System Safety Engineering and Operational Safety Management Systems Bringing two successful approaches together

International System Safety Society
Canada Chapter

by
Bob Dodd and Tony Zenga

bob.dodd@thealoftgroup.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, The Aloft Group or CMTIGroup Inc. clients.

SYSTEM SAFETY SOCIETY Organized 1962 Incorporated 1973
Professionals Dedicated to the Safety of Systems, Products & Services

Abstract

In technical high risk industries such as transportation, oil & gas, and chemical process industries, there have been two critical streams that have added immeasurably to safety of operations. One has been the development of sophisticated system safety engineering methods to deliver highly safe technology. The second has been the gradual implementation of safety management systems for operations, which continuously improve safety performance.

While these safety initiatives have been very successful, there are gaps between the two worlds. These gaps are emerging as potential threats to further improvements in safety, particularly with the continued progress towards greater automation and the associated growing tight interconnection of systems both technical and organisational.

The gaps encompass conceptual differences, data and analysis separation as well as organisational and regulatory barriers.

This presentation describes the basis and strengths of existing approaches to the separate disciplines, outlines the nature of the gaps and provides some examples and outlines potential paths towards better solutions.

Outline

1. System Safety Engineering (SSE)
2. Safety Management Systems (SMS)
3. The transition from Design to Operational context
4. The gaps between design safety and operational safety
5. Working toward solutions
6. Discussion

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 Engineering Maturity and Definition

Maturity

In September 1947 a technical paper titled "**Engineering for Safety**" was presented to the institute of aeronautical science.

"Safety must be designed and built into airplanes just as performance stability and structural integrity.

A safety group must be just as important as part of a manufacturer's organization, stress, aerodynamics or a weight group"

In early 1960 the concept was formally applied as a new approach to examine hazards associated with the Minute Man Intercontinental Ballistic Missile weapon systems. [1]

ISSS System Safety Definition

System Safety is the application of **special technical and managerial skills** to the **systematic**, **forward-looking identification and control of hazards throughout the life cycle** of a product, process or program. System Safety methodology is used in Product Design Safety, Process Safety Management, Functional Safety, Chemical Process Safety, Risk Management, Human Factors, Software Safety, Cyber safety/Cybersecurity, **and Prevention Through Design**.

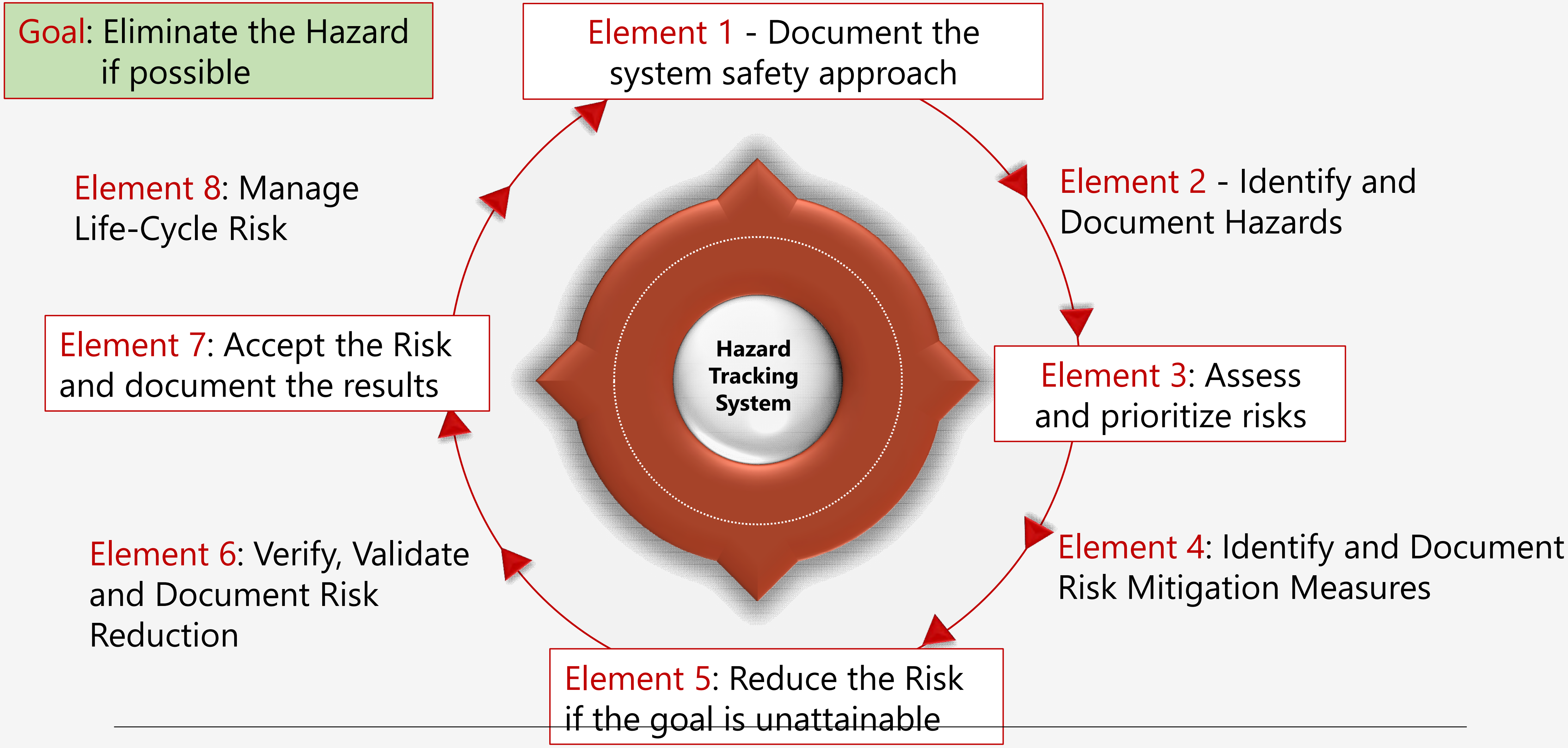
1 System Safety Engineering and management Second Edition Harold E. Roland, Brian Moriarty, pg. 10

Some System Safety Engineering widely used Standards

Standard Ref	Title Description
MIL-STD-882 - Mil	Department Of Defense Standard Practice System Safety
ARP4761 - Aero	Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment
CENELEC EN50128 - Rail	Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems
Def Stan 00-55 – Def	Requirements For Safety Related Software In Defence Equipment
Def Stan 00-56 - Def	Safety Management Requirements for Defence Systems

Other standards; NASA, ECSS, EWR, Nuclear, ….

System Safety Process - 8 Steps

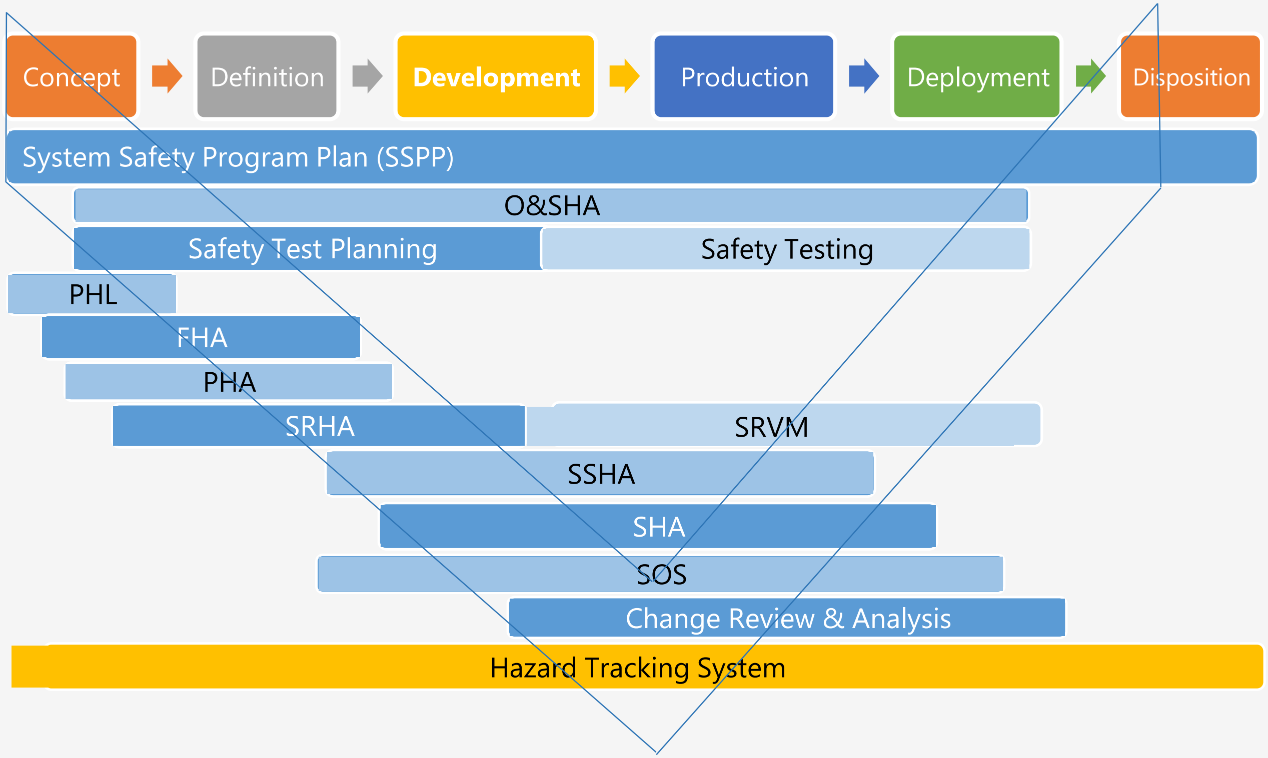


Life cycle program Phase Hazard Analysis and V&V

System / Software Safety engineering and analysis is conducted throughout the program including the System Operational Phase and disposal.

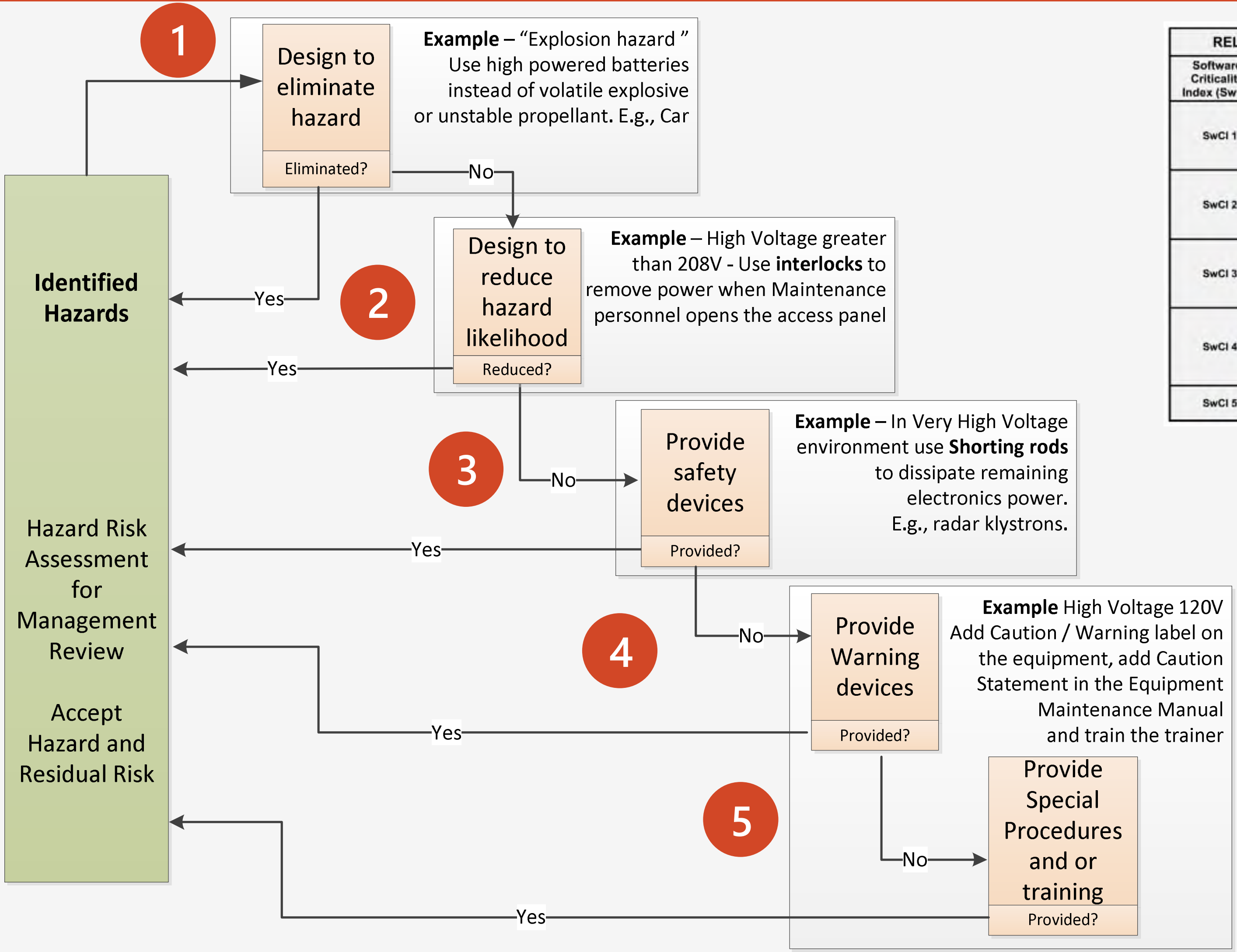
ACRONYMS

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



SYSTEM SAFETY SOCIETY
Organized 1962
Incorporated 1973
Professionals Dedicated to the Safety of Systems, Products & Services

Identification and documentation of risk mitigation measures



RELATIONSHIP BETWEEN SwCI, RISK LEVEL, LOR Tasks, AND RISK

Software Criticality Index (SwCI)	Risk Level	Software LOR Tasks and Risk Assessment/Acceptance
SwCI 1	High	• If SwCI 1 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 1 LOR tasks or prepare a formal risk assessment for acceptance of a HIGH risk.
SwCI 2	Serious	• If SwCI 2 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 2 LOR tasks or prepare a formal risk assessment for acceptance of a SERIOUS risk.
SwCI 3	Medium	• If SwCI 3 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 3 LOR tasks or prepare a formal risk assessment for acceptance of a MEDIUM risk.
SwCI 4	Low	• If SwCI 4 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 4 LOR tasks or prepare a formal risk assessment for acceptance of a LOW risk.
SwCI 5	Not Safety	• No safety-specific analyses or testing is required.

Sw Criticality Index, risk level, Level or Rigor tasks, and risk

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			

Risk Assessment Matrix

SMS – What is it?

First and foremost it is a management system

It is not:

- Accident prevention
- Safety programmes
- "What we've always done but dressed in new clothes!"

It is management of safety as a business function like finance, quality, human resources.

Combines:

- Safety Management – The discipline of safety management, with
- Institutional Arrangements – Who is accountable, how is it governed – turns it into a management system.

Where did it come from?

Three separate threads coming together:

- System Safety concepts (hazard, risk, mishaps)
- Human Factors – ergonomics (human machine interface), physiology (eg fatigue, stress), psychology (social, organisational, cognitive)
- Business Management – for aviation, driven in part by deregulation.

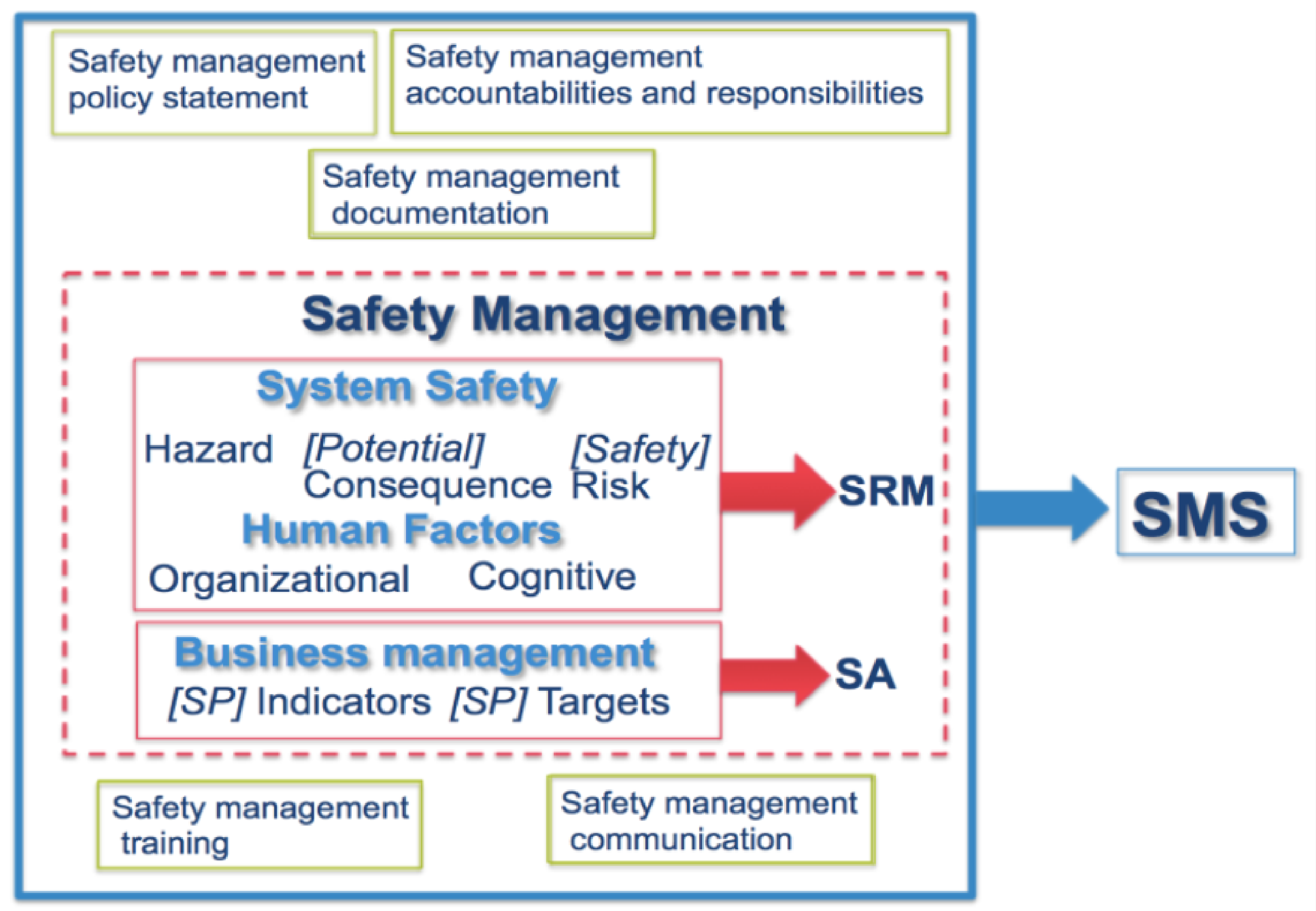
Major drivers were a series of inquiries into major disasters such as the Herald of Free Enterprise which targeted senior management deficiencies in managing safety.

What's in the SMS?

Safety Management Policy	Safety Assurance
1. Safety Management Policy Statement **2.** Safety Accountabilities and Responsibilities **3.** Integration with Public Safety and Emergency Management **4.** SMS Documentation and Records	**7.** Safety Performance Monitoring and Measurement **8.** Management of Change **9.** Continuous Improvement
Safety Risk Management	Safety Promotion
5. Hazard Identification and Analysis **6.** Safety Risk Evaluation	**10.** Safety Communication **11.** Competencies and Training

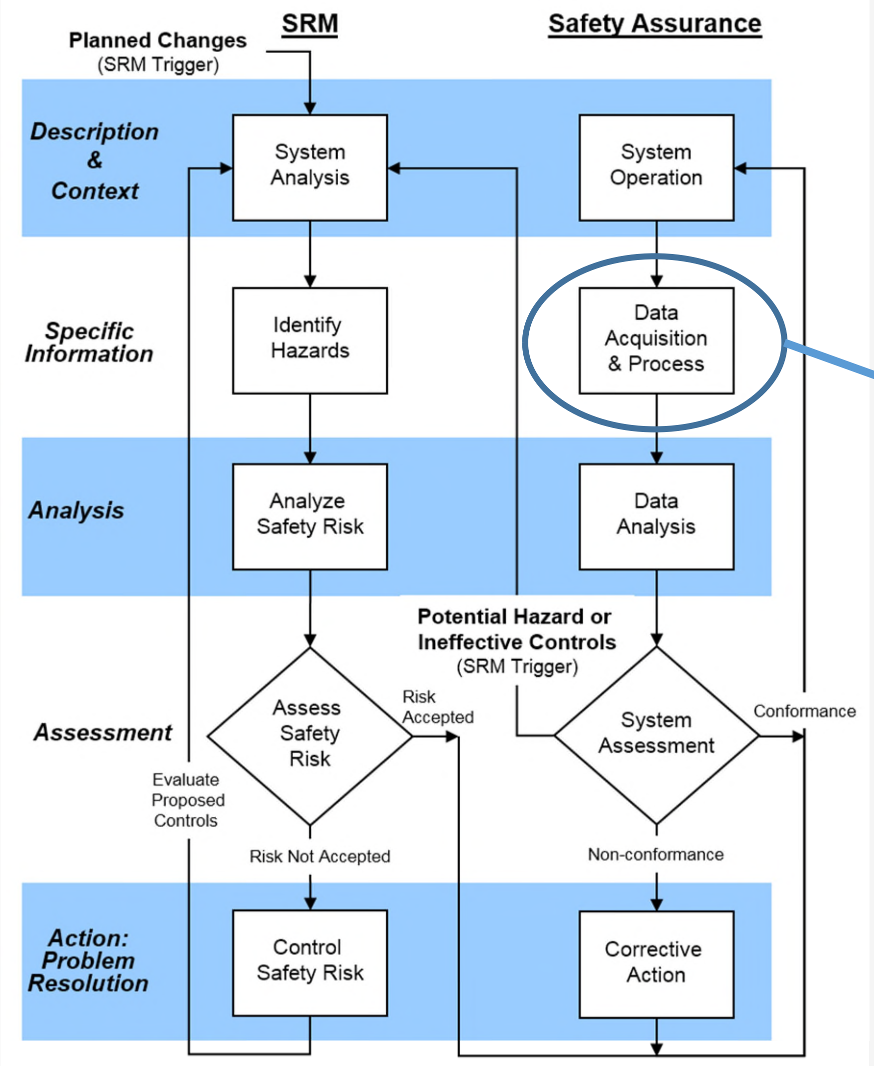
United States Federal Transit Administration

What’s in the SMS?



Dan Maurino: Why SMS, ITF Discussion Paper 2017-16

Safety Risk Management

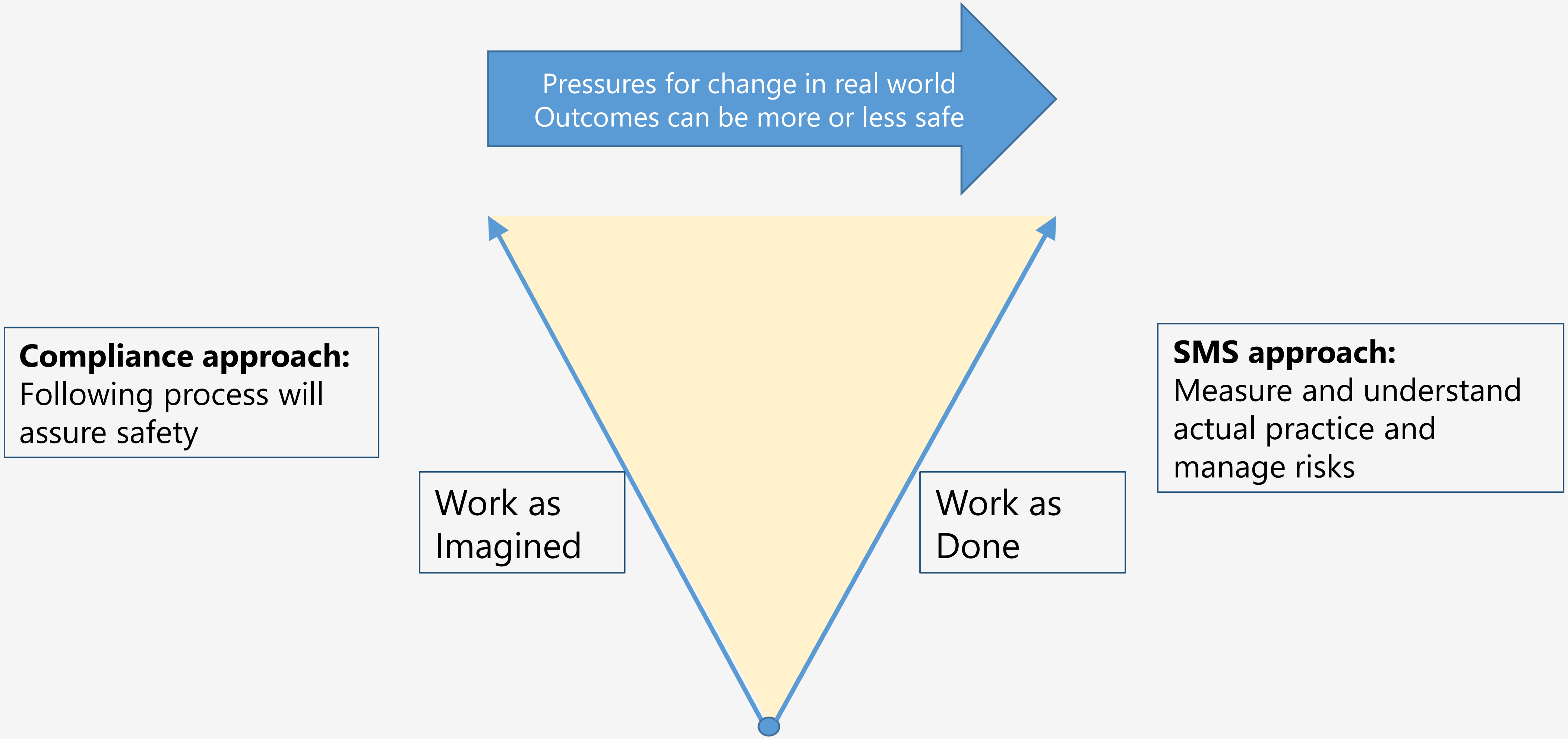


Source: FAA
https://www.faa.gov/about/initiatives/sms/explained/components/

Critical Factors:

- Focus on what really happens in the operation (work as done)
- Broad data collection – safety reporting, flight data, line observations, confidential reporting
- Reporting supported by just culture approach
- Full system approach – all aspects
- Learning from global experience – could it happen to us?

Practical Drift – Going beyond compliance

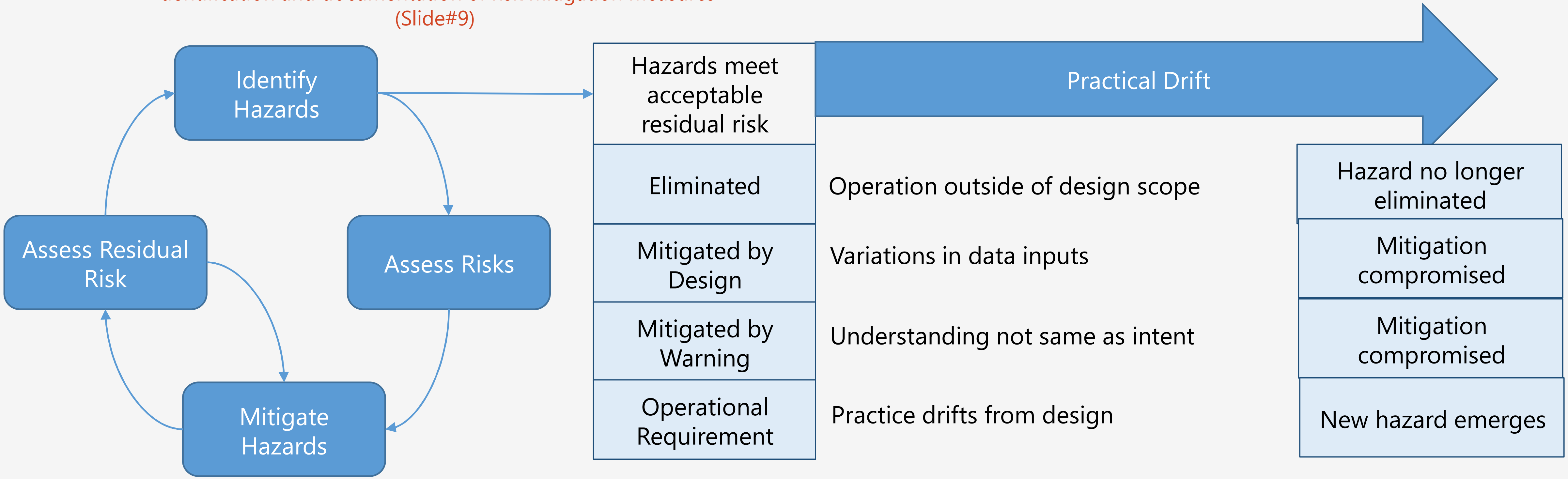


Moving from Design to Operation

Design Context

Operational Context

System Safety Engineering
Identification and documentation of risk mitigation measures
(Slide#9)



Descent Below Visual Glidepath and Impact With Seawall
Asiana Airlines Flight 214
Boeing 777-200ER, HL7742
San Francisco, California
July 6, 2013

Design/Operational Gaps

Problem Statement

The NTSB concludes that, as a result of complexities in the 777 AFCS and inadequacies in related training and documentation, the PF had an inaccurate understanding of how the AFDS and A/T interacted to control airspeed, which led to his inadvertent deactivation of automatic airspeed control.

Problem Statement

Three factors have been found to contribute to a lack of mode awareness: poor mental models, low system observability, and highly dynamic and/or nonroutine situations (Sarter and Woods 1997, 557-569). All three factors were present in this accident.

Both organizations (FAA, EASA) expressed concern that the system did not provide minimum speed protection when the AFCS was in FLCH SPD or VNAV SPD pitch mode with the A/T in HOLD mode. They expressed concern about the intuitiveness of this design from a pilot's perspective and argued that safety would be enhanced by avoiding these exceptions in the design logic.

The Problem – Critical Gaps Between Design and Operational Safety

- Hazards identified but mitigated during design (certification) may not be communicated as hazards to the operators SMS because they have been mitigated.
- As a result these hazards are effectively invisible to the SMS.
- In actual operation the “mitigated” hazards may no longer be fully mitigated.
- SMS reliant on “discovering” hazards during operation.
- Ideally the SMS hazard process should be seeded with the (mitigated) hazards from design.

The solution?

We're not suggesting a solution, but some things that we think should be in the solution:

- More and better use of HF in Design to make the system-as-designed work better in practice and therefore reduce some of the pressure to move – but there will still be practical drift because the world, context etc. will differ from the design model

- Keep the strengths of both SSE and SMS - i.e. don't try and make one into the other – they solve different problems and are good at it.

- The relationship between the two should be a well designed integration not ad hoc exchange of piecemeal data

- There needs to be a conceptual risk model that bridges the gap that doesn't force fit either side but naturally provides a basis for integration – We have been experimenting with adaptations of the BowTie risk models to meet this need and I do feel that this will be part of the solution.

Discussion

- Design and Operations
  - What happens in your industry?
  - Is this “gap” real do you think?
  - Should Design and Operating organisations work to close the gap?
  - How to address the regulatory and business challenges?
- SSE and SMS
  - Should the safety professionals in both disciplines work harder to bridge the gap?
  - How?