Managing Safety as a Design Imperative

International System Safety Society
Canadian Chapter

by

Tony Zenga Bsc. Eng

www.cmtigroup.com  https://uni-tworld.com/
tzenga@cmtigroup.com

Disclaimer - The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of the ISSS or CMTIGroup Inc. clients.
Agenda

Accidents / Incidents (basis for Lessons Learned - Aero, Rail, Auto, other)

Safety Definition

Interrelated Safety Disciplines

System Safety Engineering Challenges

System Safety is Everyone’s business

The System Safety Process - How it is done

System Safety Program Plan (SSPP)

Life cycle program Phase Hazard Analysis and V&V

Safety Stakeholders

System-of-System view

Hazard Analysis Example and Hazard Log output

Conclusion and Questions
<table>
<thead>
<tr>
<th>Company</th>
<th>Aircraft</th>
<th>Features</th>
<th>Safety Concerns</th>
<th>Status</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Unit cost US$20M (1972) ($120M today)</td>
<td>- Design flaw in the cargo doors.</td>
<td>Airline industry consensus DC-10 had a poor reputation both for fuel economy and for its</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Its safety reputation was further damaged by the crash of American Airlines</td>
<td>overall safety.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Flight 191,</td>
<td>1997 Merged with Boeing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- As of September 2015, DC-10 has been involved in 55 accidents / incidents,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 32 hull-loss accidents</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jets</td>
<td>- Glass Cockpit</td>
<td>• Failed communications and navigation electronics, random autopilot disengagement,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Landing gear indication problems,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• FADEC issues, indicated a loss of control of engine thrust could occur.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Accident / Incident (basis for lessons-learned) - Aero

<table>
<thead>
<tr>
<th>Operator</th>
<th>Aircraft</th>
<th>Accident</th>
<th>Contributory causes</th>
<th>Effect</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scandinavian Airlines Flight 751 (1991)</td>
<td>MD-81</td>
<td>- Ice off the wings caused damage to the engine fan stages, which led to engine surges. &lt;br&gt; - The surges destroyed both engines.</td>
<td>- The pilots were not trained to identify and eliminate engine surging. &lt;br&gt; - Automatic Thrust Restoration was unknown within SAS - was activated and increased the engine power without the pilot's knowledge.</td>
<td>No Fatalities</td>
<td><a href="https://en.wikipedia.org/wiki/Scandinavian_Airlines_Flight_751">https://en.wikipedia.org/wiki/Scandinavian_Airlines_Flight_751</a></td>
</tr>
</tbody>
</table>
## Accident / Incident (basis for lessons-learned) - Rail

<table>
<thead>
<tr>
<th>Operator</th>
<th>Type</th>
<th>Safety</th>
<th>Outcome</th>
<th>Source</th>
</tr>
</thead>
</table>
| Montreal, Maine and Atlantic Railway (MMA) (July 2013) | Class II Freight Railroad | - July 2013 Derailment due to a runaway train.  
- Four Cars exploded, causing destruction of business and properties with fatalities.  
- Environmental damage. | MMA Chapter 11/CCAA bankruptcy protection in August 2013  
MMA's certificate of fitness was revoked by Cdn transport Agency  
Total cost of the derailment likely to exceed $200M | [https://en.wikipedia.org/wiki/Montreal,_Maine_and_Atlantic_Railway](https://en.wikipedia.org/wiki/Montreal,_Maine_and_Atlantic_Railway) |
# Lessons-Learned – US Major Commuter Rail Accidents 2002 - 2018

<table>
<thead>
<tr>
<th>Year</th>
<th>Event Description</th>
<th>Location</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>Minot train derailment</td>
<td>Minot, North Dakota</td>
<td>1 Fatality</td>
</tr>
<tr>
<td>2005</td>
<td>Graniteville Train Crash</td>
<td>Graniteville, South Carolina</td>
<td>9 Fatalities, hundreds made ill.</td>
</tr>
<tr>
<td></td>
<td>Glendale train crash</td>
<td>Glendale, California</td>
<td>11 Fatalities, 177 Injured</td>
</tr>
<tr>
<td>2008</td>
<td>Chatsworth train collision</td>
<td>Chatsworth, California</td>
<td>25 Fatalities, 135 Injured</td>
</tr>
<tr>
<td>2015</td>
<td>Philadelphia train derailment</td>
<td>Philadelphia, Pennsylvania</td>
<td>8 Fatalities, Hundreds Injured</td>
</tr>
<tr>
<td>2016</td>
<td>Hoboken train crash</td>
<td>Hoboken, New Jersey</td>
<td>1 Fatality, 114 injured</td>
</tr>
<tr>
<td>2018</td>
<td>Cayce, South Carolina train collision</td>
<td>Cayce, South Carolina</td>
<td>2 Fatalities, 116 Injured</td>
</tr>
</tbody>
</table>
Accidents / Incidents (basis for lessons-learned – Auto and other Industries

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Safety</th>
<th>Outcome</th>
<th>Source</th>
</tr>
</thead>
</table>
| Takata Corp (founded in 1933) | Airbags - Defective inflators | - In 2013 series of fatalities and injuries initial recall 3.6 million cars.  

- 18 Jan 2019 Tesla recalls over 14,000 Model S vehicles exported to China due to Takata airbag issue.  


| Johnson & Johnson (founded in 1886) | Talc products | • Blamed for ovarian cancer caused by asbestos in their baby powder and other talc products. | - J&J loses its motion to reverse a jury verdict that awarded $4.69 billion.  
Definitions: Industry specific meaning with common goal “acceptable level of risk”

The condition of being protected from or unlikely to cause danger, risk, or injury.

Freedom from unacceptable risk of harm.

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

[1] In a risk-informed context, safety is an overall condition that provides sufficient assurance that mishaps will not result ….

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

Acceptable Risk. Risk that the appropriate acceptance authority is willing to accept without additional mitigation.

© CMTIGroup Inc. (February 2019)
**Safety Management System (SMS)**

1 Comprehensive management system designed to manage safety elements in the workplace. It includes **policy**, **objectives**, **plans**, **procedures**, **organisation**, **responsibilities** and other measures.

**System Safety Engineering (SSE)**

2 The application of **engineering and management principles**, criteria and techniques to optimize safety. The goal of System Safety is to **optimize safety** by the identification of safety related risks, **eliminating or controlling them by design and/or procedures**, based on acceptable system safety precedence.

**Occupational Health & Safety**

Occupational safety and health (OSH), also commonly referred to as occupational health and safety (OHS), occupational health, or workplace health and safety (WHS), is a **multidisciplinary field concerned with the safety, health, and welfare of people at work**.

**Others...**

Chemical Safety, Facilities Safety, Transportation Safety, Fire Smoke & Toxicity etc...

Sources: 1 Wikipedia, 2 Google search
System Safety is Everyone’s business

**Challenge**

- Very little time from contract award to system deployment - (Cut and paste from previous programs).
- Silo mindset that occurs in organisations, which resists sharing information with peers or external stakeholders.
- Spending valuable time on insignificant risks

**Opportunity**

- Repeatable SSE processes to be in place prior to contract award – Attention to be given to New or Removed Functions and Not all conditions are the same.
- Create a unified Safety vision of team collaboration between Customer, integrator and subsystem suppliers. (E.g., Lessons Learned Scandinavian Airlines Flight 751).
- Evaluate risks early in the program phase, Prioritize mitigation and Close High risk hazards.

© CMTIGroup Inc. (February 2019)
A strong Systems Engineering culture facilitates System Safety / Specialty Engineering design.

Disconnect between Systems Engineering, Systems Safety and other Specialty engineering (Human Factors, RAM, Security, QA, EMI/EMC) disciplines.

Safety Documentation traceability lapse from beginning to end of the project (e.g., multiple spreadsheets, e-mails, lack of authority approval traceability, etc).

Begin early in the program lifecycle to build the program System Safety Engineering Folder – Hazard Tracking System. Could be the best defense for SSE due diligence.
The System Safety Process - How it is done

- System Safety Program Plan
- Hazard Identification
- Assess and prioritize risks
- Hazard causal factors
- Risk Mitigation technical requirements
- Mitigation verification
- Residual Risk & Acceptance
- Mishaps & Hazard Closure
- Loss Events (Mishaps) & Hazard Identification

© CMTIGroup Inc. (February 2019)
System Safety Program Plan (SSPP)

Provides a formal basis of understanding between the prime contractor and the customer to ensure that consideration is given to safety during the program life cycle phases based on the Customer Specification.

SSPP as a minimum should contain:

1. **System Safety Organization details** - The system safety group within the overall organization (functional relationships, and lines of communication including responsibility and accountability of system safety personnel, other contractor organizational elements).

2. **System Definitions with Boundaries** – The system and its boundaries (responsibilities).


4. **Hazard Analysis** - System safety methodology, analysis technique and format used in qualitative and quantitative analysis to identify hazards, their causes and effects, and corrective action. The technique for establishing a single closed-loop hazard tracking system.

5. **Safety Verification** - The verification requirements for ensuring that safety is adequately demonstrated by analysis.

6. **System Safety Program Milestones** – Safety milestones to evaluate the effectiveness of the system safety effort can be made at Quarterly Program Reviews. A program schedule of safety tasks showing Deliverables.

**Who should have an SSPP?** Because each level of a system is responsible for safety and is involved in the hazard analysis and mitigation process. The SSPP is required from the customer, the prime contractor and the subsystem suppliers.
Life cycle program Phase Hazard Analysis and V&V

System / Software Safety is conducted throughout the program

ACRONYMS

- FHA: Functional Hazard Analysis
- O&SHA: Operating and Support Hazard Analysis
- PDR: Preliminary Design Review
- PHA: Preliminary Hazard Analysis
- PHL: Preliminary Hazard List
- SHA: System Hazard Analysis
- SRHA: System Requirements Hazard Analysis
- SRVM: System Requirement Verification Matrix
- SSHA: Subsystem Hazard Analysis
- SSPP: System Safety Program Plan

© CMTiGroup Inc. (February 2019)
SoS Consideration

1. Systems need to be adequately defined.

2. In the SoS environment if the train is defined as a System, a condition that causes it to stop less than a Safety defined distance (by braking curves) could be catastrophic.

3. If the System is the Train and the propulsion stops then the hazard may not be catastrophic.
SSHA Hazard analysis example & Hazard Log output

- **Top event**: Fall Mishap
- **Hazard**: Side door opens spontaneously while train in motion
- **SSHA**: Door system
- **Scenario**: Passenger door opens spontaneously, passenger falls while the train is in motion.

Example hazard analysis using a Hazard Tracking System:

Clip 1 FHA to SSHA Cause (5 minutes)
Clip 2 Mitigating the hazard Cause (3.5 minutes)
Clip 3 Systems Engineer review of Hazard Cause mitigation (4 minutes)
Clip 4 Hazard Cause Mitigation Verification results (3 minutes)
Clip 5 FHA, SSHA output for entry into Hazard log / Safety Case (4 minutes)

https://cmtidemo.uni-twworld.com/custompmp/homepage.php
Conclusion and Take away

- System Safety is everyone’s business (subsystem suppliers, system integrators, system operators and system users).

- SSE is an “art” and a “science” with well defined methodologies, processes and tools (increases collaboration and communication).

- The cost of an effective SSE program is an excellent investment that eliminates or reduces the likelihood of mishaps and prevents company reputational damage.
The world is not dangerous because of those who do harm, but because of those who look and do nothing.

Albert Einstein

Thank You for your attendance and participation