Workshop - Design of Dependable Systems – Fundamentals of Aircraft Safety
7th Scandinavian Conference on SYSTEM & SOFTWARE SAFETY, Stockholm, October 22-23, 2019

Design of Dependable Systems
Fundamentals of Aircraft Safety
Part 2

Kristina Forsberg, Saab, Håkan Forsberg, MDH
2019-10-23

PART 2 - Aircraft development from a safety perspective

- Requirements for development of aircraft and aircraft systems
  - CS 25.1309 / FAR 25.1309
  - AMC 25.1309

- Safety process
  - FHA
  - PSSA
  - SSA
  - CCA

Aviation Safety - organisations

Governments joined together in the United Nations organ for International Civil Aviation Organization (ICAO)

The airlines of the world also joined together, in an organisation called the International Air Transport Association – the IATA

In Europe the governments joined together in the European Union, and handed over a lot of their authority to the European Aviation Safety Agency- The EASA

Aircraft Safety

Airworthiness standards are based on, and incorporate, the objectives and principles or techniques of ***the fail-safe design concept***, which considers the effects of failures and combinations of failures in defining a safe design.

FAIL-SAFE DESIGN CONCEPT – PRINCIPLES AND TECHNIQUES

(i) Designed Integrity and Quality, including Life Limits, to ensure intended function and prevent failures.

(ii) Redundancy or Backup Systems to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.

(iii) Isolation and/or Segregation of Systems, Components, and Elements so that the failure of one does not cause the failure of another.

(iv) Proven Reliability so that multiple, independent failures are unlikely to occur during the same flight.

Source: CS-25 BOOK 2 AMC 25.1309

FAIL-SAFE DESIGN CONCEPT – PRINCIPLES AND TECHNIQUES

(v) Failure Warning or Indication to provide detection.

(vi) Flight crew Procedures specifying corrective action for use after failure detection.

(vii) Checkability: the capability to check a component's condition.

(viii) Designed Failure Effect Limits, including the capability to sustain damage, to limit the safety impact or effects of a failure.

Source: CS-25 BOOK 2 AMC 25.1309

FAIL-SAFE DESIGN CONCEPT – PRINCIPLES AND TECHNIQUES

(ix) Designed Failure Path to control and direct the effects of a failure in a way that limits its safety impact.

(x) Margins or Factors of Safety to allow for any undefined or unforeseeable adverse conditions.

(xi) Error-Tolerance that considers adverse effects of foreseeable errors during the aeroplane's design, test, manufacture, operation, and maintenance.

Source: CS-25 BOOK 2 AMC 25.1309

CS 25.1309 EQUIPMENT, SYSTEMS AND INSTALLATIONS

The requirements of this paragraph, except as identified below, are applicable, in addition to specific design requirements of CS-25, to any equipment or system as installed in the aeroplane. Although this paragraph does not apply to …

(a) The aeroplane equipment and systems must be designed and installed so that:
(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the aeroplane operating and environmental conditions.
(2) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a)(1) of this paragraph.

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that –
(1) Any catastrophic failure condition
(i) is extremely improbable; and
(ii) does not result from a single failure; and
(2) Any hazardous failure condition is extremely remote; and
(3) Any major failure condition is remote.

(c) Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action. A warning indication must be provided if immediate corrective action is required. Systems and controls, including indications and annunciations must be designed to minimise crew errors, which could create additional hazards.

(d) Electrical wiring interconnection systems must be assessed in accordance with the requirements of CS 25.1709.

Failure Condition classification

(1) ***No Safety Effect:*** Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the aeroplane or increase crew workload.

(2) ***Minor:*** Failure Conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.

(3) ***Major:*** Failure Conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.

(4) ***Hazardous:*** Failure Conditions, which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating, conditions to the extent that there would be:

- (i) A large reduction in safety margins or functional capabilities;
- (ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
- (iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.

(5) ***Catastrophic:*** Failure Conditions, which would result in multiple fatalities, usually with the loss of the aeroplane.

Source: CS-25 BOOK 2 AMC 25.1309

PROBABILITY TERMS

(FAA AC 25.1309-1A OR JAR AMJ 25.1309)

- **Probable** Failure Conditions: Probable Failure Conditions are those anticipated to occur one or more times during the entire operational life of each aeroplane. Probable Failure Conditions are those having a probability of the order of **1×10^{-5}** or greater.
  Minor Failure Conditions may be probable.

Improbable Failure Conditions are divided into two categories as follows:

- (i) **Remote**: Unlikely to occur to each aeroplane during its total life but may occur several times when considering the total operational life of a number of aeroplanes of the same type.
  Improbable (Remote) Failure Conditions are those having a probability of the order of **1×10^{-5}** or less, but greater than of the order of 1×10^{-7}.
  Major Failure Conditions must be no more frequent than Improbable (Remote).

- (ii) **Extremely Remote**. Unlikely to occur when considering the total operational life of all aeroplanes of the same type, but nevertheless has to be considered as being possible.
  Improbable (Extremely Remote) Failure Conditions are those having a probability of the order of **1×10^{-7}** or less, Annex to ED Decision 2007/020/R Amendment 4 but greater than of the order of 1×10^{-9}.
  Hazardous Failure Conditions must be no more frequent than Improbable (Extremely Remote).

- **Extremely Improbable** Failure Conditions: Extremely Improbable Failure Conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type, and have a probability of the order of **1×10^{-9}** or less.
  Catastrophic Failure Conditions must be shown to be Extremely Improbable.

Acceptable Means of Compliance 25.1309

Aircraft-level functions are implemented using diverse and redundant system architectures and capabilities as mitigation techniques to achieve an acceptable level of safety at the aircraft level

Acceptable level of safety at the aircraft level for large aiplanes:

Ensure that Major Failure Conditions are Remote, Hazardous Failure Conditions are Extremely Remote, and Catastrophic Failure Conditions are Extremely Improbable.

Source: CS-25 BOOK 2 AMC 25.1309

Aircraft Development

- Several guidance documents are used in order to cover the different phases and aspects of concern developing safety-critical avionics.

- An additional important RTCA document not included in the picture is **DO-160** which covers Environmental Conditions and Test Procedures for Airborne Equipment

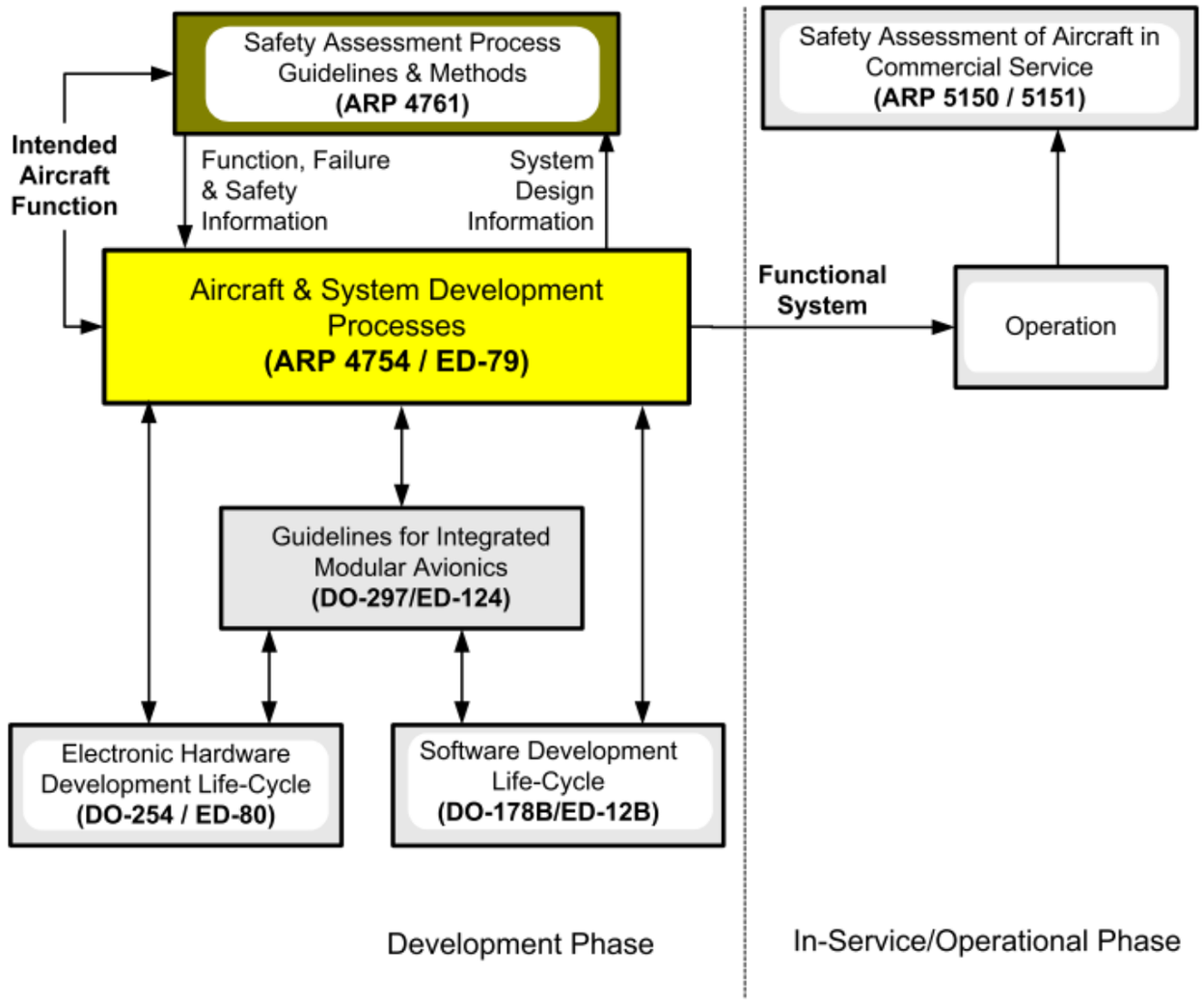

FIGURE 1 - GUIDELINE DOCUMENTS COVERING DEVELOPMENT AND IN-SERVICE/OPERATIONAL PHASES

Image Source: SAE ARP4754A

ARP 4754A development

Safety Assessment Process
combined with
Fail-safe design techniques
is used to show compliance with certification requirements

- **Safety assessment process includes:**
  - FHA, Functional Hazard Assessment
  - PSSA, Preliminary System Safety Assessment
  - SSA, System Safety Assessment
  - CCA, Common Cause Analysis

Processes and analysis methods are detailed in ARP 4761

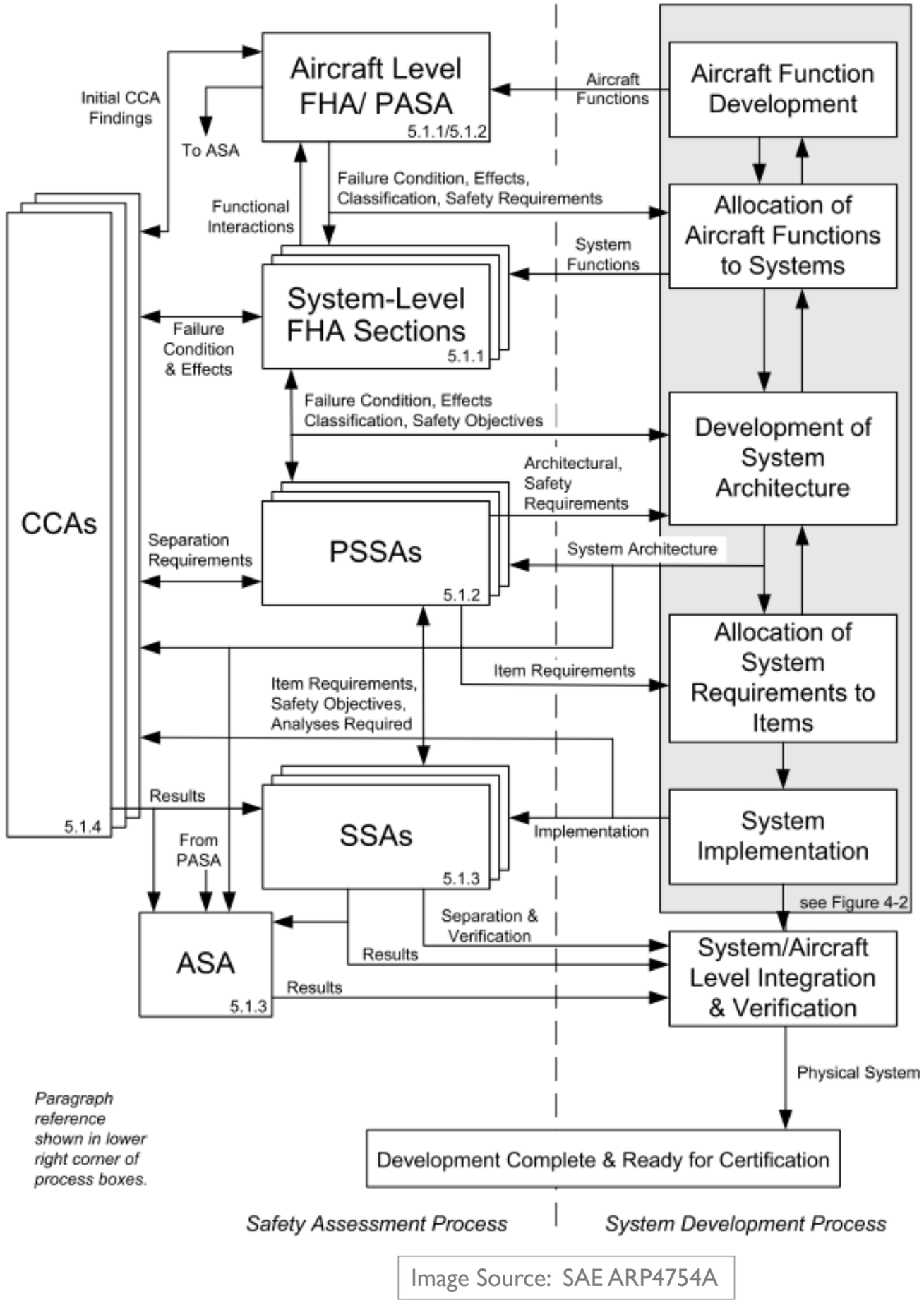

Image Source: SAE ARP4754A

Safety Assessment Process

- **FHA**: Examines aircraft and system functions to identify potential functional failures and classifies the hazards associated with specific failure conditions. The FHA is developed early in the development process and is updated as new functions or Failure Conditions are identified. Thus, the FHA is a living document throughout the design development cycle.

- Need understanding of **Intended function,** for MCAS e.g.
  - Design parameters
  - Authority (activation limits)
  - Activation conditions
  - Procedure in flight manual
  - …

MCAS classification

- In normal flight an activation of MCAS to the maximum assumed authority of 0.6 degrees was classified as a “major failure”

- In case of an extreme maneuver an activation of MCAS was classified as a “hazardous failure”

Source: Dominic Gates, The Seattle Times, ”Flawed analysis, failed oversight: How Boeing, FAA certified the suspect 737 MAX flight control system,” March 17, 2019 (updated March 21, 2019)

Safety Assessment Process

- **PSSA:** Establish the aircraft or specific system or item safety requirements and provide a preliminary indication that the anticipated aircraft or system architectures can meet those safety requirements.

- MCAS safety objectives:
  - Erroneous activation HAZ, the probability of FC less than **$1x10^{-7}$** /fh
  - Uncommanded activation (?)

Safety Assessment Process

- **SSA**: Collects, analyzes, and documents verification that the aircraft and systems, ***as implemented***, meet the safety requirements established by the PSSA.

- MCAS authority
  - Failed to account for how the system could reset itself each time a pilot responded, thereby missing the potential impact of the system repeatedly pushing the airplane's nose downward.
- MCAS design parameters
  - MCAS was capable of moving the stabilizer more than four times farther than was stated in the initial safety analysis document.