RAMCRAFT
Reliability & Safety Management

# Safety Management in Multidisciplinary Systems

## SSRM symposium
## TA University, 26 October 2011

**By Boris Zaets**





RAMCRAFT
Reliability & Safety Management

# AGENDA

1 **Introduction**
2 **Safety standards and guidelines**
4 **System Safety Management**
5 **Safety Targets Definition and Allocation**
6 **Safety Analysis Technique**

RAMCRAFT Reliability & Safety Management

# REFERENCES

| | | |
|---|---|---|
| Military | MIL-STD-882C | System Safety Program Requirements |
| | MIL-STD-882D | Standard Practice for System Safety |
| UK Defence | DEF STAN 00-56, Issue 4 | Safety Management Requirements for Defence Systems |
| SAE | ARP4761 | Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne System and Equipment |
| NATO | STANAG 4671 | Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR) |
| RTCA, Inc. | DO-254 | Design Assurance Guidance For Airborne Electronic Hardware |
| | DO-178 | Software Considerations in Airborne Systems and Equipment Certification |
| CENELEC | EN 50126 | Railway applications: Systematic Allocation of Safety Integrity Requirements |

3

RAMCRAFT Reliability & Safety Management

# DEFINITIONS

- **Safety**: Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment
- **Mishap:** An unintended event, or sequence of events, that causes death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment
- **Hazards**: A physical situation, or state of a system, often following from some initiating event, that may lead to an Mishap


4

## DEFINITIONS (cont.)

- **System Safety Concept** is the application of special technical and managerial skills to the systematic, forward looking identification and control of hazards throughout the life cycle of project, program or activity
- **Safety Management:** The application of organizational and management principles in order to achieve safety with high confidence.
- **Risk Management** is a process of ensuring that hazard and potential accidents are identified and managed, and is a process managed within the Safety Management System
- **Safe** does not imply that there is an absence of risk, but that the risk has been demonstrably reduced to a level that is Broadly Acceptable or Tolerable.

5

## Safety Management Activities

- Identify all safety legislation, regulations, standards and particular requirements relevant to the safety of the system
- Define the system, its boundaries and its operating environment. The definition of the system shall include all relevant elements that constitute the system.
- Produce the Safety Management & Program Plans

6

## Risk Management Activities

- Hazards and Mishaps (accidents) Identification
- Hazard Analysis
- Risk Estimation
- Risk Reduction
- Risk Acceptance

7

## Mishap Criteria Categories

| Description | Category | Definition |
|---|---|---|
| Catastrophic | I | Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation. |
| Critical | II | Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation. |
| Marginal | III | Could result in injury or occupational illness resulting in one or more lost work days (s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be complished. |
| Negligible | IV | Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation. |

8

RAMCRAFT
Reliability & Safety Management

# Safety Objectives Example

- A set of safety requirements for a system will include requirements that directly relate to compliance with safety legislative, regulations, standards or customer policy, contractual requirements, and requirements that are derived from other safety requirements.

| SEVERITY PROBABILITY | Level | Probability Range | Catastr. I | Critical II | Marginal III | Negligible IV |
|---|---|---|---|---|---|---|
| FREQUENT | A | $x>10^{-1}$ | 1 | 3 | 7 | 13 |
| PROBABLE | B | $10^{-2}<x<10^{-1}$ | 2 | 5 | 9 | 16 |
| OCCASIONAL | C | $10^{-3}<x<10^{-2}$ | 4 | 6 | 11 | 18 |
| REMOTE | D | $10^{-5}<x<10^{-3}$ | 8 | 10 | 14 | 19 |
| IMPROBABLE | E | $x<10^{-5}$ | 12 | 15 | 17 | 20 |

9

RAMCRAFT
Reliability & Safety Management

# General System Safety Design Requirements - Example

- Eliminate identified hazards or reduce associated risk through design, including material selection or substitution. When potentially hazardous materials must be used, select those with least risk throughout the life cycle of the system.
- Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous chemicals, high voltage, electromagnetic radiation, cutting edges, or sharp points).
- Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration and vibration).
- Design to minimize risk created by human error in the operation and support of the system.
- Consider alternate approaches to minimize risk from hazards that cannot be eliminated. Such approaches include interlocks, redundancy, fail safe design, system protection, fire suppression, and protective clothing, equipment, devices, and procedures.
- Protect the power sources, controls and critical components of redundant subsystems by physical separation or shielding.

10

RAMCRAFT
Reliability & Safety Management

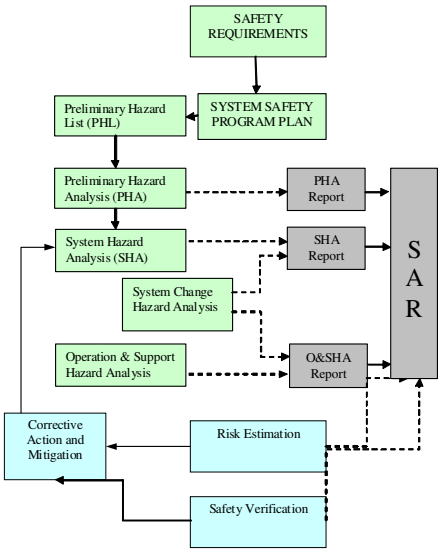
# Unacceptable Conditions - Example

- Single component failure, common mode failure, human error, or a design feature that could cause a mishap of Catastrophic or Critical mishap severity categories.
- Dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of Catastrophic or Critical mishap severity categories.
- Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.
- Packaging or handling procedures and characteristics that could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.
- Hazard categories that are specified as unacceptable in the development agreement.

11

RAMCRAFT
Reliability & Safety Management

# Safety Assessment Process




12

## System Safety Program Plan

- System Safety Programme Plan (SSPP) is the principal methodology for managing the achievement of the safety requirements. The SSPP shall include the following:
  - Program scope and objectives
  - System safety organization
  - System safety program milestones
  - Life Cycle phases
  - General system safety requirements and criteria
  - Hazard analysis techniques, format and depth
  - System safety data
  - Safety verification
  - Audit program
  - Training
  - System safety interfaces

13

## Safety Assessment Technique

### Functional Hazard Assessment

- Functional Hazard Assessment (FHA) is **systematic examination of functions to identify and classify failure conditions of those functions according to their severity** and it is performed in the early phases of the design.
- The FHA should identify the failure conditions **for each phase of system life** when the failure effect and classification vary from one phase to another.
- The FHA also **establishes derived safety requirements** needed to mitigate the function failure effects, which effect failure condition classification.
- As a result of FHA, the **Hazard identification** will be performed. This will create Preliminary Hazard List (**PHL**) and provides the basis for the initial Hazard Log.

14

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

## FHA Example

| 1 Function | 2 Failure Condition (Hazard Description) | 3 Phase | 4 Effect of Failure Condition on Aircraft/Crew | 5 Classification | 6 Reference to Supporting Material | 7 Verification |
|---|---|---|---|---|---|---|
| Decelerate Aircraft on the Ground | Loss of Deceleration Capability | Landing /RTO/ Taxi | See Below | | | |
| | a. Unannunciated loss of deceleration capability | Landing /RTO | Crew is unable to decelerate the aircraft, resulting in a high speed overrun. | Catastrophic | | S18 Aircraft Fault Tree |
| | b. Annunciated loss of deceleration capability | Landing | Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun. | Hazardous | Emergency landing procedures in case of loss of stopping capability | S18 Aircraft Fault Tree |
| | c. Unannunciated loss of deceleration capability | Taxi | Crew is unable to stop the aircraft on the taxi way or gate resulting in low speed contact with terminal, aircraft, or vehicles. | Major | | |
| | d. Annunciated loss of deceleration capability | Taxi | Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs. | No Safety Effect | | |
| | Inadvertent Deceleration after V1 (Takeoff/RTO decision speed) | Takeoff | Crew is unable to takeoff due to application of brakes at the same time as high thrust settings, resulting in a high speed overrun. | Catastrophic | | S18 Aircraft Fault Tree |

15

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

## Preliminary Hazard Analysis

- Preliminary Hazard Analysis (PHA) is a high level analysis of the functions of the system based on an appraisal of the system by a team with different areas of expertise, centred on "What if ?" questions. **It should consider all relevant available data, including the accident and incident data from similar systems** recorded in the PHL Report.
- Preliminary Hazard Analysis (PHA) should identify **failures contributing to the Hazards** identified from the FHA.
- PHA is used to complete the failure conditions list and the corresponding safety requirements. It is also used to **demonstrate how the system will meet the qualitative and quantitative requirements** for various hazards identified
- PHA will include **preliminary risk assessment and the proposed/ implemented mitigations**
- PHA should be performed **as early as possible** during the system lifecycle in order to obtain maximum benefit.

16

RAMCRAFT
Reliability & Safety Management

# PHA Example - Engine Cut in Flight

- **System Phase**
  - Flight
- **Effect of Hazard**
  - No propulsion, followed by Emergency Recovery
- **Hazard cause**
  - Engine malfunction
  - Fuel system malfunction
  - Oil system malfunction
- **Item Identification**
  - Fuel System, Oil System, Power system, Throttle actuator, Main Computer
- **Risk assessment**
  - Severity: Critical
  - Probability: Probable
- **Hazard Indication**
  - BIT
- **Mitigation Method**
  - Redundancy of Throttle actuator
  - Redundancy of Propulsion sensors (RPM, Crank position, temperature, fuel level, oil level)
  - Redundancy of fuel pumps
  - Redundancy of relevant Power rails
  - Redundancy of fuel pressure filters
  - Redundancy of Central Computer

17

RAMCRAFT
Reliability & Safety Management

# Safety Assessment Technique

## System Hazard Analysis

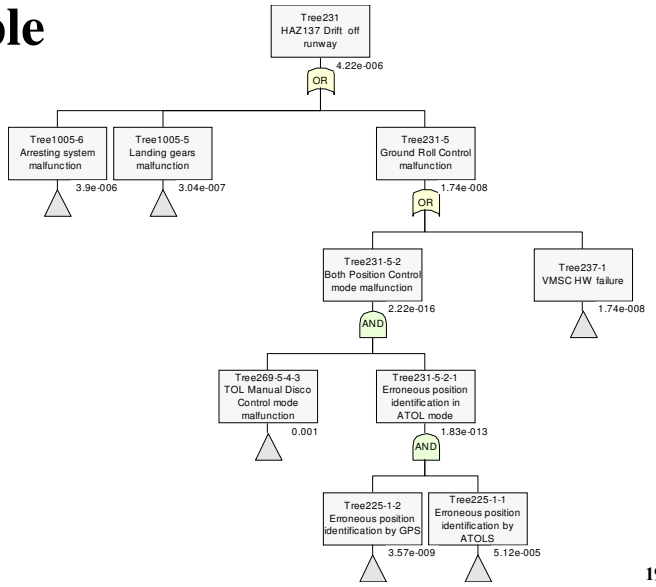
- System Hazard Analysis (SHA) is performed to **refine and extend the identification and causes of hazards and accident sequences from the previous analyses**, by consideration of the abstract functions of the system and subsequently the components that implement them.
- The difference between PHA and SHA is that a PHA is a method to evaluate proposed architectures and derive system/subsystem safety requirements; whereas the SHA is a verification that the implemented design meets both the quantitative and qualitative safety requirements defined in FHA and PHA.
- SHA is an iterative process that evolves throughout the program
- The SHA will comprise the results of activities stated in this SPP and in R&M Programme Plan. This will include:
  - Failure Modes Effects and Criticality Analysis (FMECA).
  - Fault Tree Analysis (FTA)
  - Common Cause Analysis (CCA)

18

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

## FTA Example



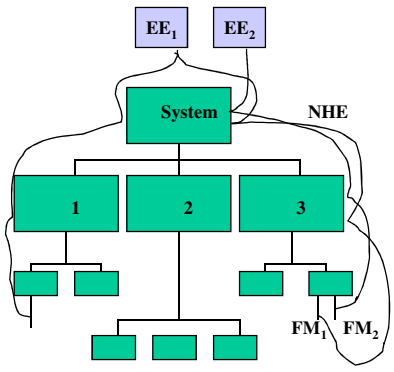

19

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

## FMECA

- Reference Document: MIL-STD-1629 - Failure Mode, Effect and Criticality Analysis (FMECA)
- FMECA is applied at the functional block level (or component level if required) and proceeds through increasing hierarchical levels (bottom-up approach) until analysis is completed at System level.
- Ground rules and assumptions:
  - Only one failure at a time in the analyzed unit is assumed.
  - All input signals are assumed to be undistorted and all potential failures are supposed to be created by malfunction of the given functional block only.




20

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

## Operating and Support Hazard Analysis

- Operating and Support Hazard Analysis (O&SHA) consists of the identification and analysis of **hazardous activities, or carried out under hazardous conditions, associated with the operation and support of sub-systems and equipment** during various stages of the lifecycle.
- O&SHA evaluates hazardous tasks undertaken by operation and support staff during phases such as **storage, transportation and operation** of the system.
- O&SHA covers the hazards caused by system operation and have an **impact on ground personnel and/or environment**.
- O&SHA takes into account **human failures**

21

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

## O&SHA Example: Inadvertent Laser Fire

| | |
|---|---|
| **Turnaround Phase** | Preflight |
| **Background** | During preflight testing the Laser is activated according to LASER test procedure. Unintended Laser firing could expose operational personnel to radiation hazards. |
| **Hazard Description** | Laser activation may present a hazard to personnel and flammable materials. Laser activation must be at quite low power levels because the available power is concentrated into beams of very small cross sectional area |
| **Effect of Hazard** | The hazard to personnel is burning of the area of the body exposed to the radiation. The major hazard is eye damage, which may arise not only by direct illumination but also by reflected radiation. |
| **Hazard Cause** | Possible hazard causes are human error or/and malfunction of safety interlock and HW/SW safety keys |
| **Item Identification** | TE, PCDU, Central Computer, Mission Computer, Payload |

22

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

## O&SHA Example: Inadvertent Laser Fire

| | |
|---|---|
| **Rational for Safety Assessment** | Inadvertent Laser fire can happen as a result of safety margin reduction caused by single event or combination of several events:<br>•Inadvertent Laser Power ON. Inadvertent Laser Fire Command<br>•Inadvertent Laser Trigger Enable |
| **Risk Assessment** | Severity: II<br>Probability: Incredible<br>Risk: Acceptable |
| **Hazard Indication** | Hazard indication by BIT |
| **Mitigation Method** | •Laser Fire shall be performed only if the following conditions shall be fulfilled:<br>•Safe provisions of Laser Power by simultaneous activation of UAV Master Arm and Flight Tester Master Arm commands<br>•Laser Trigger Enable<br>•Laser Fire Command<br>•Application of Guard Payload cover during Payload test<br>•Usage of Warning labels and Safety goggles for operational personnel<br>•Adequate communication between Ground station and UAV operators |

23

RAMCRAFT Reliability & Safety Management

# Safety Assessment Technique

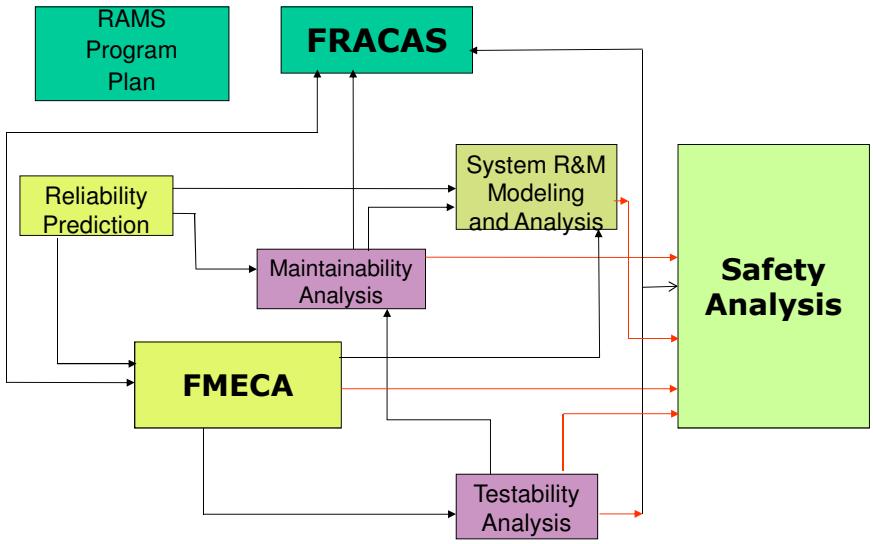
## Safety Assessment

- The purpose of Safety Assessment is to perform and document a comprehensive evaluation of the mishap risk being assumed prior to test or operation of a system.
- Safety Assessment Report (SAR) summarizes the safety assessment activity.

24

RAMCRAFT
Reliability & Safety Management

# RAMS Data Flow and Interfaces




25