
<td></td>
<td><strong>11</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Negligible</strong></td>
<td><strong>13</strong></td>
<td><strong>16</strong></td>
<td><strong>18</strong></td>
<td><strong>19</strong></td>
<td><strong>20</strong></td>
</tr>
<tr>
<td>(IV)</td>
<td></td>
<td></td>
<td><strong>18</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Catastrophic: Could result in death, permanent total disability, loss exceeding $10M, or irreversible severe environmental damage that violates the law</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Critical: Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $1M but less than $10M, or reversible environmental damage causing a violation of law or regulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Marginal: Could result in injury or occupational illness resulting in one or more lost work days, loss exceeding $500K but less than $1M, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Negligible: Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $500K, or minimal environmental damage not violating law or regulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>Probability (Occurrences per 100K Flight Hours)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Frequent</td>
<td>( p &gt; 100 )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Probable</td>
<td>( 100 \geq p &gt; 10 )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Occasional</td>
<td>( 10 \geq p &gt; 1 )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>Remote</td>
<td>( 1 \geq p &gt; 0.1 )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Improbable</td>
<td>( 0.1 \geq p \geq 0.01 )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DEVELOP CONTROLS
System Safety Hazard Order of Precedence

• Eliminate hazard through design selection
  – select design or material that removes hazard

• Reduce risk through design alteration
  – consider a design change that reduces mishap severity or probability

• Incorporate engineered features or devices
  – reduce severity or probability using engineered features or devices

• Provide warning devices
  – install devices that alert personnel to hazard

• Incorporate signage, procedures training, PPE
  – use this control when all others are not feasible
# DEVELOP CONTROLS

System Safety Hazard Order of Precedence

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Eliminate hazards through design selection</td>
</tr>
<tr>
<td>2.</td>
<td>Reduce risk through design alteration</td>
</tr>
<tr>
<td>3.</td>
<td>Incorporate engineered features or devices</td>
</tr>
<tr>
<td>4.</td>
<td>Provide warning devices</td>
</tr>
<tr>
<td>5.</td>
<td>Incorporate signage, procedures, training, and PPE</td>
</tr>
</tbody>
</table>

**Preferred Approach**

**Reliance on Humans**

High

Low
IMPLEMENT CONTROLS
System Safety Hazard Order of Precedence

• Eliminate hazard through design selection
  – Crash worthy fuel tank

• Reduce risk through design alteration
  – Energy absorbing landing gear

• Incorporate engineered features or devices
  – Engine overspeed protection; torque limiting

• Provide warning devices
  – Warning and caution lights

• Incorporate signage, procedures training, PPE
  – Placards; Operator and maintainer training; aircraft maintenance procedures
Design Selection / Design Alternatives/ Engineered Features and Devices

1) Balistically tolerant rotor and drive system
2) High mass components retained in 20/20/18g crash conditions
3) Anti-plow keel beams
4) Reduced rollover potential with CEFS installed
5) Energy absorbing landing gear (30 fps limits)
6) Crashworthy fuel cells (65 feet drop)
7) Jettisonable cockpit doors and pop-out windows
8) Wire strike protection
IMPLEMENT CONTROLS

System Safety Hazard Order of Precedence

Warning Devices
IMPLEMENT CONTROLS

System Safety Hazard Order of Precedence

Special Procedures and Training
Reporting systems, processes, and procedures are established for reporting failures (RFA, JDRS)
System Safety Design Influence
(Rescue Hoist D-Ring Reversal)

Superseded MS 18107 hook

Spring-loaded guard

Positive locking feature

New design with cable D-Lok

System Safety Design Influence

### Safety Hazard Assessment: Rescue Hoist D-Ring

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Hazardous Effects</th>
<th>Causal Factors</th>
<th>IS</th>
<th>IP</th>
<th>IRC</th>
<th>Risk Mitigation</th>
<th>FS</th>
<th>FP</th>
<th>FRC</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harness D-ring disengages from rescue hoist hook</td>
<td>Injury or death of hoist passenger(s); destruction of hoist cargo; potential for injury/damage to ground personnel and equipment</td>
<td>Twisting or oscillation of the hook/D-ring connection when cable is unloaded can result in the D-ring riding up, over the top of the spring loaded guard.</td>
<td>I</td>
<td>E</td>
<td>Low</td>
<td>Rescue hoist hook guard redesigned to provide positive locking feature.</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>Closed. Hazard eliminated thru redesign of hook guard to preclude potential for D-ring reversal.</td>
</tr>
</tbody>
</table>

**IS = Initial Risk Severity Classification**
**IP = Initial Risk Probability Classification**
**IRC = Initial Risk Category**
**FS = Final Risk Severity Classification**
**FP = Final Risk Probability Classification**
**FRC = Final Risk Category**

### Risk Mitigation Measure: 1

1. Design Selection

### Probability

<table>
<thead>
<tr>
<th>PROBABILITY</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Remote      |   |   |   |   | |< 0.1%
| Improbable  |   |   |   |   |   |
System Safety Design Influence (Landing Gear Wheel Servicing)

Sikorsky continues to maintain its keen focus on safety enhancements and the prevention of injury to our customers, passengers, maintainers, and employees. During our review of the root cause of injuries across the entire aviation industry, injury to maintainers due to unintentional over-pressurization of landing gear wheels was identified as an improvement opportunity. We are now pleased to announce an Improvement to the S-92 to help prevent such injury in the future.

Industry statistics show that maintenance personnel are periodically injured by the improper and unauthorized use of high pressure or unregulated pressure sources, such as nitrogen bottles, to service tires. The consequence is often a burst of the wheel or tire resulting in debris that hits the worker. Despite the prohibitions and warnings in the technical manuals, instances of this type of injury persist – with even one preventable injury being too many. To address this, Sikorsky began work with its manufacturing partners and suppliers to implement a device on the wheel that will prevent over-pressurization. The new device is a screw-in replacement of the original tire servicing valve for each of the 6 wheels on the S-92. This part will become standard on the S-92 beginning at the end of April 2007. Customers who have taken delivery of aircraft

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Hazardous Effects</th>
<th>Causal Factors</th>
<th>IS</th>
<th>IP</th>
<th>IRC</th>
<th>Risk Mitigation</th>
<th>FS</th>
<th>FP</th>
<th>FRC</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Landing gear wheel burst</td>
<td>Severe injury and/or death of aircraft maintainer</td>
<td>Failure to properly set nitrogen bottle regulator pressure prior to servicing landing gear wheels.</td>
<td>I</td>
<td>D</td>
<td>Med.</td>
<td>Incorporated an integral pressure relief valve into the landing gear wheel nitrogen servicing valve.</td>
<td>I</td>
<td>E</td>
<td>Low</td>
<td>Closed. The S-92A program implemented the mitigation measure and verified its effectiveness thru testing. Sikorsky Management and the civil certifying agencies accepted the FRC.</td>
</tr>
</tbody>
</table>

IS = Initial Risk Severity Classification  
IP = Initial Risk Probability Classification  
IRC = Initial Risk Category  
FS = Final Risk Severity Classification  
FP = Final Risk Probability Classification  
FRC = Final Risk Category
SYSTEM SAFETY

Keys to Successful System Safety Engineering

• Ensure System Safety Engineer in engaged early in the program or project

• Ensure System Safety Engineer is adequately resourced

Benefits of System Safety Engineering

• Reduced Project Cost

• On Time Project Schedule

• Delivery of Safe System
Summary

The system safety processes executed throughout the life cycle of a project will save the project cost and time. But more importantly conducting system safety processes prevent accidents saving lives and money associated with the insured and uninsured costs of an accident.
SYSTEM SAFETY

Video

THIS DOCUMENT CONTAINS NO INFORMATION SUBJECT TO ITAR OR EAR.
SYSTEM SAFETY

What are your questions?
Thank You For Your Time And Attention!

We pioneer flight solutions that bring people home from everywhere...every time!