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

Accident / Incident (basis for lessons-learned) - Aero

Company	Aircraft	Features	Safety Concerns	Status	Source
McDonnell Douglas (1972 – 1979)	DC-10	- Three-engine wide body Jet airliner - Unit cost US$20M (1972) ($120M today)	- DC-10 was noted for a poor safety record in early operations, - Design flaw in the cargo doors. - Its safety reputation was further damaged by the crash of American Airlines Flight 191, - As of September 2015, DC-10 has been involved in 55 accidents / incidents, - 32 hull-loss accidents	FAA withdrew the DC-10's type certificate in 1979. Airline industry consensus DC-10 had a poor reputation both for fuel economy and for its overall safety. 1997 Merged with Boeing.	https://en.wikipedia.org/wiki/McDonnell_Douglas
Eclipse Aerospace EA500 (2002 – 2008)	New class of Very Light Jets	- Very advanced technology - Unit Cost $2.5M - powered by 2 lightweight turbofan engines - Glass Cockpit	• Smoke streaming from a cockpit display, • Pixilated flight display monitors, • Failed communications and navigation electronics, random autopilot disengagement, • Landing gear indication problems, • FADEC issues, indicated a loss of control of engine thrust could occur.	Production halted in October 2008 due to lack of funding. Company entered Chapter 11 bankruptcy on 25 November 2008. Program Cost $1.4B	https://www.wired.com/2008/08/faa-scrutinizes/ https://en.wikipedia.org/wiki/Eclipse_500

Accident / Incident (basis for lessons-learned) - Aero

Operator	Aircraft	Accident	Contributory causes	Effect	Source
Scandinavian Airlines Flight 751 (1991)	MD-81	- Ice off the wings caused damage to the engine fan stages, which led to engine surges. - The surges destroyed both engines.	- The pilots were not trained to identify and eliminate engine surging. - Automatic Thrust Restoration was unknown within SAS - was activated and increased the engine power without the pilot's knowledge.	No Fatalities	https://en.wikipedia.org/wiki/Scandinavian_Airlines_Flight_751

Accident / Incident (basis for lessons-learned) - Rail

Operator	Type	Safety	Outcome	Source
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

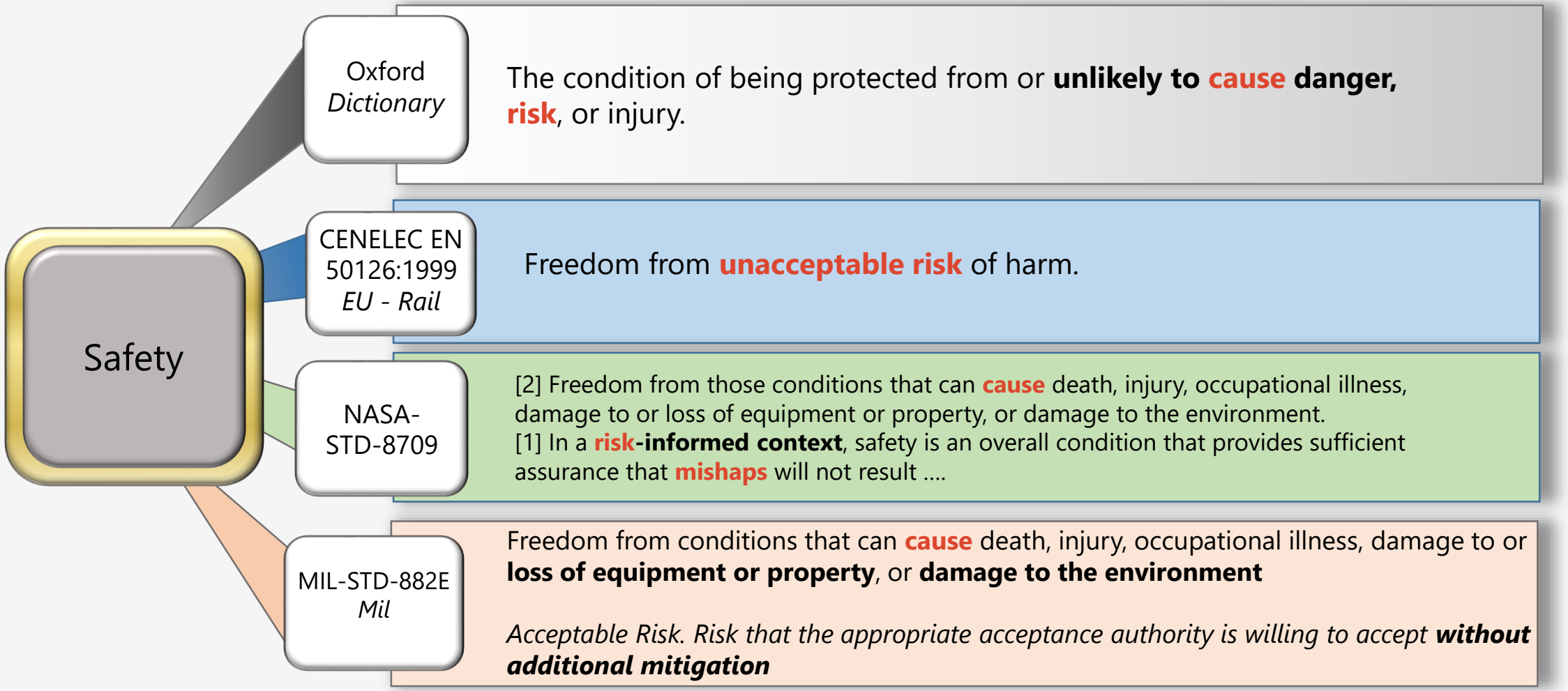
Lessons-Learned – US Major Commuter Rail Accidents 2002 - 2018

2002		
Minot train derailment	Minot, North Dakota	1 Fatality
2005		
Graniteville Train Crash	Graniteville, South Carolina	9 Fatalities, hundreds made ill.
Glendale train crash	Glendale, California	11 Fatalities, 177 Injured
2008		
Chatsworth train collision	Chatsworth, California	25 Fatalities, 135 Injured
2015		
Philadelphia train derailment	Philadelphia, Pennsylvania	8 Fatalities, Hundreds Injured
2016		
Hoboken train crash	Hoboken, New Jersey	1 Fatality, 114 injured
2018		
Cayce, South Carolina train collision	Cayce, South Carolina	2 Fatalities, 116 Injured

Accidents / Incidents (basis for lessons-learned – Auto and other Industries

Company	Product	Safety	Outcome	Source
Takata Corp (founded in 1933)	Airbags - Defective inflators	- In 2013 series of fatalities and injuries initial recall 3.6 million cars. - National Highway Traffic Safety Administration ordered nationwide recall of more than 42 million cars.	In June 2017, Takata filed for bankruptcy was acquired by Key Safety Systems. Takata estimates airbag recall costs at $24 Billion.	https://en.wikipedia.org/wiki/Takata_Corporation https://www.bloomberg.com/news/articles/2016-03-30/takata-said-to-put-worst-case-airbag-recall-costs-at-24-billion
		• 18 Jan 2019 Tesla recalls over 14,000 Model S vehicles exported to China due to Takata airbag issue.	-	https://electrek.co/2019/01/18/tesla-recalling-14000-model-s-china-takata-airbag-issue/
PG&E - Pacific Gas and Electric Company (founded in 1905)	Utility Equipment	• Investigators to determined whether PG&E equipment was at fault for sparking last year's Camp Fire, which killed 86 people.	Facing at least $30 billion in liabilities related to wildfires in 2017 and 2018.	https://uk.finance.yahoo.com/news/pg-e-secures-5-5-163000843.html?guccounter=1
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. - Reputational Damage.	https://www.nytimes.com/2018/12/19/business/johnson-johnson-baby-powder-verdict.html

Definitions: Industry specific meaning with common goal "acceptable level of risk"



Interrelated Safety Disciplines

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.
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.
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

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

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.

System Safety is Everyone's business (cont'd)

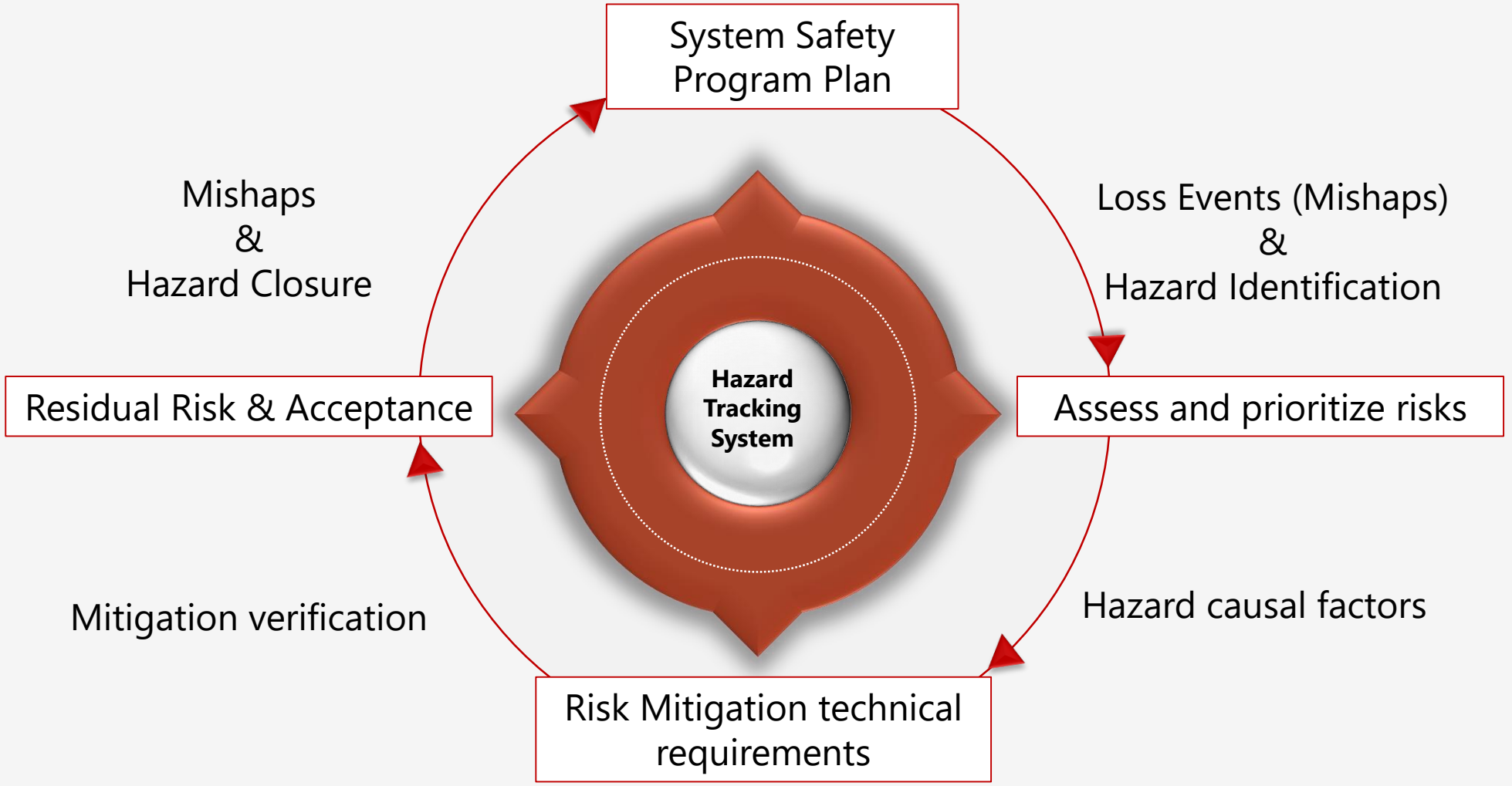
Disconnect between Systems Engineering, Systems Safety and other Specialty engineering (Human Factors, RAM, Security, QA, EMI/EMC) disciplines.

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

A strong Systems Engineering culture facilitates System Safety / Specialty Engineering design.

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



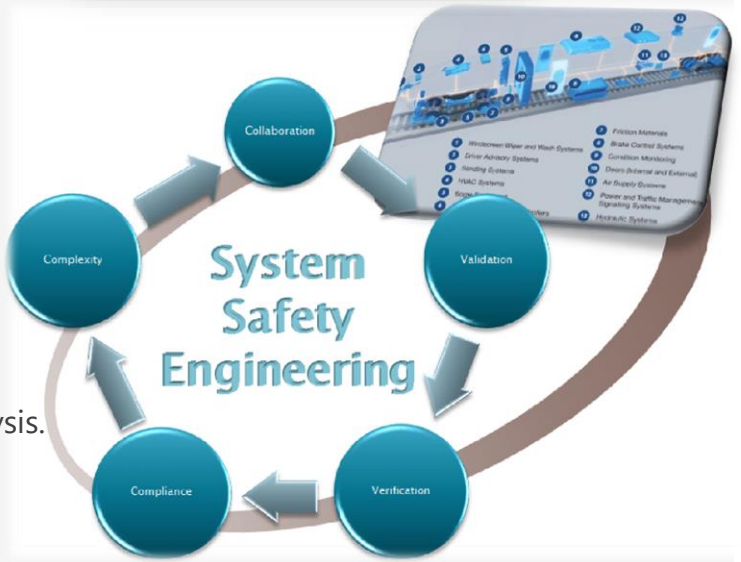
System Safety Program Plan (SSPP)

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:

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

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).
3. **System Safety Requirements** - Applicable safety standards and System specifications sources, Risk assessment procedures. Hazard severity categories, probability levels.
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 Delivrables



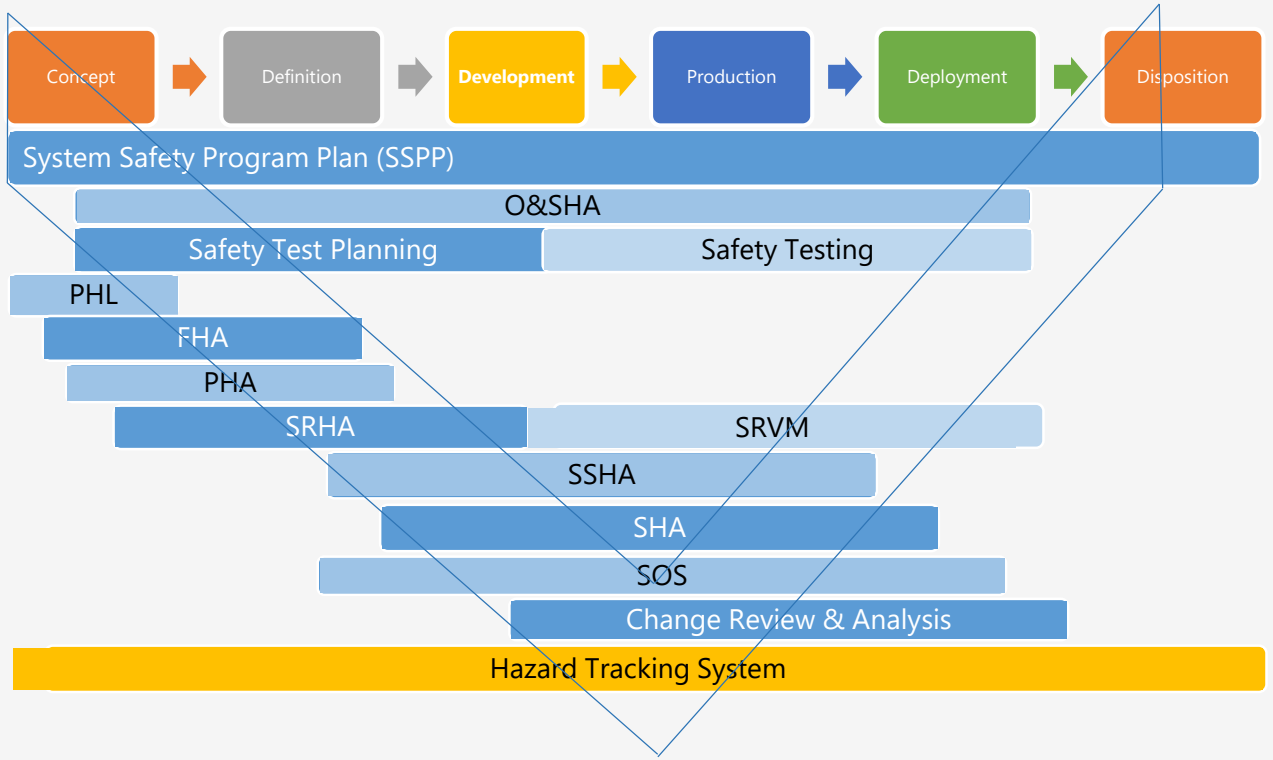
Who should have an SSPP ? Because each level of a system is responsible for safety and is involved in the hazard analysis and mitigation process. The SSPP is required from the customer, the prime contractor and the subsystem suppliers.

Life cycle program Phase Hazard Analysis and V&V

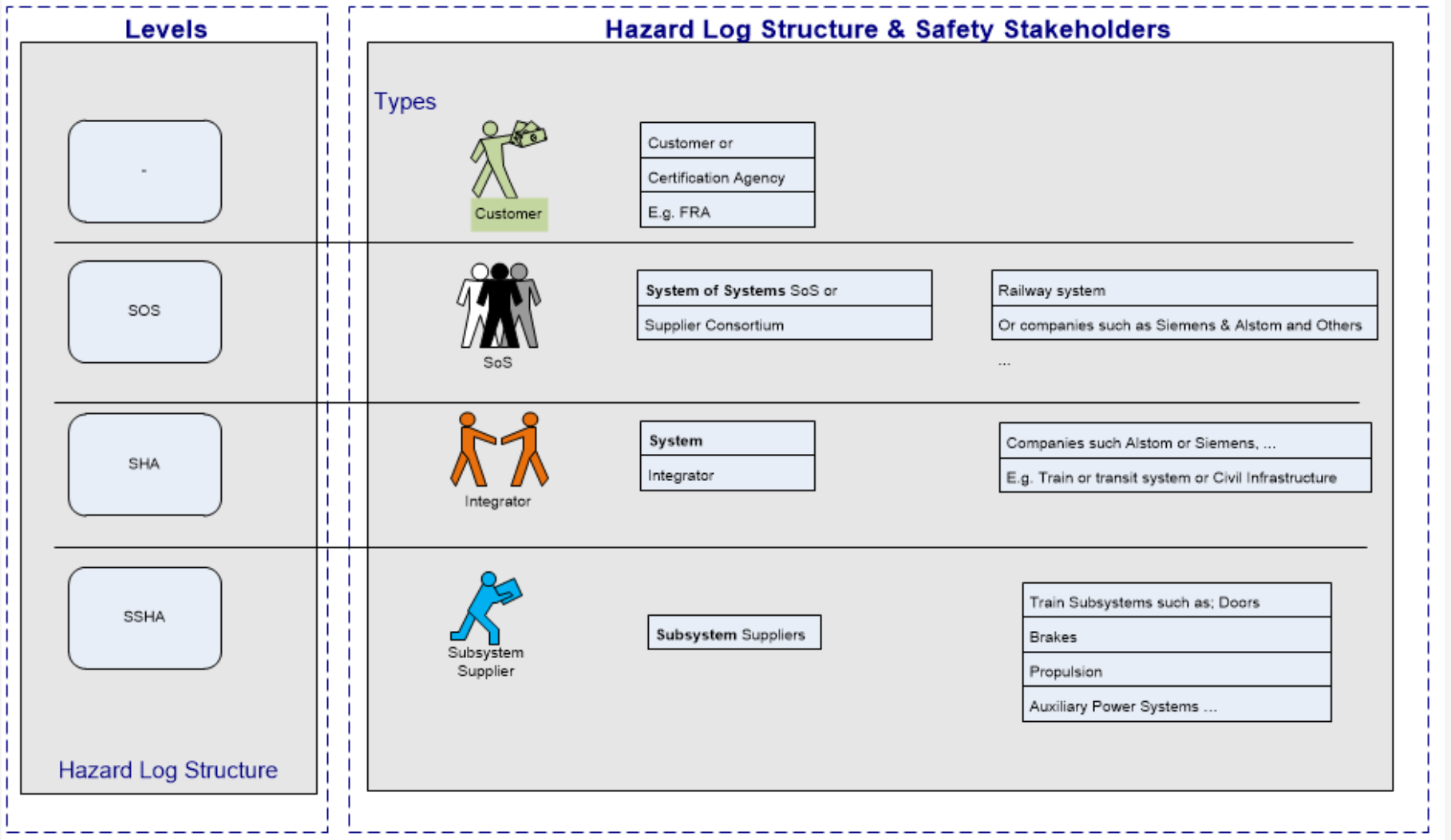
System / Software Safety is conducted throughout the program

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



Safety Stakeholders



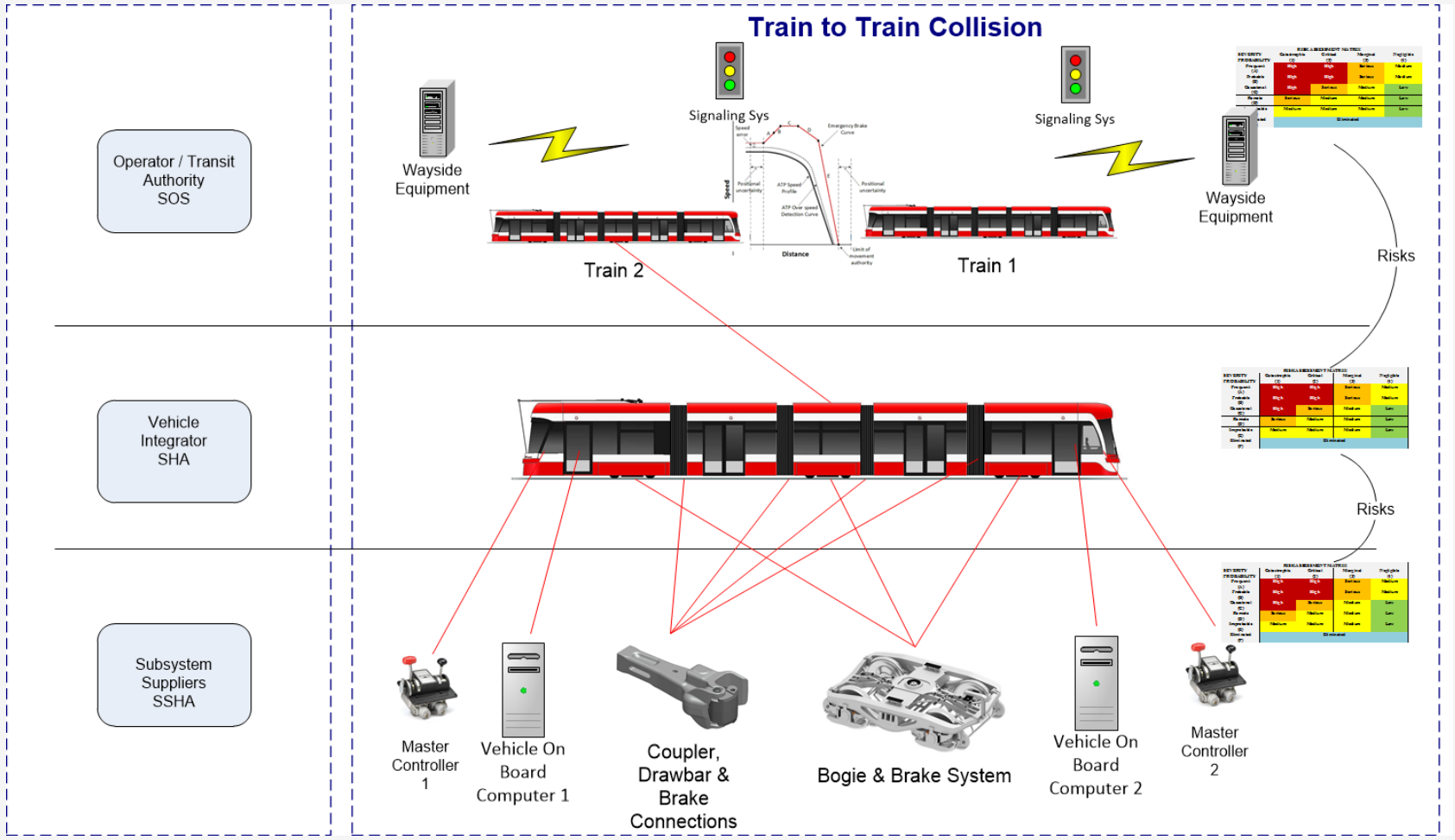
System-of-System view

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-tworld.com/custompmp/homepage.php

Conclusion and Take away

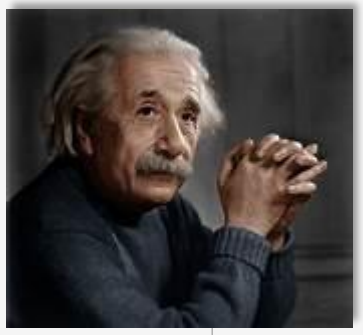
- System Safety is everyone's business (subsystem suppliers, system integrators, system operators and system users).

- 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.

Thought from Albert ….

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