Session 17
SYSTEM SAFETY

System Safety Principle

- **Definition**
- **Phases of System**
- **Planning**
- **Hazard Analysis**
- **Safety Assessment**
- **Risk Management**
- **Safety Order of Precedence**
- **Behavioral-Based Safety**
- **Models used by System Safety**

System Safety Definition

- The application of **engineering** and **management** principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of **operational effectiveness** and **suitability**, **time**, and **cost**, throughout all phases of the **system life cycle.**

System Safety Definition

The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

- **Safety is not checklist.**
- **It is necessary to interpret the principles.**

System Safety Definition

The application of engineering and management principles, criteria, and techniques to achieve **acceptable** mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

- **What is acceptable risk?**
- **100% guarantee is never achieved!**

System Safety Definition

The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, **within the constraints** of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

- **Perfect technical solution is not always possible.**

System Safety Definition

The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

- **When we are done with system safety?**
- **When it went through all life-cycles stages: Initial requirements, Design, Implementation, Service, Decommissioning, Disposal**

System Safety Definition

The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the **system** life cycle.

- **System** are set of elements which interact according to a design, where an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction.

System Safety Definition

System safety is a specialty within system engineering that supports program risk management. It is 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.**

System Safety

The underlying principle is one of synergy: **a whole is more than sum of its parts.**

Systems-based approach to safety requires the application of **scientific**, technical and **managerial** skills to hazard identification, hazard analysis, and elimination, control, or management of hazards throughout the life-cycle of a system, program, project or an activity or a product

System Safety Engineering

System Safety Engineering is an engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria and techniques to identify and eliminate hazards, or reduce the risks associated with hazards.

*****System Safety - Office of Safety and Mission Assurance – NASA*

***** *NAVFAC*

System Safety Engineering

Four specific types of engineered system context are generally recognized in systems engineering :

- product system
- service system
- enterprise system
- system of systems

*** ***DCS - Distributed Control System***

System Safety Engineering

System of systems?

System of systems is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems.

System Safety

Why management?

Because experience has shown that many failures are not due to systems being built the wrong way but actually the **wrong systems having been built.**

In other words, management is there to make sure that engineering actually is doing the right thing (in all aspects).

Brief History of Systems Engineering

Water Distribution System in Mesopotamia	4000 BC
Irrigation System in Egypt	3300 BC
Urban Systems e.g. Athens and Greece	400 BC
Roman Highway Systems	300 BC
Water Transportation Systems e.g. Erie Canal	1800s
Telephone Systems	1877
Electrical Power Distribution Systems	1800
Systems Eng'g Concepts@Bell Labs and the military (WWII)	1900
Bell Telephone Laboratories	1940
DOD applied systems eng'g to missiles and missile defense	1940s
RAND Corp. (US Air Force) developed systems analysis	1946
ATLAS ICBM Program Managed by Ramo-Woolridge Corp	1954-1964
Defense Systems Management College (DMSC)	1971
National Council on Systems Eng'g	1990
International Council on Systems Eng'g (INCOSE)	1995
75US, 141 international universities offer systems eng'g program	2006

The System Phase

The Conceptual Phase - considers the basic principles of the system and formulates the preliminary designs and methods of operation. *It is at this stage that hazard and operability studies should be taken.*

The Design and Engineering Phase - develops the basic idea from the conceptual phase and augments them to translate into practical equipment and procedures. This phase should include testing and analysis of the various components to ensure compliance with various system specifications. *It is at this stage that job safety analysis should be undertaken.*

The System Phase

The Operational Phase - involves the bringing together of the various components - i.e. manpower, materials, machinery, methods - in order to achieve the purpose of the system. *From a practical viewpoint, it is at this stage that safe systems of the work should be developed and communicated.*

The Disposal Phase - begins when machinery and manpower are no longer needed to achieve the purpose of the system. *All components must be efficiently disposed of, transferred, reallocated or placed into storage.*

System Safety

What we do?

- 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

System Safety

How to do it?

- **Oversight and progress monitored thru:**
  - **Peer review of deliverable safety analyses**
  - **Customer / Regulatory Authority approval**
  - **Periodic System Safety Working Group meetings**

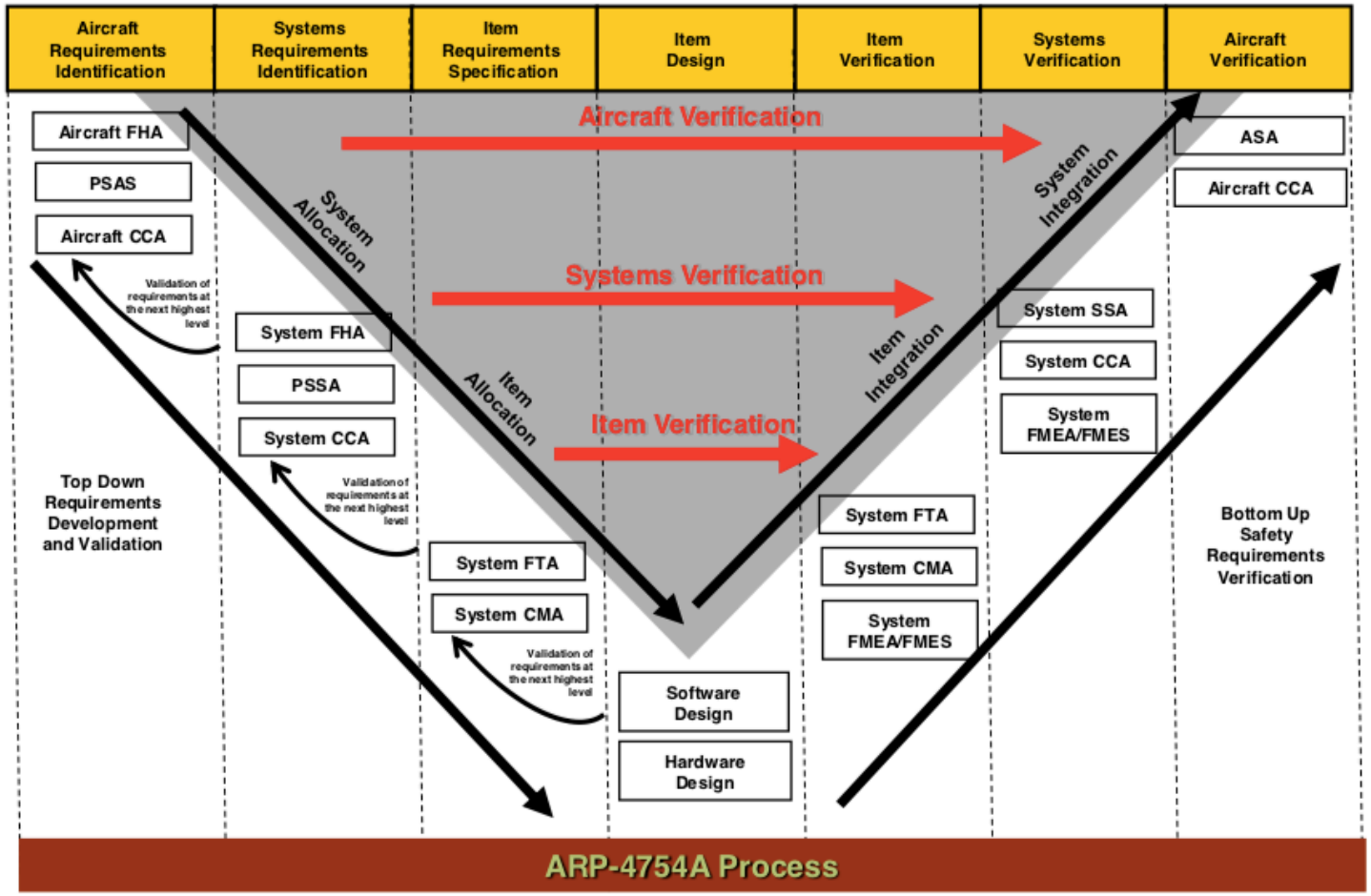
System Safety

When to do it?

- **Throughout the entire program starting from design to maintenance**

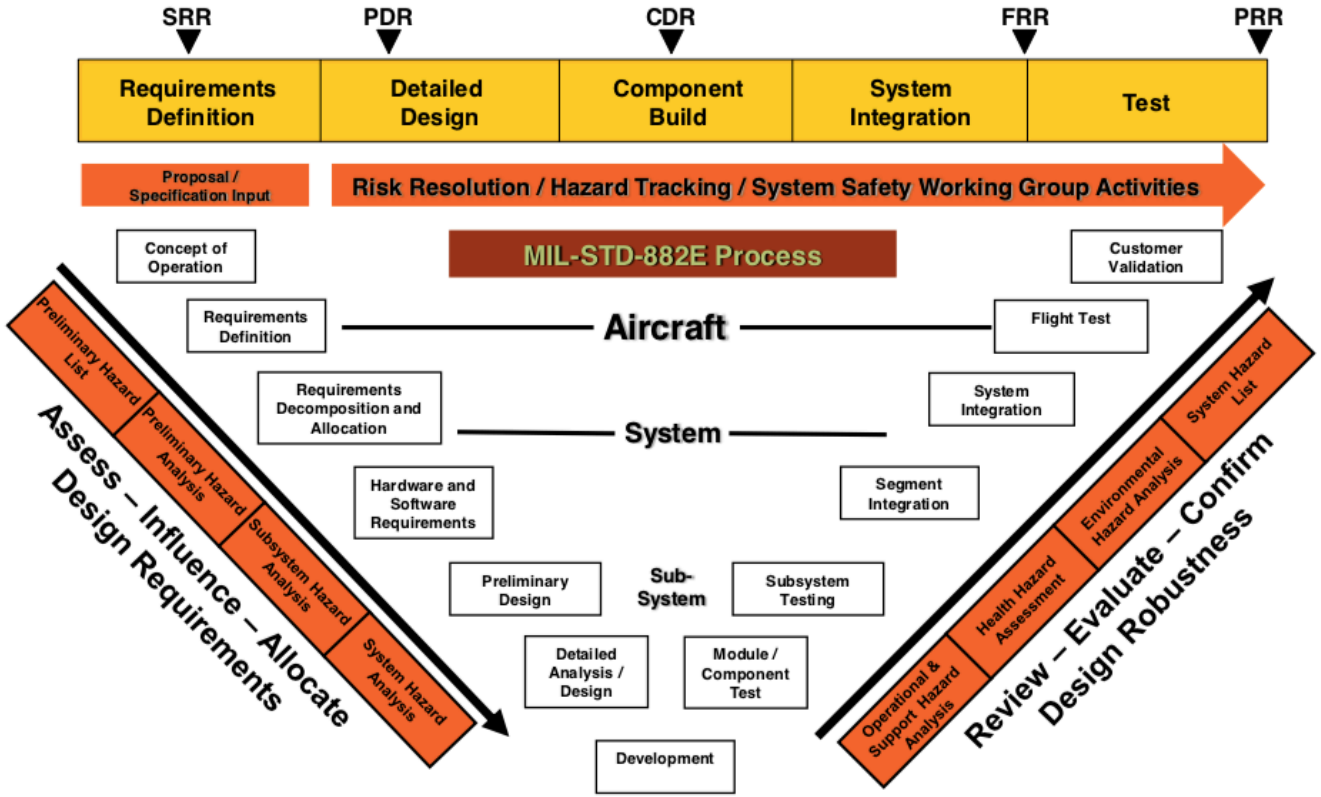
SYSTEM SAFETY – CIVIL PROGRAMS

Interaction Between Safety and Development Processes



SYSTEM SAFETY – USG PROGRAMS

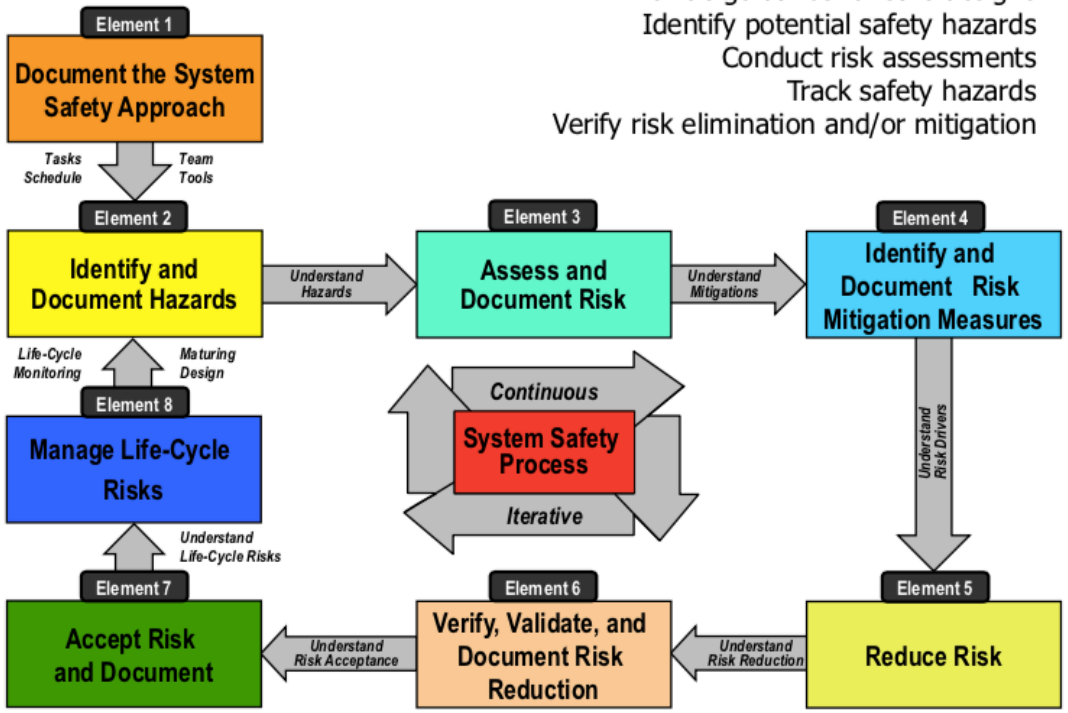
Integrated with System Engineering (SE) Process



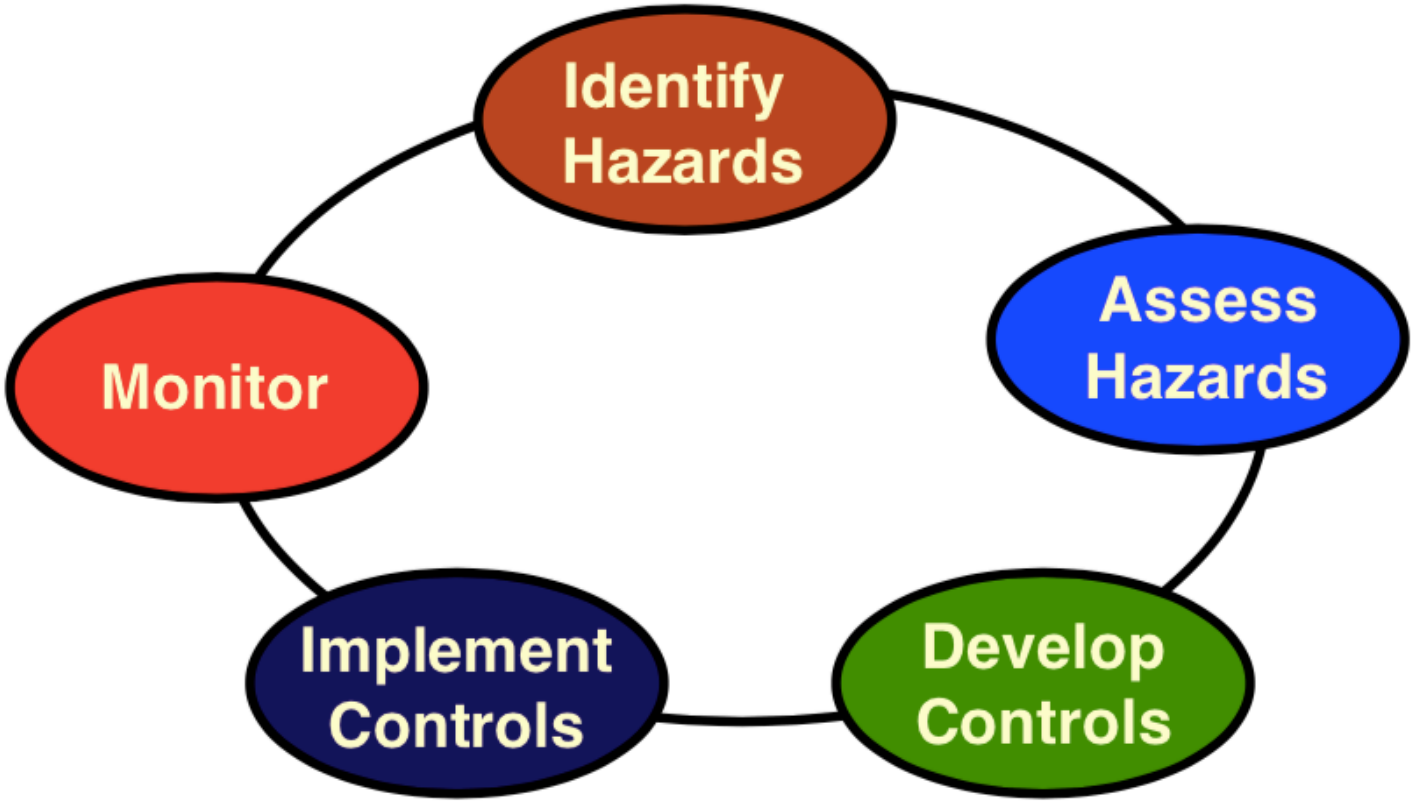
DOD SYSTEM SAFETY PROCESS

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



RISK MANAGEMENT PROCESS



Principles of System Safety

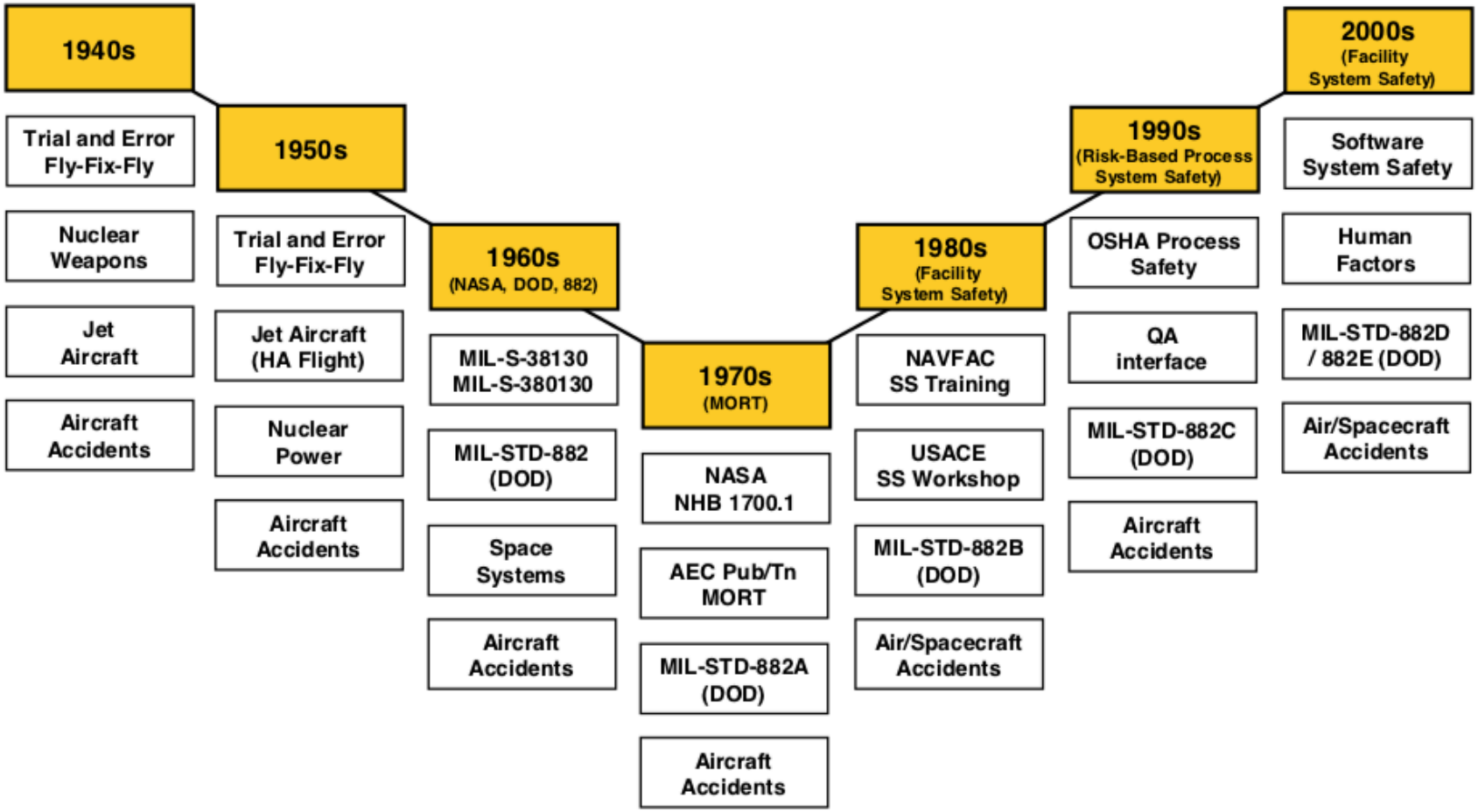
1. A pre-requisite for the study of system safety is a working knowledge of the principles of systems of work:

- Job safety analysis
- An appreciation of how hazard and operability studies

2. System safety technique emanated from the aviation and aerospace industries, where the overriding concern is for the complete system to work as designed, so that no one gets injured as a result of malfunction.

SYSTEM SAFETY

History



Principles of System Safety

3. Therefore, system safety technique maybe applied in order to eliminate any machinery malfunctions or mistakes in design that could have serious consequences.

4. Thus- there is a need to analyze critically the complete system in order to anticipate risks and estimate the maximum potential loss associated with such risks.

5M model of System Engineering

1. **Mission.** The mission is the purpose or central function of the system. This is the reason that all the other elements are brought together.
2. **Man.** This is the human element of a system. If a system requires humans for operation, maintenance, or installation this element must be considered in the system description.
3. **Machine.** This is the hardware and software (including firmware) element of a system.

5M model of System Engineering

4. **Management.** Management includes the procedures, policy, and regulations involved in operating, maintaining, installing, and decommissioning a system.
5. **Media.** Media is the environment in which a system will be operated, maintained, and installed. This environment includes operational and ambient conditions.

System Safety Hazard Order of Precedence

Priority 1: Design for minimum risk.

1. **Eliminate hazard through design selection - select design or material that removes hazard**
2. **Reduce risk through design alteration - consider a design change that reduces mishap severity or probability**

IMPLEMENT CONTROLS

System Safety Hazard Order of Precedence

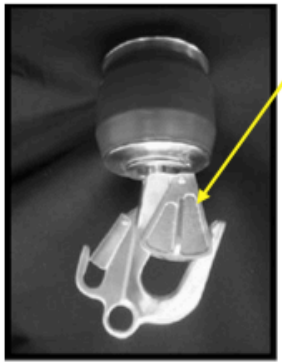
Design Selection / Design Alternatives/ Engineered Features and Devices

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

SYSTEM SAFETY

System Safety Design Influence
(Rescue Hoist D-Ring Reversal)

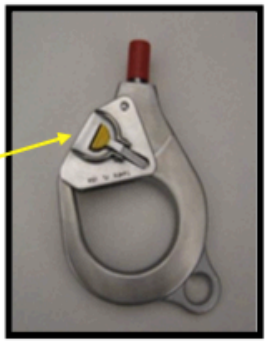
1. Design Selection



Spring-loaded guard

Superseded MS 18107 hook

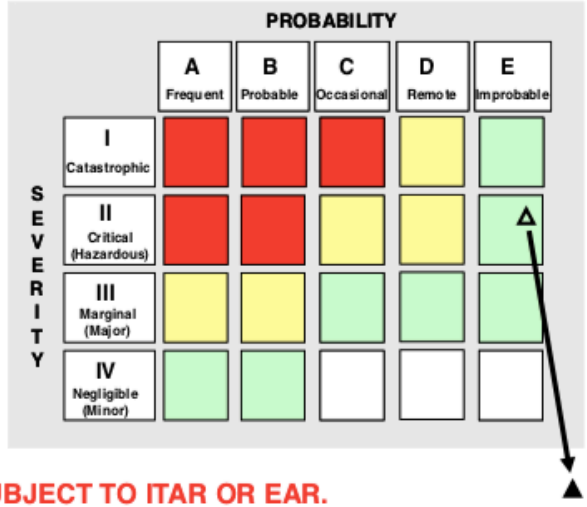
Positive locking feature



New design with cable D-Lok

Safety Hazard Assessment: Rescue Hoist D-Ring										Risk Mitigation Measure: 1
Hazard	**Hazardous Effects**	**Causal Factors**	**IS**	**IP**	**IRC**	**Risk Mitigation**	**FS**	**FP**	**FRC**	**Status**
Harness D-ring disengages from rescue hoist hook	Injury or death of hoist passenger(s); destruction of hoist cargo; potential for injury/damage to ground personnel and equipment	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.	I	E	Low	Rescue hoist hook guard redesigned to provide positive locking feature.	None	None	None	Closed. Hazard eliminated thru redesign of hook guard to preclude potential for D-ring reversal.

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



Safety Order of Precedence

Priority 2: Incorporate engineered features or safety devices.

…..reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.

SYSTEM SAFETY

System Safety Design Influence
(Landing Gear Wheel Servicing)

Attention: Aviation Director
Chief of Maintenance
Chief Helicopter Pilot

CCS-92-AOL-07-00006
26 Mar 07

Subject: S-92 Landing Gear Wheel Improvement

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 for 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

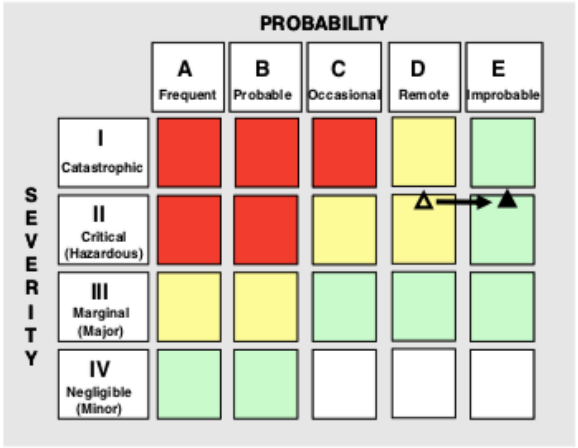
2. Safety Devices

Overpressure relief valve

Safety Hazard Assessment: Landing Gear Wheel Servicing — **Risk Mitigation Measure: 2**

Hazard	Hazardous Effects	Causal Factors	IS	IP	IRC	Risk Mitigation	FS	FP	FRC	Status
Landing gear wheel burst	Severe injury and/or death of aircraft maintainer	Failure to properly set nitrogen bottle regulator pressure prior to servicing landing gear wheels.	I	D	Med.	Incorporated an integral pressure relief valve into the landing gear wheel nitrogen servicing valve.	I	E	Low	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.

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



SUBJECT TO ITAR OR EAR.

Safety Order of Precedence

Priority 3: Provide warning devices.

……devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response. Warning signs shall be provided to alert operational and support personnel of such risks as exposure to high voltage and heavy objects.

IMPLEMENT CONTROLS

System Safety Hazard Order of Precedence

Warning Devices

Safety Order of Precedence

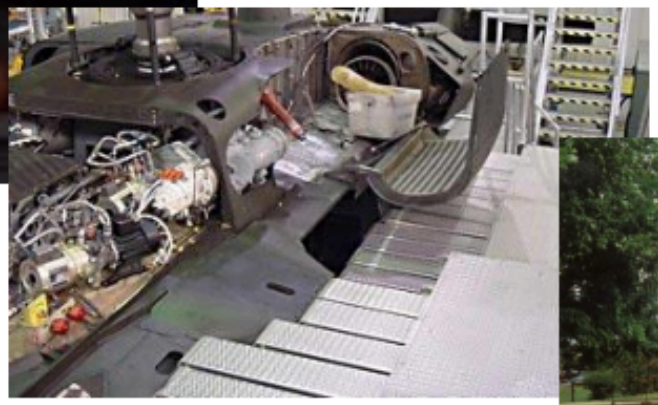
Priority 4: Develop procedures and training.

Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic, hazardous, major, or critical severity.

IMPLEMENT CONTROLS

System Safety Hazard Order of Precedence

Special Procedures and Training



Two (2) Basic and Interrelated Aspects of Safety System Engineering

1. **System Safety Management** - provides the framework wherein findings and recommendations resulting from the application of system safety analysis techniques can effectively be reviewed and implemented.

2. **System Safety Analysis** - employs the three basic elements of identification, evaluation, and communication to facilitate the establishment of cause.

Method of Analysis Used in Safety

Hazard and Operability Study

1. Technique of Operations Review - analytical technique of tracing the underlying and contributory factors that cause failure of a system. It is associated with the theory of multi-causality of accidents.

2. Gross Hazard Analysis - this is done early in the design stage, and would be a part of "HAZOP" (hazard operability) study. It is the initial step in the system safety analysis, and it considers the total system.

Method of Analysis Used in Safety

4. Classification of Risks - involves the identification and evaluation of risks by type and impact (i .e. maximum potential loss on the company). A further analysis - Risk Ranking may also be undertaken.

5. Risk Ranking - a rank ordering of the identified and evaluated risks is drawn up, ranging from the most critical down to the least critical. This enables priorities to be set, and resources to be allocated.

Method of Analysis Used in Safety

6. Failure Modes and Effects - the kinds of failures that could happen are examined, and their effects in terms of maximum potential loss are evaluated. Again this analysis would from part of an overall HAZOP Study.

7. Fault Tree Analysis - an analytical technique that is used to trace the chronological progression of factors contributing to the accident situation, and useful not only for the system safety, but also in accident investigation. The principle of multi-causality is utilized in this type of analysis.

Fault-Tree Analysis

- technique used to trace back through the chronological progression of causes and effects that have contributed to a particular event, whether it be an accident (industrial safety) or failure (system safety).
- logic diagram based on the principle of multi-casualty that traces all the branches of events that could contribute to an accident or failure.

System Safety Analysis Provides

1. Loss identification
2. Evaluation and communication factor
3. Interactions within a given system which could cause inadvertent injury, death or material damage during any phase or activity associated with given systems lifecycle.

Inspection Testing and Maintenance

Maintaining reliability throughout the entire life cycle of a system/s involves three distinct and equally important tasks which must be performed on a periodic basis:

- Periodic Visual Inspection
- Functional Testing
- Maintenance Activities

Many overlook the need to visually inspect the system and concentrate only on the functional testing of the components. However, each of these tasks are necessary and contribute to the assurance of the system

Inspection Testing and Maintenance

Periodic Visual Inspection

A **periodic inspection** is a visual examination of the equipment to verify that nothing has changed from the initial design and installation that would affect its performance. Those charged with performing an inspection should be looking for a number of conditions which might affect the system's ability to perform when called upon.

Inspection Testing and Maintenance

Periodic Visual Inspection

A **periodic inspection** is a visual examination of the equipment to verify that nothing has changed from the initial design and installation that would affect its performance. Those charged with performing an inspection should be looking for a number of conditions which might affect the system's ability to perform when called upon.

Inspection Testing and Maintenance

Periodic visual inspection - should consider various changes during its use:

- Change in environmental conditions
- Device orientation
- Physical damage
- Degree of cleanliness

Inspection Testing and Maintenance

Functional testing - is intended to validate the functionality of the system. Tests are performed by operating each component of the system to assure it performs as required in the case of an actual emergency event.

Inspection Testing and Maintenance

Functional testing - a proper testing program should include the following:

- testing the operation of all Emergency Control Functions in the system
- test method for many components may also involve the use of calibrated test equipment
- testing frequencies

Inspection Testing and Maintenance

Functional testing - a proper testing program should include the following:

- testing the operation of all Emergency Control Functions in the system
- test method for many components may also involve the use of calibrated test equipment
- testing frequencies

Inspection Testing and Maintenance

Maintenance - is the work necessary to keep the fire system operating properly. One form of maintenance is simply a response to a failure identified by a visual inspection or a test of the equipment. Whenever repairs are not made immediately, a temporary alternative means of protection should be put in place until the system is returned to an acceptable level of readiness.

Inspection Testing and Maintenance

Maintenance - is the work necessary to keep the fire system operating properly. One form of maintenance is simply a **response to a failure identified by a visual inspection or a test of the equipment.** Whenever repairs are not made immediately, a temporary alternative means of protection should be put in place until the system is returned to an acceptable level of readiness.

Inspection Testing and Maintenance

Maintenance - is the work necessary to keep the fire system operating properly. One form of maintenance is simply a **response to a failure identified by a visual inspection or a test of the equipment.** Whenever repairs are not made immediately, a temporary alternative means of protection should be put in place until the system is returned to an acceptable level of readiness.

Inspection Testing and Maintenance

Maintenance - many components in a system will require **preventative maintenance** at a prescribed frequency. These maintenance activities address components that degrade over time:

- calibration or periodic resetting
- components that have finite lifespan that needs replacement
- components that needs cleaning

Inspection Testing and Maintenance

In a survey conducted by the California State Board of Fire Services*, building owners were asked about the current operational status of their fire systems and about the factors contributing to failures. 73% of the respondents cited a lack of maintenance as the cause for system failures. The truth is a proper inspection, testing and maintenance program will benefit not only in money savings over time, but even more importantly, will minimize an organization's risk of liability.

Source: "Report to the Legislature in Response to House Resolution No. 14, Fire Alarm Systems," December 30, 1983, Office of the State Fire Marshal, Sacramento, CA 95823.

SYSTEM SAFETY

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.


Any
Questions?