SESSION ONE HANDOUT

The following extract is from Section 5.1 of ARP 4754B ((R) Guidelines for Development of Civil Aircraft and Systems).

5.1 Safety Assessment

The safety assessment process is used to show compliance with certification requirements and internal safety standards. The process includes specific assessments that are conducted and updated during system development. These assessments interact with system development processes throughout the development lifecycle. The safety assessment process consists of the six principal assessment processes summarized in the sub-sections 5.1.1 through 5.1.6. These principal assessment processes consist of the Aircraft Functional Hazard Assessment (AFHA), Preliminary Aircraft Safety Assessment (PASA), System Functional Hazard Assessment (SFHA), Preliminary System Safety Assessment (PSSA), System Safety Assessment (SSA), and Aircraft Safety Assessment (ASA) processes.

The safety assessment process includes safety analysis methods which may be applied throughout the typical development cycle to provide the analyst a means of qualitatively and/or quantitatively assessing the safety of a design. These methods include Fault Tree Analysis (FTA), Dependency Diagram (DD), Markov Analysis (MA), Model Based Safety Analysis (MBSA), Failure Mode and Effects Analysis/Summary (FMEA/FMES), Cascading Effects Analysis (CEA), Particular Risk Analysis (PRA), Zonal Safety Analysis (ZSA), and Common Mode Analysis (CMA). The method(s) selected will vary based on system characteristics and organizational practices. The results of these methods may stand alone or be incorporated into any of the higher-level assessments.

Independence between functions, systems, equipment, or items may be required to satisfy the safety requirements. Therefore, it is necessary to ensure that such independence exists, or that the lack of independence is acceptable. The PRA, ZSA, and CMA provide the methods for evaluation of independence or the identification of specific dependencies due to common cause. These methods may also aid the PASA and PSSA in generation of independence requirements (e.g., physical, installation requirements).

The safety assessment process is detailed in ARP4761A/ED-135.

Figure 5-1 shows the fundamental relationships between the safety assessment processes and the system development processes. In reality, there are many feedback loops within and among these relationships, though they have been omitted from the figure for clarity.

The level of detail needed for the various safety assessment activities is dependent on the aircraft-level failure condition classification, the degree of integration, and the complexity of the system implementation. The safety assessment process should be planned and managed so as to provide the necessary assurance that all relevant failure conditions have been identified, and that all significant combinations of

failures that could cause those failure conditions have been considered. The safety assessment process is of fundamental importance in establishing appropriate safety objectives for the aircraft and systems and determining that the implementation satisfies these objectives.

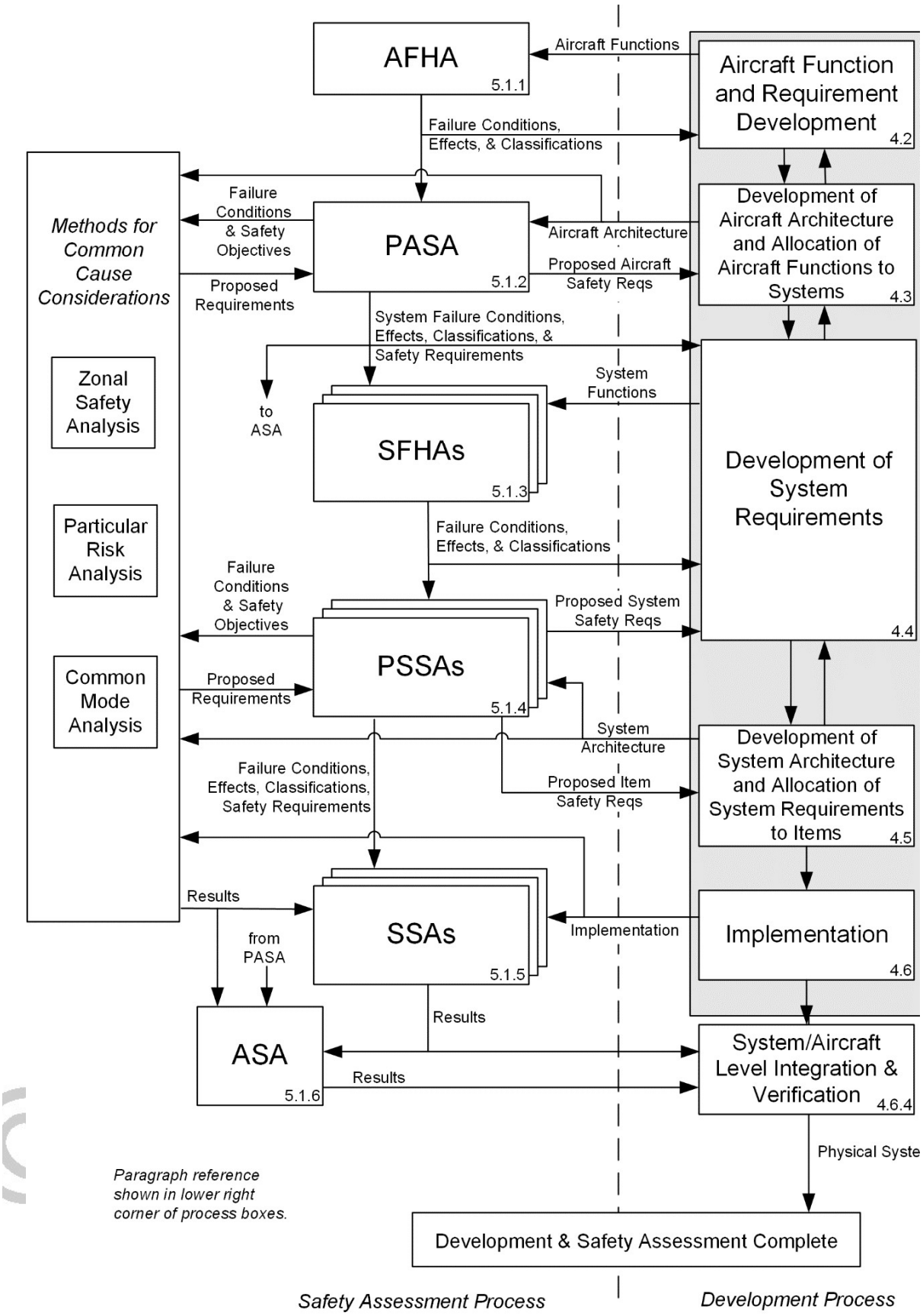

Figure 5-1 – Safety Assessment Process Model

Figure 5-1 Safety Assessment Process

5.1.1 Aircraft Functional Hazard Assessment

The AFHA is a process that allows the identification and evaluation of potential hazards related to an aircraft's functions regardless of the details of its design. The objectives of the AFHA process are to identify the failure conditions associated with the aircraft functions.

The objectives of the AFHA process are accomplished by systematically analyzing the aircraft-level functions to identify the failure conditions, determine their effects on the aircraft, crew, and occupants, and then to establish the associated severity classification. The classification of these Failure Conditions establishes the safety objectives for the aircraft. Assumptions made during the AFHA process should be captured and confirmed to be correct.

Failure conditions and associated safety objectives may be monitored through the development process to track that the design implementation is satisfying the safety objectives.

Appendix A of ARP4761A/ED-135 provides guidelines on how to perform an AFHA.

5.1.2 Preliminary Aircraft Safety Assessment

The PASA is a systematic, comprehensive evaluation of a proposed aircraft architecture to determine how failures, errors, or external events can lead to aircraft-level failure conditions identified by the AFHA and how the aircraft-level safety objectives can be met. The objectives of the PASA process are to evaluate the proposed architecture against the safety objectives, and to propose aircraft-level safety requirements and assumptions.

The PASA identifies the interactions and dependencies between the aircraft systems, assesses how their failures can lead to the aircraft-level failure conditions identified by the AFHA, and determines whether the aircraft-level safety objectives can be met. The PASA process interacts with the development process by evaluating the aircraft architecture against aircraft- level safety objectives and identifies the need for specific aircraft-level and system-level safety requirements. Just as the development process is iterative, the PASA process is iterative throughout the development cycle. The PASA process may use various qualitative and/or quantitative safety analysis methods. Common cause considerations are taken into account in the PASA process. The PASA evaluates combined functional failure effects of the related systems and potential common cause failures between them, including consideration of their shared resources. The PASA also identifies the independence requirements and Function Development Assurance Level (FDAL) assignments for the associated aircraft functions. Once the aircraft-level safety requirements have been identified through the PASA process and the implementing systems' designs mature, the ASA process may be initiated.

Appendix B of ARP4761A/ED-135 provides guidelines on how to perform a PASA.

5.1.3 System Functional Hazard Assessment

The SFHA is a systematic process that allows the identification and evaluation of potential hazards related to a system's functions regardless of the details of its implementation. It is performed at the beginning of the system development process and re-evaluated any time changes are made to the system functions. The objectives of the SFHA process are to identify the failure conditions associated with the system functions.

The objectives of the SFHA process are accomplished by systematically analysing the system-level functions to identify the failure conditions, determine their effects on the aircraft, crew, and occupants, and then to establish the associated severity classification. Crew awareness, flight phase, and environmental and operational conditions are also considered in the assessment. The classification of these failure conditions establishes the safety objectives for the system. Assumptions made during the SFHA process should be captured and confirmed to be correct.

Failure conditions and associated safety objectives may be monitored through the development process to track that the design implementation is satisfying the safety objectives.

Appendix C of ARP4761A/ED-135 provides guidelines on how to perform an SFHA.

5.1.4 Preliminary System Safety Assessment

The PSSA process is a systematic evaluation of a proposed system architecture to determine how failures, errors, or external events can lead to system-level failure conditions identified by the SFHA and how the system-level safety objectives can be met. The objectives of the PSSA process are to evaluate the proposed system architecture against the safety objectives and allocated requirements from PASA, and to propose system-level safety requirements and assumptions.

Through the PSSA process, safety requirements for system, subsystem, and items are identified to guide the architecture development as necessary to meet the safety objectives and requirements. The PSSA process may use various safety analysis methods to determine these requirements. The PSSA also identifies the necessary FDAL and Item Development Assurance Level (IDAL) assignments for the system functions and items.

The PSSA process identifies where protective strategies may be needed to meet the safety objectives. Such protective strategies may include redundancy, monitoring, partitioning, development assurance rigor, built-in-test, and safety-related maintenance tasks/intervals.

The PSSA process is interactive and associated with the design definition. Just as the development process is iterative, the PSSA process is iterative. The PSSA process starts in the early phases of design with the evaluation of the system architecture to identify and propose system-level safety requirements. System-level safety requirements are then allocated to subsystems and finally subsystem requirements are allocated to equipment/items. The PSSA assignment of IDALs to

items determines the appropriate hardware and software development assurance rigor. The PSSA also generates item requirements including but not limited to safety, reliability, independence, and separation. Common cause considerations are taken into account in the PSSA process. Care should be taken to account for potential latent failures and their associated exposure times. Once the system-level safety requirements have been identified through the PSSA process and the implementing subsystems/equipment/items' designs mature, the SSA process may be initiated.

Appendix D of ARP4761A/ED-135 provides guidelines on how to perform a PSSA.

5.1.5 System Safety Assessment
The SSA is a systematic, comprehensive evaluation of the implemented system. The objective of the SSA process is to confirm that the safety objectives and relevant safety requirements are satisfied. The difference between the PSSA and the SSA is that the PSSA is a process to evaluate proposed architectures and identify safety requirements, whereas the SSA is a process to verify that the implemented design meets both the qualitative and quantitative safety objectives and requirements as defined in the SFHA and PSSA, and safety requirements passed from the PASA.

The SSA integrates the results of the various analyses to verify the safety of the overall system and to cover all relevant safety requirements identified in the PSSA. The SSA process documentation includes results of the related analyses and their substantiations as needed. The SSA also includes applicable common cause consideration results.

The SSA process is generally represented through succeeding levels of verification through different levels of systems, subsystems, and items. Through these upward hierarchical verification levels, hardware reliability requirements and architectural requirements are verified against the safety requirements identified in the PSSA process.

The SSA establishes maximum exposure times for latent failures to be considered for aspects of the aircraft operation and maintenance.

Appendix E of ARP4761A/ED-135 provides guidelines on how to perform an SSA.

5.1.6 Aircraft Safety Assessment
The ASA is a systematic, comprehensive evaluation of the complete aircraft. The objective of the ASA process is to confirm that the safety objectives and relevant safety requirements are satisfied. The difference between a PASA and an ASA is that a PASA is a process to evaluate proposed architectures and identify safety requirements, whereas the ASA is verification that the implemented design meets both the qualitative and quantitative safety objectives and requirements as defined in the AFHA and PASA.

The ASA integrates the results of the various analyses to verify the safety of the overall aircraft and systems. This ASA is refined and updated throughout the development process to reflect the updated design.

The ASA uses the results obtained from the PASA and SSAs and includes assessment of interdependencies between the aircraft functions and systems. The ASA ensures that system failure modes are considered for inclusion. The ASA also includes applicable common cause consideration results and checks for consistency of those results with PASA's and SSAs' results.

Appendix F of ARP4761A/ED-135 provides guidelines on how to perform an ASA.

5.1.7 Safety Program Plan

For appropriate management of the safety assessment process, a safety program plan should be created. The safety program plan(s) should define the scope and the content of the safety activities that are applicable at the aircraft and system levels.

The following provides an overview of topics that should be covered, unless otherwise justified, through the safety program plan to support development assurance:

1. Identify the input data for the safety assessment process
2. Identify applicable safety standards
3. Identify the project safety organization and define responsibilities within this organization and its relationship with partners and/or suppliers with respect to the safety process
4. Describe the applicable safety assessment activities and their outputs, including the associated deliverables
5. Define the key project milestones for which safety process outputs are required
6. Include the principles of the management and validation of the safety objectives, assumptions, and safety requirements, and the verification that the design meets those requirements
7. Identify the links with the other appropriate plans (e.g., validation plan, verification plan, process assurance plan)

The safety program plan may address additional safety topics beyond those that support development assurance, including company policies, company procedures, and specific safety details necessary to support certification. Appendix B herein provides an example for organizing the contents of an aircraft-level safety program plan.

5.1.8 Safety-Related Flight Operations or Maintenance Tasks

The safety assessment may rely on or take into consideration flight crew, aircraft operations, or maintenance personnel actions. The tasks and procedures assumed to be performed may be necessary to ensure safety requirements are met. Where human performed tasks or limitations are relied on to ensure safety or to form part of the certification substantiation, they should be identified and recorded in the certification data. Regulatory guidance on specific types of tasks and limitations may be applicable (e.g., AC/AMC 25-19A for Certification Maintenance Requirements on transport category airplanes).

5.1.9 Relationship with In-Service Safety

A process for accomplishing in-service safety assessment is described in ARP5150A and ARP5151A or in other documents, such as the guidance material of EASA Part 21 (GM21) when required by applicable regulation. These documents contain an in-depth study of the processes used to establish and maintain surveillance of safety concerns on in-service aircraft (i.e., continued airworthiness) and to resolve those issues and document the resolutions.

Taken as a whole, ARP4761A/ED-135 and ARP5150A (or ARP5151A or other applicable guidance material) encompass the safety assessment process for the entire life cycle of the civil aircraft and its systems and items from conceptual design to obsolescence.

Safety is not self-sustaining. When an aircraft is delivered it has an initial level of safety as identified by the SSA(s) and ASA. As aircraft are operated, the level of safety is maintained through a continuing process of monitoring service experience, identifying safety-related issues and opportunities, and then addressing these issues through appropriate product or procedure changes.

The In-Service Safety Assessment Process includes the following:

1. Maintain the airworthiness (certification) of the aircraft
2. Maintain the safety of the aircraft
3. Improve the safety of the aircraft

The in-service safety assessment process is expected to be continuous, iterative, and closed-loop. When an event is identified, assessed, and action implemented, the monitoring continues to validate the effectiveness of the action.