Safety Assessment Processes of ARP4761: Major Revision

Jim Marko

Manager, Aircraft Integration & Safety Assessment

14 November 2018

Presentation Outline

- What is changing
- ARP4761 Relationship to ARP4754A Development Assurance
- New methods
- Changes to existing methods
- Safety methods other than ARP4761A

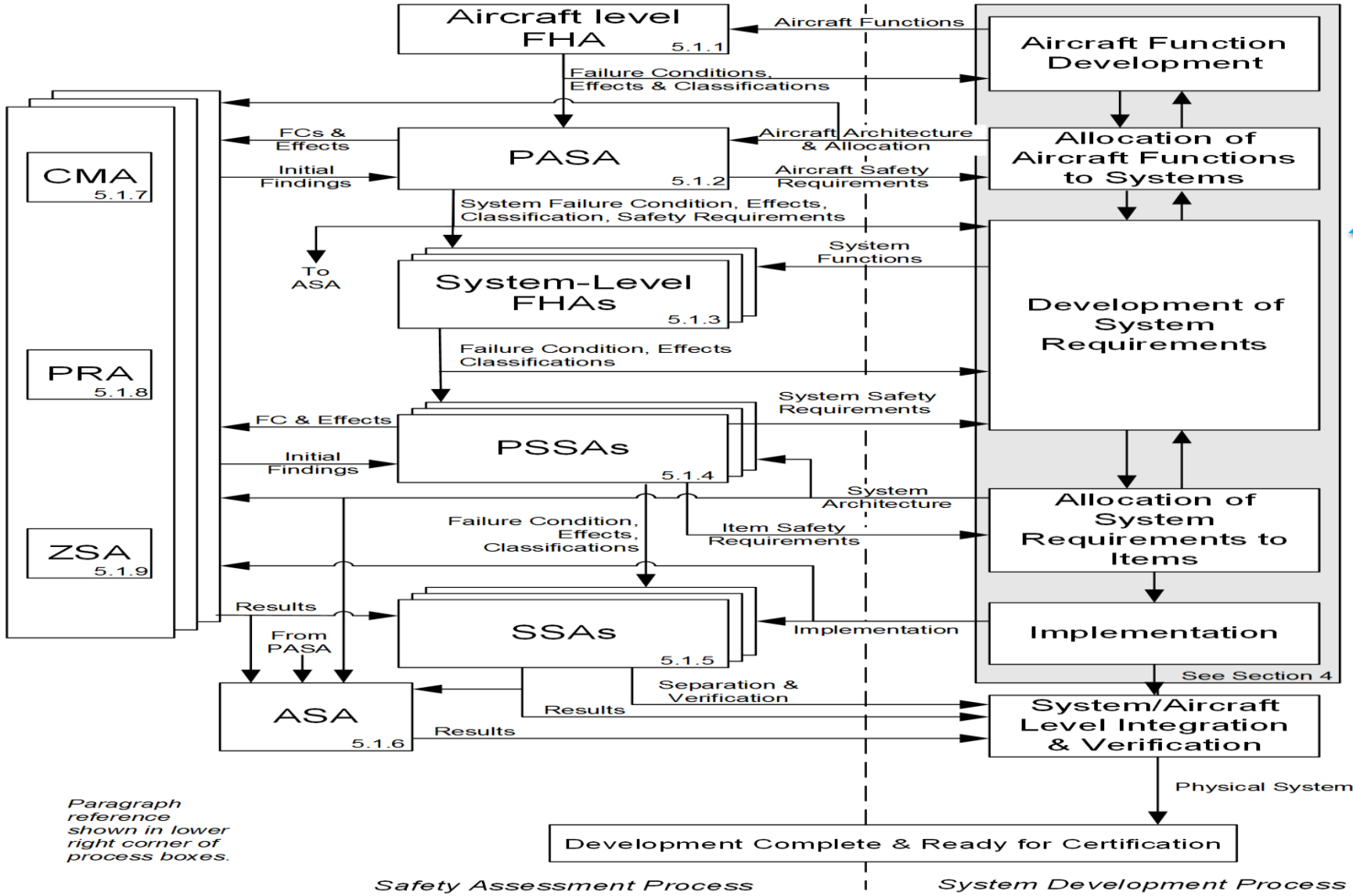
ARP4761A Safety Assessment Process

What's happening to ARP 4761?

- Revision commenced in early 2012 within the SAE S18 Aircraft & Systems Development and Safety Assessment Committee.
- Essentially a near complete revision of the document that is nearing publication.
- New processes and analytical methods being added to reflect the trend towards more highly integrated and increasingly complex system designs.
- Introduces the concept of Aircraft-Level safety assessment to complement the traditional system-level safety assessment approach.

Current ARP 4761 Rev-Appendices	New Appendices for ARP 4761 Rev A	Other Developments
Functional Hazard Assessment	Aircraft Functional Hazard Assessment	Single Event Effects AIR 6218
Preliminary System Safety Assessment	Preliminary Aircraft Safety Assessment	
System Safety Assessment	System Functional Hazard Assessment	In-Service Safety Assessment ARP 5150/5151
	Aircraft Safety Assessment	
FTA, DD, FMEA, Markov	Cascading Effects Analysis	
Common Mode Analysis	Development Assurance Assignment	
Particular Risk Analysis	Model Based Safety Assessment	
Zonal Safety Analysis		
Contiguous Example	Contiguous Example	

ARP4761A Safety Assessment Process Interactions



ARP 4754A Development Assurance Processes

ARP4761 Relationship to ARP4754A Development Assurance

- Modern aircraft architecture is increasingly becoming a “system-of-systems”, where many systems interact with and are dependent upon each other to perform aircraft functional objectives.

- The era of having federated systems that can be correctly and completely assessed in silos, independent from other systems, is rapidly closing.

- The Challenge: Ensuring that a correct and complete safety assessment process is carried out in this environment.

- ARP 4761A has been designed to start at the highest functional level and capture the safety objectives that are necessary to meet these aircraft and system functional requirements.

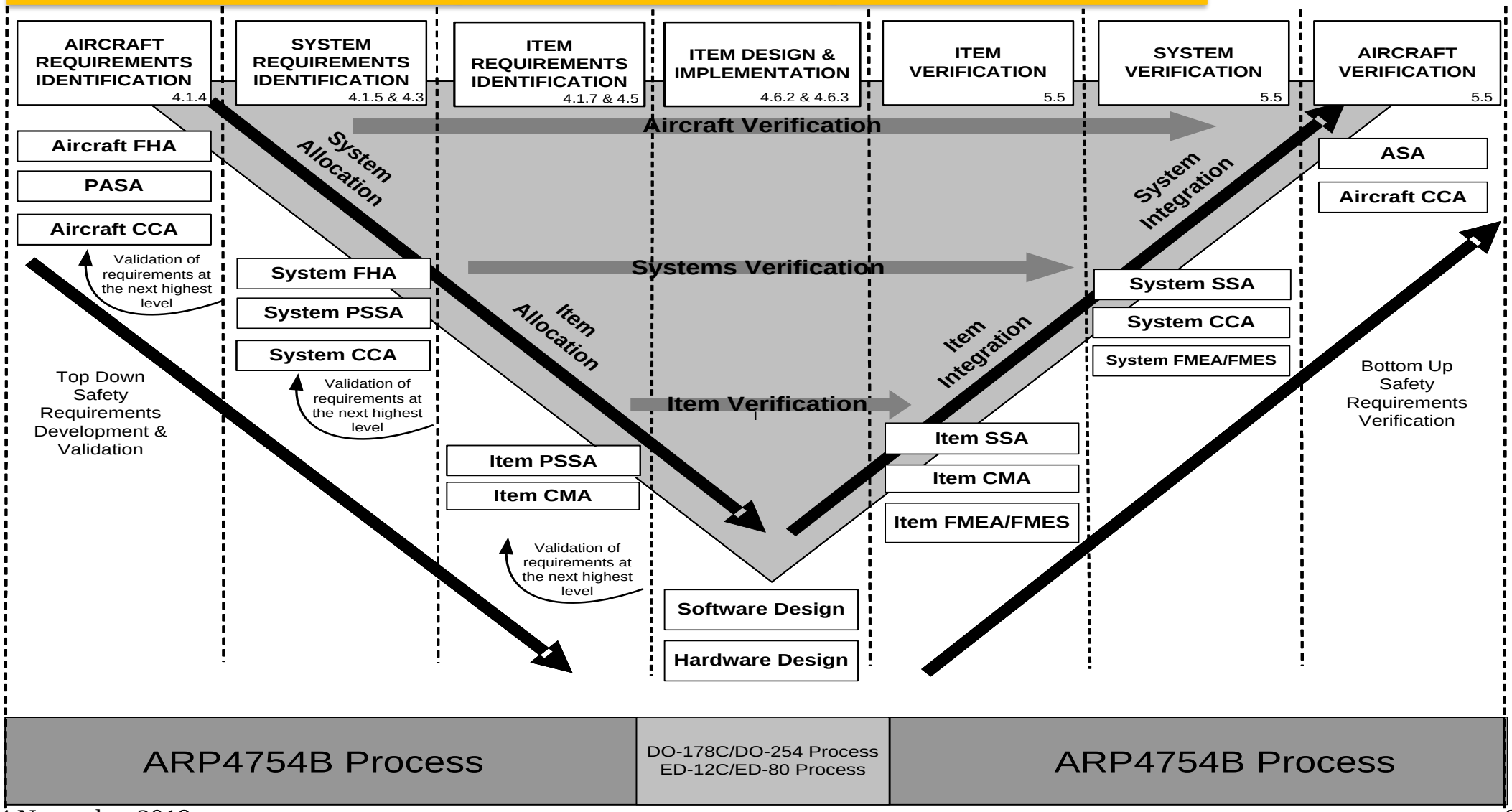
ARP4761 Relationship to ARP4754A Development Assurance

- The safety assessment processes of ARP 4761A are carried out at all stages of the design development process eventually producing derived safety requirements.

- These derived safety requirements can be both qualitative and quantitative in nature that feed into the systems development assurance processes of ARP 4754A.

- The ARP 4754A processes perform validation and verification of safety requirements in order to increase the confidence that errors have been minimized to the maximum extent practicable.

ARP4761 Relationship to ARP4754A Development Assurance



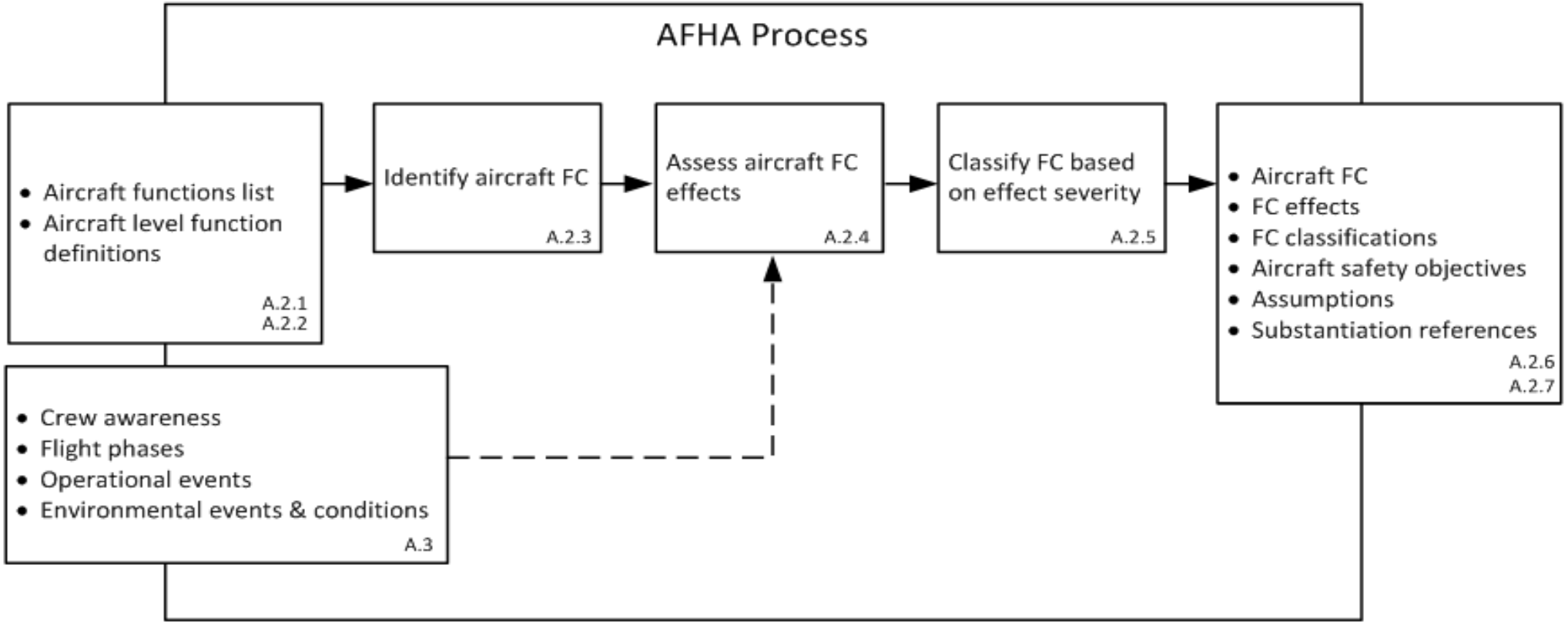
Aircraft Functional Hazard Assessment (AFHA)

- The Aircraft Functional Hazard Assessment (AFHA) is a top level process that allows the identification and evaluation of potential hazards related to an aircraft regardless of the details of its design.

- It is performed early in the development process and is used to establish the safety objectives for the functions of the aircraft to achieve a safe design.

- The AFHA process is a top down method for identifying aircraft-level functional failure conditions, how those functions can fail (i.e. loss or malfunction) and the severity of failure condition effects.

Aircraft Functional Hazard Assessment (AFHA)



Aircraft Functional Hazard Assessment (AFHA)

- The AFHA is not expected to significantly change as the development process proceeds since the aircraft level functions and decomposition do not depend on system architecture.
- Only assumptions found to be incorrect, changes to basic airframe definitions, introduction of new functions or high level operating parameters have the potential to invoke a revision of the AFHA.
- AFHA results are an input to the PASA.
- If the PASA identifies deficiencies in the analysis, or design deficiencies that cause aircraft functional information to be changed, this may result in an iteration of the AFHA.

Aircraft Functional Hazard Assessment (AFHA)

Completeness and correctness of the AFHA:

- All the aircraft level functions have been considered;
- All failure conditions have been identified for each aircraft function;
- The failure effects on the aircraft, crew and occupants are complete and correct for each failure condition occurring during each flight phase;
- The correct failure classification has been selected based on the failure effects; and
- The assumptions used to develop the assessment are confirmed and evidence is provided.

Preliminary Aircraft Safety Assessment (PASA)

- The PASA process, beginning during the initial aircraft architecture development phase, assesses a proposed aircraft architecture with the intent of identifying the need for aircraft level safety requirements.

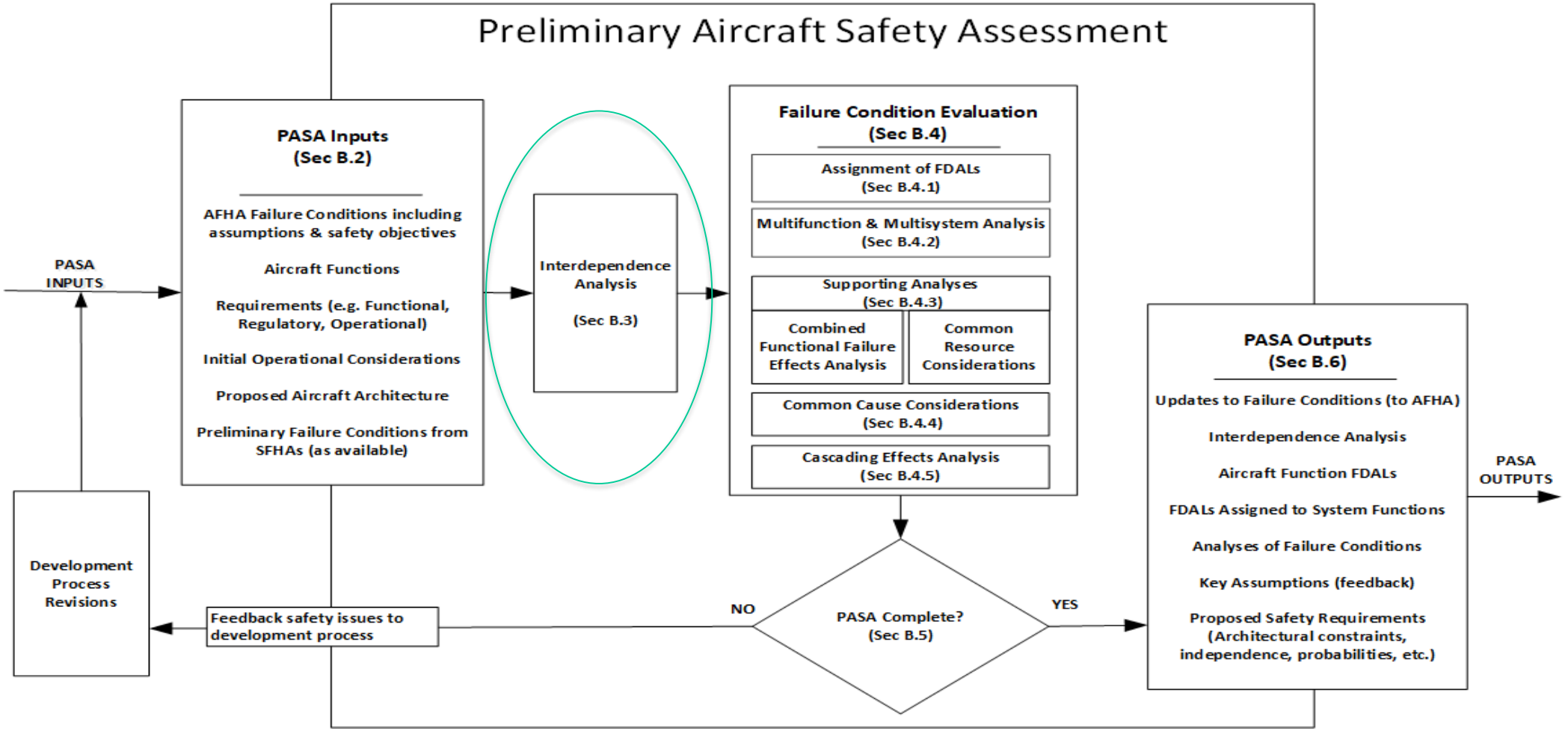
- The PASA is important when evaluating complex integration of aircraft systems that pose additional failure combinations that might not otherwise be present when aircraft functions are implemented by stand-alone systems.

- The PASA identifies the interactions and dependencies between the aircraft systems that together implement an aircraft-level function.

Preliminary Aircraft Safety Assessment (PASA)

- PASA assesses how these interactions can lead to the aircraft level failure conditions identified by the AFHA, and determines whether the safety objectives can be met.
    - Includes assessing the reliance on common resources, e.g. hydraulic power, electrical power, air data, air-ground logic, common computing and data networks.
- The main objectives of the PASA are to assess the aircraft architectures and develop safety requirements so that aircraft and individual systems development can proceed with reduced risk.

Preliminary Aircraft Safety Assessment (PASA)



Preliminary Aircraft Safety Assessment (PASA)

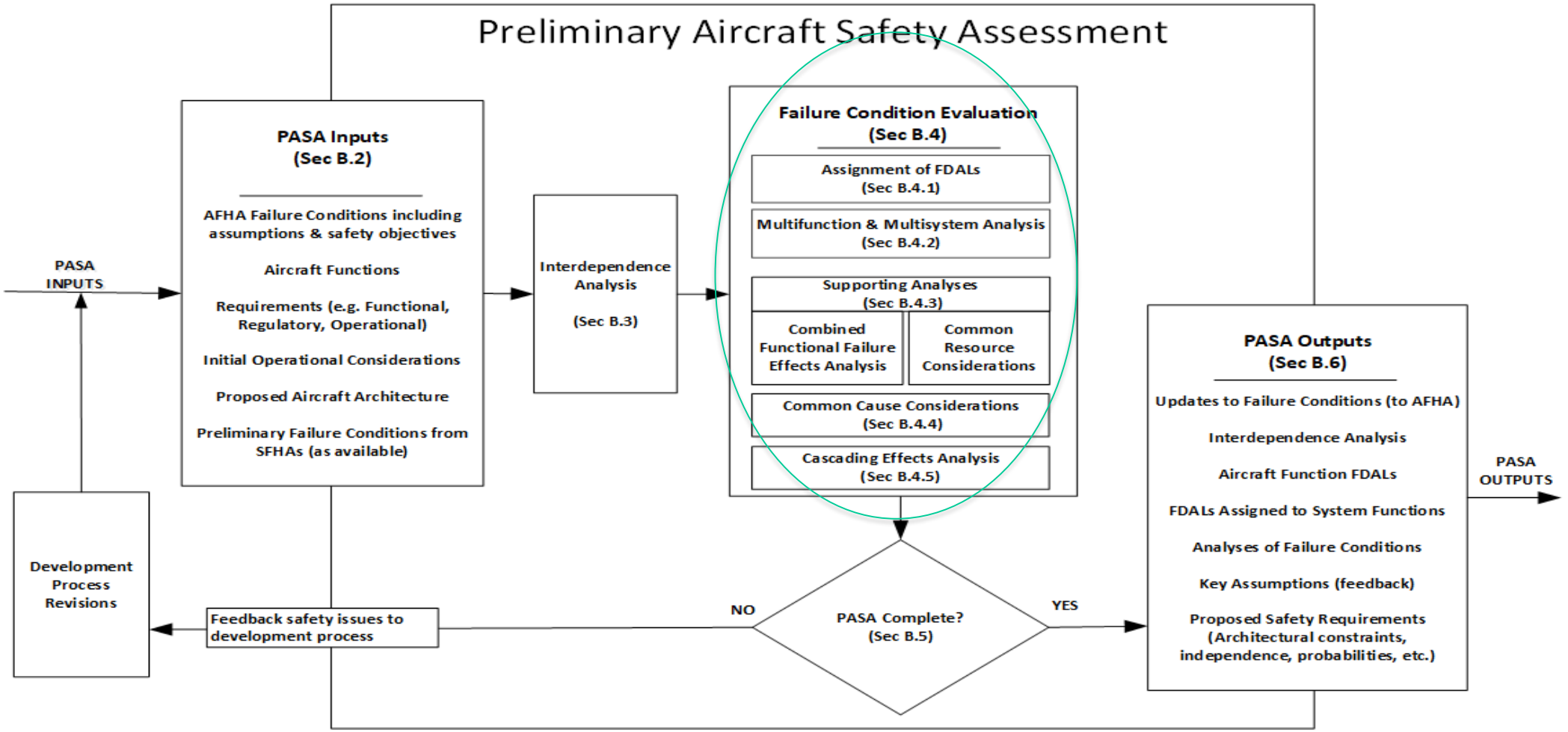
Interdependence analysis

- Provides visibility of the interactions between aircraft functions and systems.
- Used in the failure condition evaluation to identify the need for functional independence and separation.
- An interdependence analysis can be conducted by systematically following these process steps:
    1. Select an aircraft-level function and associated AFHA failure conditions to analyze,
    2. List all systems in the aircraft architecture (which may include resource systems),
    3. Identify which systems could contribute to that aircraft-level failure condition,
    4. Repeat above steps for each aircraft level function and associated AFHA failure condition.

Preliminary Aircraft Safety Assessment (PASA)

Aircraft Function	Aircraft Failure Cond #	Aircraft Failure Condition	System	Wheel Brake System				…	Flight Control System							Engine		…
			System Function /Implementation	Control normal brake	Control emergency brake	Provide anti-skid	Provide auto-brake	…	Control ailerons	Control spoilers	Control rudder	Control elevator	Control stabilizer	Control flaps	Control slats	Control Thrust Direction	Control Throttle	…
Decelerate aircraft on ground	3.2.3.L1	Inability to stop the aircraft within the available runway		X	X	X	X	…		X				X	X	X	X	…
Decelerate aircraft on ground	#	Inadvertent activation of deceleration function on the ground		X	X	…	X	…	…	X	…	…	…	…	…	X		…

Preliminary Aircraft Safety Assessment (PASA)



Preliminary Aircraft Safety Assessment (PASA)

Failure Condition Evaluation

- From the Interdependence analysis, an assessment of these systems contributions to aircraft-level failure conditions is carried out.
- Introduces the concept of an aircraft-level, fault tree for each aircraft-level failure condition to help understand interactions and relationships of systems.
- Derives safety and design requirements for the various systems in order to establish that aircraft level system architecture can reasonably be expected to meet the aircraft level safety requirements.

Preliminary Aircraft Safety Assessment (PASA)

Multifunction & Multisystem Analysis (MF&MS)

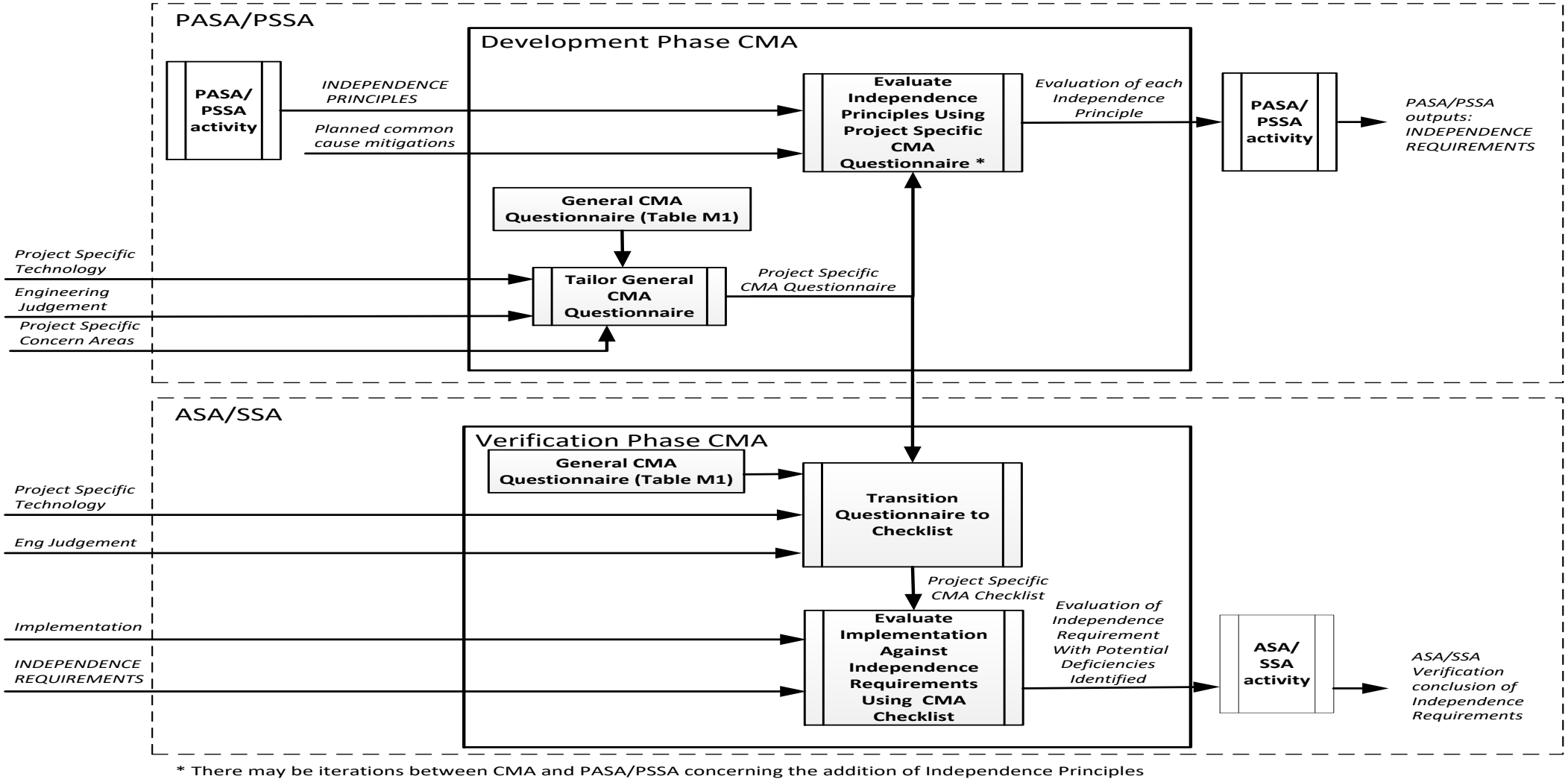
- Performed against the proposed aircraft architecture to understand the systems that contribute to an aircraft-level failure condition and to derive safety requirements.
- Evaluate how system functional failures (including resource systems) combine to lead to the considered aircraft failure condition.
- Map combined failures (whether loss of function or a malfunction) of system functions to assess the impact on the aircraft and model branches into an aircraft-level Fault Tree.
- Where an aircraft level failure condition may be caused by any one of a number of systems (a top level OR gate in the fault tree), then failure conditions are analyzed in the SFHA/PSSA level within each system.

Preliminary Aircraft Safety Assessment (PASA)

Supporting Analyses:

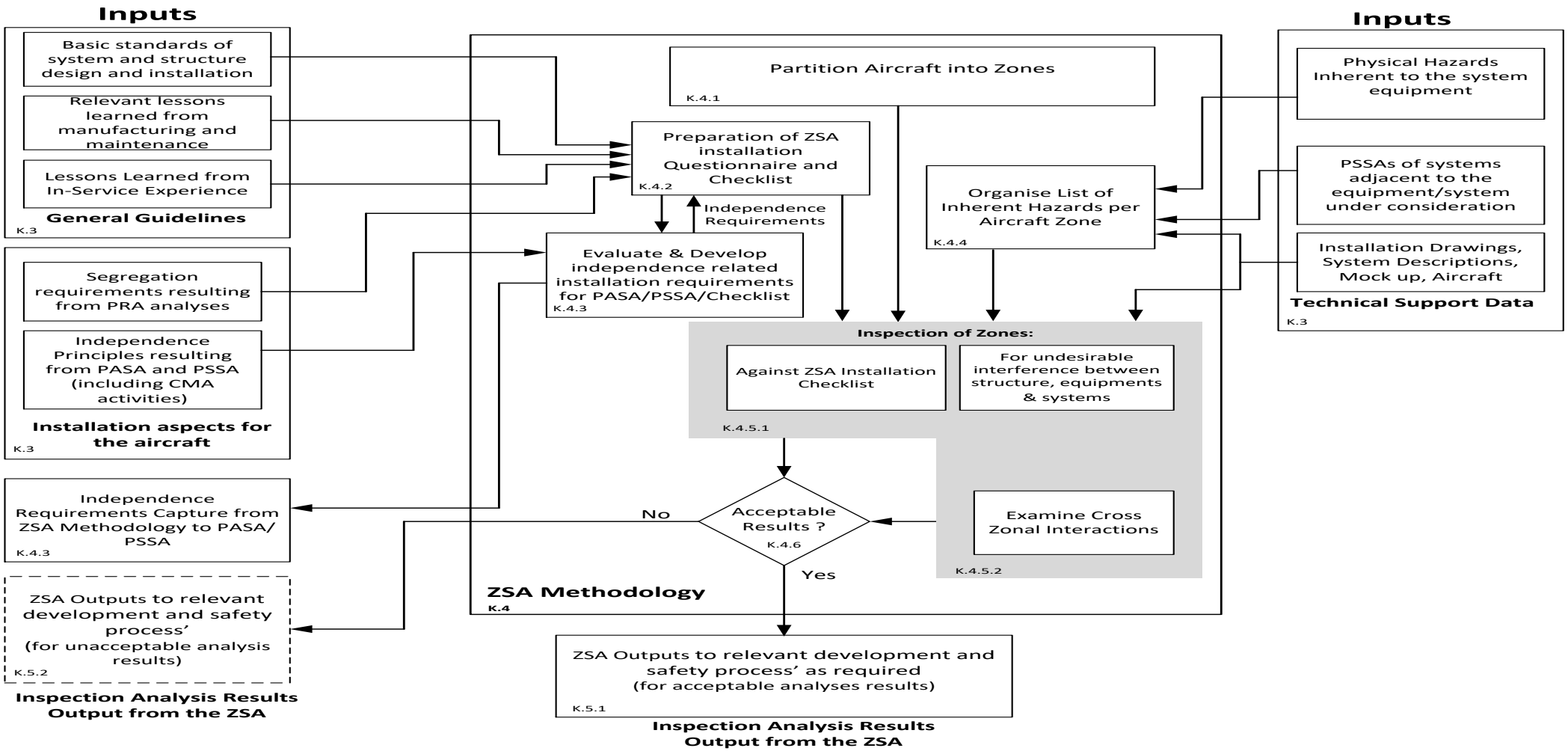
- Gathers pertinent systems failure modes that contribute to the top-level failure conditions when conducting the multi-function/multi-system safety assessments and aids the completeness of the assignment of FDALs.
    - Combined Functional Failure Effects Analyses (COFFE)
        - Help develop branches in the fault tree
    - Common Cause Considerations
        - Identification of functional & physical independence requirements,
        - Common Mode Analysis (CMA),
        - Zonal Safety Analysis (ZSA),
        - Particular Risk Analysis(PRA).

Common Mode Analysis (CMA)



* There may be iterations between CMA and PASA/PSSA concerning the addition of Independence Principles

Zonal safety Analysis (ZSA)



Preliminary Aircraft Safety Assessment (PASA)

Supporting Analyses:

- Common Resource Considerations
  - Systems that provide the resources (e.g. electrical, hydraulic) are potential common causes to be evaluated against the independence principles.
    - How could the use of common resources violate independence of systems contributing to aircraft-level failure condition, and
    - Are interactions across the aircraft-level functions considered in the SFHAs of common resource systems?

Cascading Effects Analysis (CEA)

Supporting Analyses:

Cascading Effects Analysis (CEA)

- Useful for understanding the behaviors of highly integrated aircraft and system architectures.
- Examines the connections between the systems and evaluates the effects resulting from the propagation of a single failure or a combination of failures.
- Qualitative bottom-up method which evaluates a failure condition, failure mode, or combination of failure modes and determines its total effect on the aircraft.
- The CEA analysis stops when the propagating effects stop.

Cascading Effects Analysis (CEA)

- Examples of possible CEA applications include:
  - Determining the effects of resource system failure conditions as part of the AFHA or SFHA
  - Determining the effects of resource system failure modes or combinations of resource system failure modes as part of the PASA
  - Determining the effects of shared or integrated component failure modes as part of the PSSA

Model Based Safety Assessment (MBSA)

- Process associated with performing a safety analysis using Failure Propagation Models (FPM) to achieve results that are consistent to those obtained from the classical (e.g. FTA) safety analysis methods.

- FPM which represents the system architecture and its dysfunctional behavior, is analyzed using a suitable computational tool set to generate Functional Failure Sets (FFS) and/or Minimal Cut Sets (MCS) for a specific failure condition.

- MBSA assesses failure effects via fault injection to visualize the effects of independent or common cause events which may be used to identify common cause potentials for events and common mode independence assumptions.

Assignment of Functional Development Assurance Levels (FDAL)

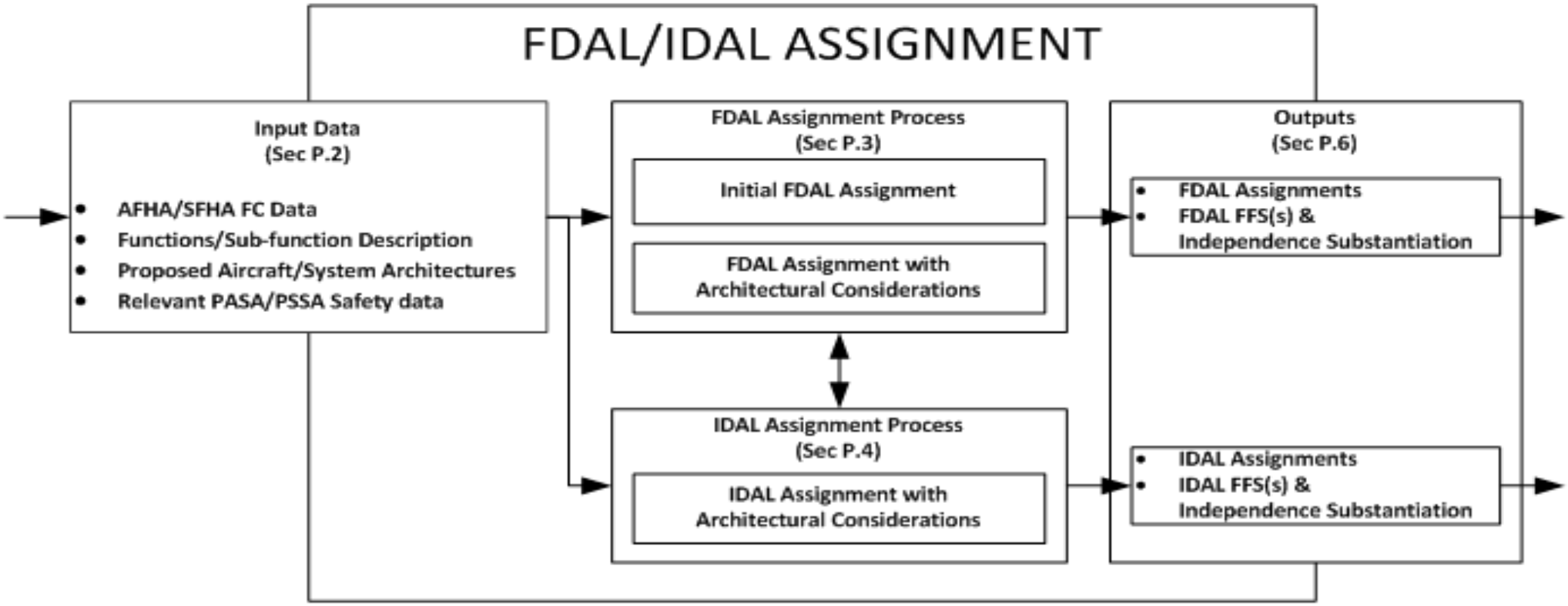
- Transferred from ARP 4754A to ARP 4761A, details the step-by-step process for assignment of FDALs (PASA only at this stage) for each aircraft level function and contributing system functions using the combined results of the previous assessments.

- For functional failures that can be allocated directly to one system, FDAL are assigned at the top-level failure condition; their subsystem functions and items within that system are assigned an FDAL and an item DAL (IDAL) which are covered in the PSSA.

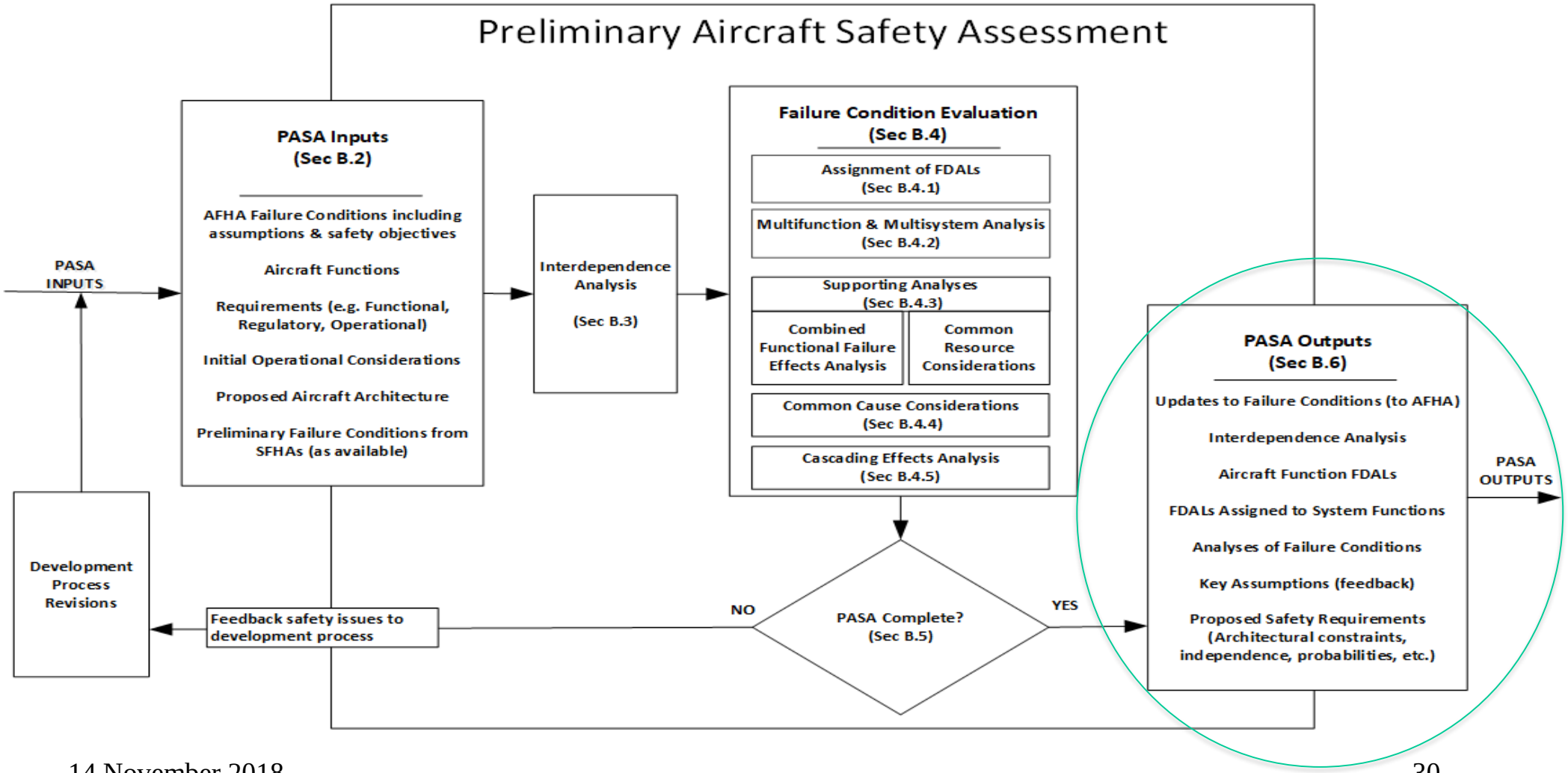
- The FDALs modulate the system development rigor (ARP4754A) while IDALs modulate the item development rigor for software (DO-178) and airborne electronic hardware (DO-254).

- Application of this process should be reconsidered each time any of the FHAs are revised, the aircraft/system architecture is modified, during the PSSA when all causes of the failure conditions need to be identified and reassessed, or changes to development assumptions.

Assignment of Functional DAL(FDAL)



Preliminary Aircraft Safety Assessment (PASA)



System Functional Hazard Assessment (SFHA)

- Aircraft-level functions are linked to system functions by the aircraft level architecture, AFHA/PASA and how these functions are allocated to the SFHA.
- AFHA is an aircraft level assessment conducted regardless of the details of its design.
- The System Functional Hazard Assessment (SFHA) is a system level process that identifies and evaluates potential hazards related to an aircraft system function regardless of the details of its implementation.
- Performed at the beginning of system development process, re-evaluated anytime significant changes are made to the aircraft system to determine the effects of failure conditions and their severity for:
  - Functions performed by the system,
  - Systems that contributed to the function under consideration, or
  - Other affected systems as a result of failures

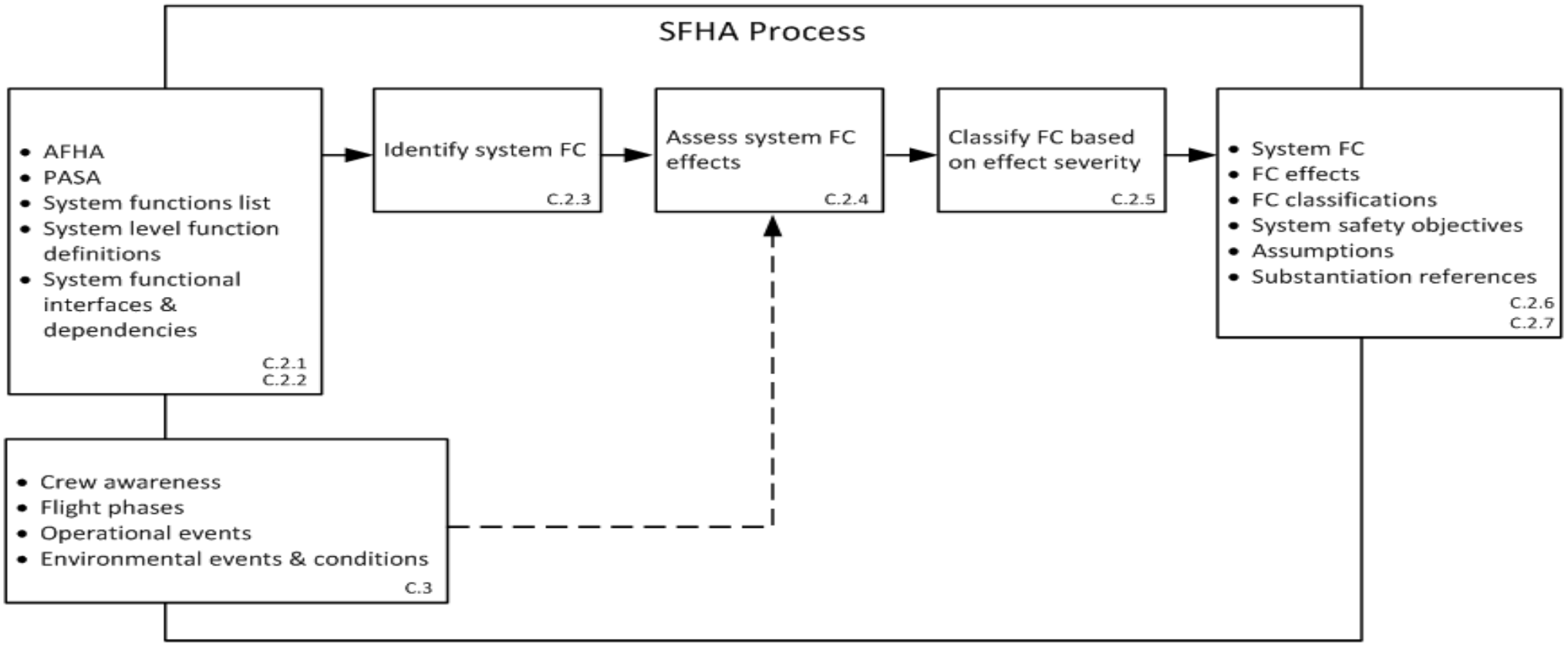
System Functional Hazard Assessment (SFHA)

- System Failure Conditions are analyzed for their effect on the aircraft, crew and occupants to determine the associated severity classification considering crew awareness, flight phase, environmental and operational conditions.

- The SFHA does not analyze potential causes (i.e. implementations) for system failure or specific failure modes of equipment.

    - For example, the effects of “loss of airspeed indication” are the same whether the design is mechanical, analog, or digital. The SFHA should not assume knowledge of the detailed design of the system, even if the proposed design is known at the time of SFHA development.

System Functional Hazard Assessment (SFHA)



Preliminary System Safety Assessment (PSSA)

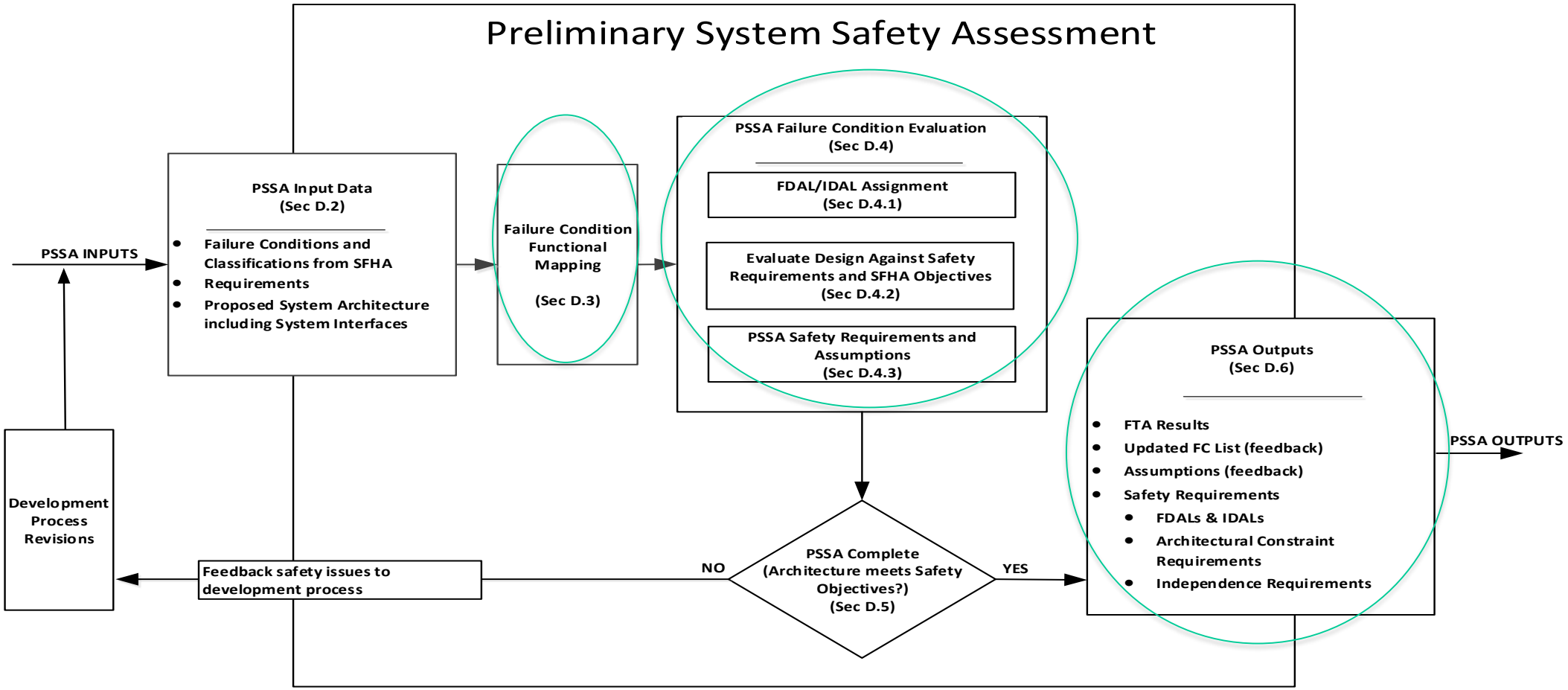
- The Preliminary System Safety Assessment (PSSA) process is a systematic examination of a proposed system architecture which evaluates the failure conditions and associated safety objectives identified by the SFHA and safety requirements allocated from the PASA.

- Assignment of FDALs for each system-level and contributing system (including resource systems) functions is undertaken.

- Safety requirements for the system, sub-system, and items are generated to guide the architecture development as necessary to meet the safety objectives and requirements (i.e. this is where the design implementation gets assessed).

- Iterative process of reassessment throughout the development cycle where safety requirements are passed on to the requirements management processes (e.g. V&V).

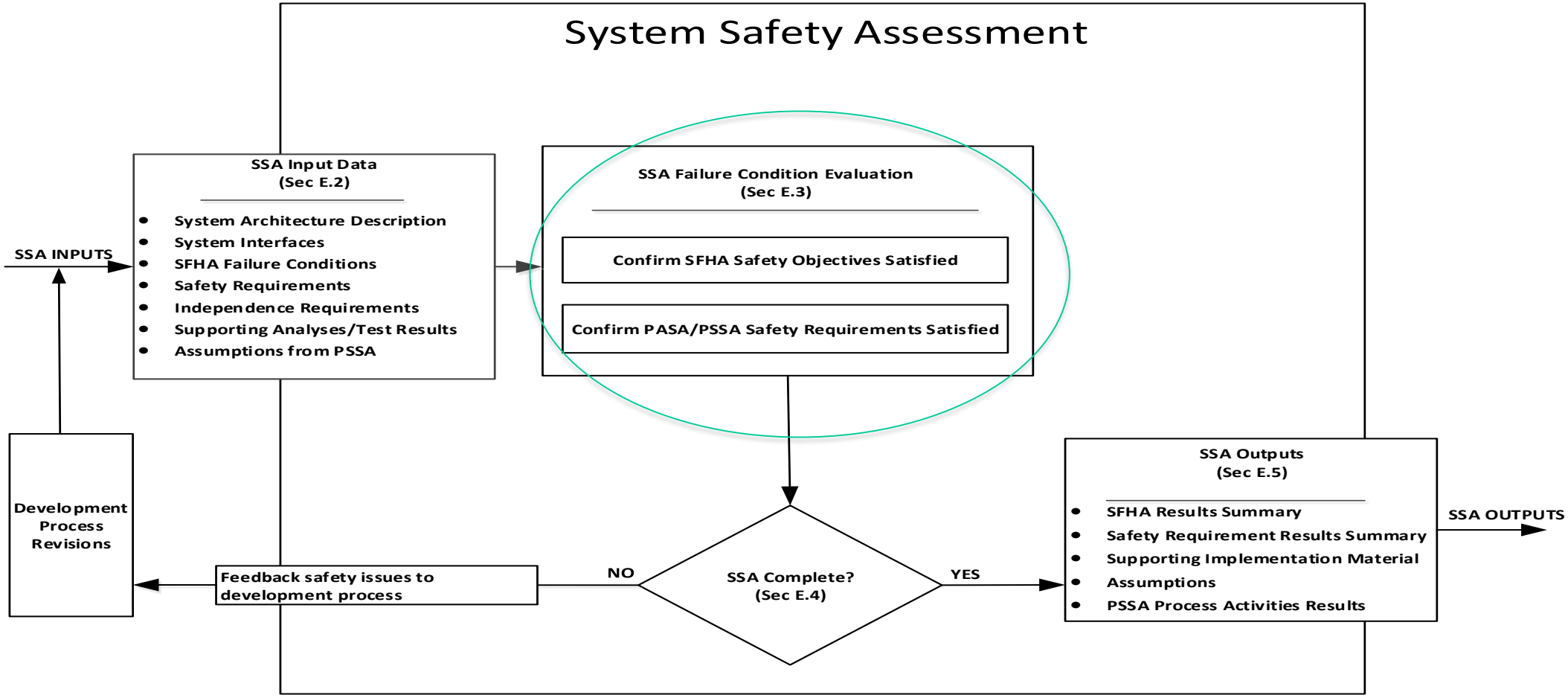
Preliminary System Safety Assessment (PSSA)



System Safety Assessment (SSA)

- The System Safety Assessment (SSA) is a systematic examination of a system, its architecture and its installation to demonstrate that the implemented system meets its safety requirements and safety objectives from:
  - Failure conditions and classifications defined in the SFHA.
  - Objectives and assumptions associated with the safety requirements from the PSSA.
- The SSA process may include the application of the analysis methods at more than one level of abstraction (system, sub-system, equipment or part of equipment) or by more than one organization (e.g., aircraft OEM, system supplier).
- The various levels of SSA support a single analysis performed on a system.

System Safety Assessment (SSA)



Aircraft Safety Assessment (ASA)

- The ASA is a systematic, comprehensive evaluation of the aircraft implementation to show that the failure conditions identified in the AFHA have been addressed and that corresponding safety requirements have been met.
- The ASA process results in confirmation that the interactions of system functions, their interdependencies, independence, separation and their contribution to associated failure conditions have been appropriately identified and assessed.
- The ASA does not replace the SSAs for showing that failure conditions identified in the system level FHA have been addressed and that system-level safety requirements are met.
- The ASA is intended to be performed when the aircraft architecture is mature.

Aircraft Safety Assessment (ASA)

- Initial ASA evaluation should confirm which AFHA failure conditions are satisfied by analysis conducted for a single system in its SSA or identify if further analysis is needed at the aircraft level in the ASA.

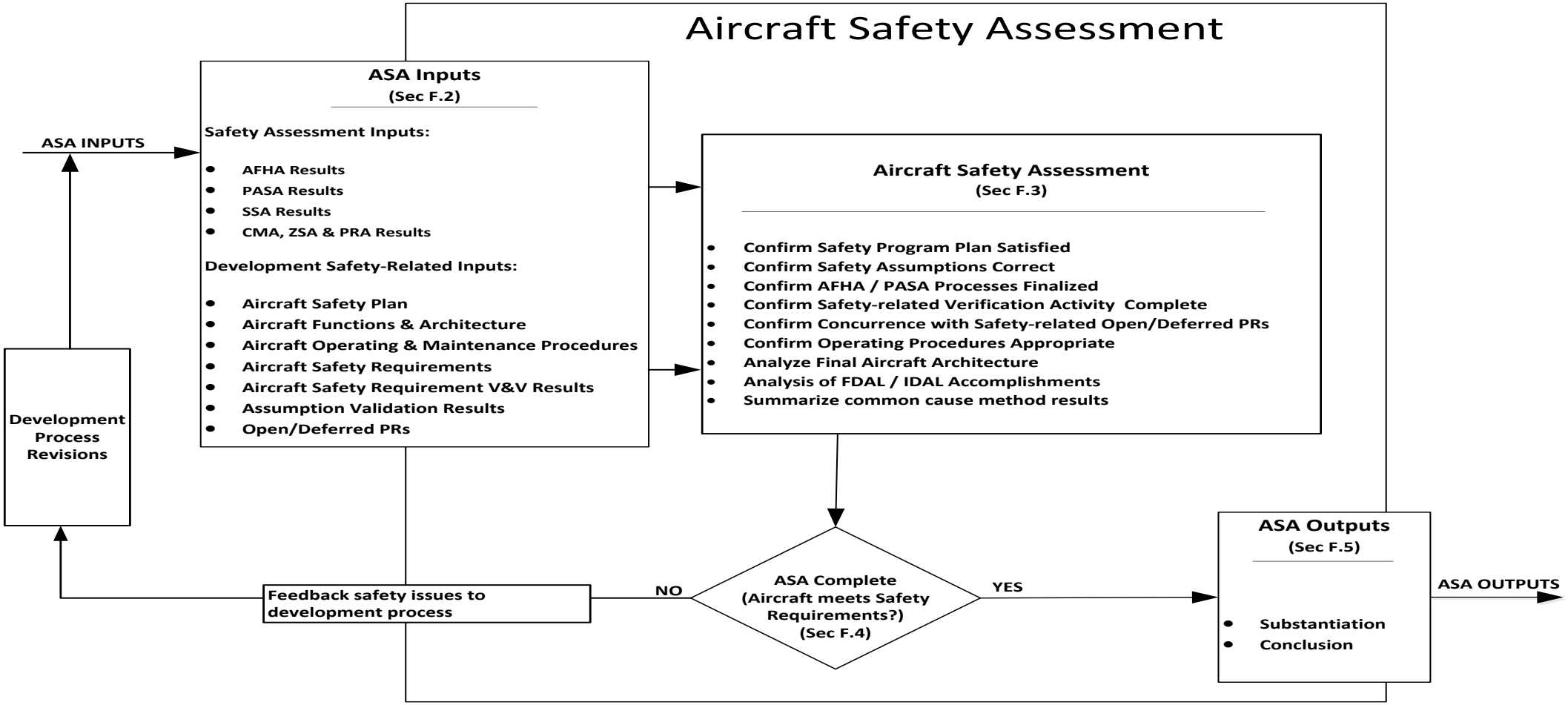
- Once any further aircraft level analysis in the ASA is complete, the ASA should re-evaluate the AFHA failure conditions with the complete set of analyses to ensure these failure conditions and their associated safety requirements have been adequately satisfied.

Aircraft Safety Assessment (ASA)

Activities performed:

- Confirm the applicable aircraft safety requirements are valid and considered stable based on reviews of the aircraft development and safety data.
- Confirm that results from other analyses outside of the ASA (e.g. SSA, PRA) used to satisfy aircraft-level safety requirements are completed.
- Activities conducted within the ASA which are an extension from the PASA to show the aircraft-level safety requirements are satisfied.

Aircraft Safety Assessment (ASA)



Contiguous Example

- Describes in detail, a contiguous example of the safety assessment process for a function on a fictitious aircraft design.
- Commencing with an aircraft level function, the example goes from the development of the AFHA/PASA (top of the left hand “V”) to the SSA/ASA (top of the right hand “V”) and includes all the safety process/analysis methods in between for a single system.
- A function was chosen which has sufficient complexity to allow use of all the methodologies, yet was simple enough to present a clear picture of the flow through them. This function/system/item was analyzed using all the methods and tools described in this ARP document.
- The purpose of the example is to demonstrate how each method may be applied.

Atmospheric Neutron Single Event Effects (SEE) Analysis AIR6219

- Atmospheric radiation is comprised mainly of high energy neutrons that can interact with a semiconductor device's silicon structure causing adverse behavior.
- High energy neutrons have been shown to be mainly responsible for causing single event upsets (SEUs) in memories and other devices in aircraft since the early 1990s.
- The purpose of the SEE analysis method outlined in AIR 6218 is to evaluate the electronic circuits utilized in a particular design for their sensitivity and response to neutron radiation.
- This sensitivity and response information are used during all development phases to evaluate SEE impact on safety requirements and may also be used for integrity and availability requirements.

Atmospheric Neutron Single Event Effects (SEE) Analysis AIR6219

- Targeted equipment(s) are any self-contained assembly composed of one or several hardware and software items that perform a distinctive function necessary to the operation of the system.
- Basically the electronic boxes typically found in the aircrafts electronics bay that can be swapped out quickly.
- AIR 6218 describes a method to assess the potential effects of atmospheric radiation at the equipment level as an aspect of the overall system safety assessment process via:
  - Identifying sensitive devices.
  - Identifying mitigations and equipment effects for each component.
  - If necessary, testing is performed (e.g. Los Alamos) or design decisions are made.

Atmospheric Neutron Single Event Effects (SEE) Analysis AIR6219

Single Event Effect	Device/Function Response
Single Event Upset	Change in state in memory or latch
Multiple Bit Upset	Upset to more than one bit in same logical word
Single Event Latch-up	Loss of gate, function or control due to high current induced state with possible damage
Single Event Transient	Spurious signals/transients that may affect circuits if not properly filtered in design
More.. (IEC62396 for listing)…	

In-Service Safety Assessment (ARP 5150/5151)

ARP 5150 Transport Airplanes & ARP 5151 General Aviation Airplanes and Rotorcraft

- Guidelines, methods and tools used to perform the ongoing safety assessment process for transport airplanes in commercial service.

- Provides a systematic process of industry best practices to measure and monitor safety to help determine priorities and focus available resources in areas that offer the greatest potential to improve aviation safety.

- A robust Safety Management System (SMS) is introduced that will help ensure risks are identified and properly eliminated or controlled. There are many sections within ARP5150A that can help satisfy the requirements of SMS, including its Safety Risk Management (SRM) and Safety Assurance (SA) elements.

In Conclusion

- ARP 4761A is intended to document industry best safety practices
- Once published, Revision A of the document will be implemented on new designs and changed products as necessary.
- Revision A will get reaffirmed in 5 years time and be reviewed in 10 years to determine if changes are required.
- Reality is that to cope with ever increasingly complexity of designs and high degrees of systems integration, Revision A will be the Industry Standard Practice for at least the next 20 years.
- Be ready for it!

QUESTIONS

??

Jim.marko@tc.gc.ca

613-773-8295