Functional Safety Management (FSM) for Complex Engineered Systems

Keynote Address: 2018 Mech-Aero Conference
Atlanta, GA, November 7, 2018

Dr. Daniel P. Schrage
Professor and Director, Vertical Lift
Research Center of Excellence (VLRCOE)
School of AE, Georgia Tech

Keynote Outline

- Background on Instructor
- Keynote Rationale and Objectives
- Understanding the Evolution to Complex Engineered Systems
- Overview and History of Functional Safety Management
  - Brief Review of its Application in Different Domains
- Evolution of Functional Safety Management for Civil Aircraft and Systems to its Current and Future Global Application
  - Why its Application for Military Aircraft and UAS has been difficult
  - What needs to be done for Air Taxis and UAS programs
- Example Projects from AE636218 Safety By Design (SBD) and Flight Certification(SBD) and Go Fly Individual Flying Machines Prize Challenge

Background on Speaker: Dr. Daniel P. Schrage, Professor, Georgia Tech

- Education
  - BS Engineering, USMA, West Point, 1967
  - MS Aerospace Engineering, Georgia Tech, 1974
  - MA Business Administration, Webster U., 1975
  - DSc Mechanical & Aerospace Engineering, Washington U. (St.Louis, MO), 1978
- Military Experience (1967-1978)
  - Honest John Nuclear Missile Battery Commander, 1968-69, in Munich and Augsburg Germany during the 1968 Czech Crisis & REFORGER 1
  - Army Aviator, Commander and S-3, 13th CAB,1970-71, Mekong Delta, South Vietnam, participated in Cambodia Invasion & Helicopter Vietnamization
  - Vibration & Dynamics Engineer, UTTAS & AAH SSEB Technical Evaluator for Vibration & Dynamics, Aviation Systems Command (AVSCOM1974-1978
- Civil Service Experience (1978-1984)
  - Structures & Aeromechanics Division Chief, Development & Qualification Directorate, AVRADCOM (St.Louis, Mo), 1978-82; Also, Technical Area Chief for AHIP (OH-58D) SSEB, Army Aviation's first integrated cockpit, 1978-1979; Structures & Aeromechanics Lead for CH-47D Chinook Modernization Program; Director for Advanced Systems, AVRADCOM, 1982-84; Also, **led successful LHX Concept Formulation transition to RAH-66 Comanche; s**upported JVX Tech Assessment
  - Associate Tech Director for S&T, AVRADCOM, 1982-84; Also, served as acting Chief Scientist, Combined Arms Center, Ft. Leavenworth, KS (1983-six months)
- Academia and Advisement to Industry and Government Experiences (1984-Present)
  - Professor, School of AE, Georgia Tech, 1984-Present; Also Red Team Technical Chief for Industry LHX Designs and other aviation programs
  - Director, Rotorcraft Center of Excellence(RCOE), 1986-Present; Also, Army Science Board (2), Air Force Studies Board, NASA Structures & Material Committee, FAA Safety Advisory Committee and Certification Process Study, National Research Council Studies on Review of NASA HSR Program; and Advanced Engineering Environments; NASA Space Shuttle Return to Flight Safety Assessment Study
  - Established **Georgia Tech Graduate Program in Aerospace Systems Design in early 1990s based on the need for Quality and Systems Engineering implementation through Integrated Product and Process Development (IPPD)** – Now the largest Aerospace Systems Design &Systems Engineering program in the world: participated in MIT led Lean Aircraft Initiative (LAI), 1992-95. **Co-PI on DARPA SEC for Intelligent UAVs & Heliplane Programs**, 2000-2010
  - Developed several major programs and laboratories at Georgia Tech: Aerospace Systems Design Laboratory (ASDL), 1992; Flight Simulation Laboratory (FSL), 1994; Unmanned Aerial Vehicle Research Facility (UAVRF), 1995; initiated Integrated Product Lifecycle Engineering (IPLE) Laboratory, 2007
  - Introduced Safety By Design and Flight Certification Course, School of AE, Georgia Tech, 1995-Present; based on civil & military certification experience.
  - Have developed and taught short courses around the world on Rotorcraft Design, Integrated Product and Process Development(IPPD) and Safety By Design .
  - Provided the IPPD Tradeoff Methodology for the Full Spectrum Team (FST) **Future Combat Systems (FCS) Concept Design & Systems Engineering (CDSE) Phase I. Provided the IPPD Near-Term Decision Support Methodology for the emerging DoD Future Vertical Lift (FVL) Program**
- Retired Senior Executive Servant(SES-Level 3) and COL (06) USAR

Rationale and Objectives for the Keynote

- Rationale
  - Complex systems such as civil and military inhabited and uninhabited aircraft systems have become (and are becoming even more so) cyber physical vehicle systems (CPVS)
  - Certification and airworthiness qualification, safety assessment, and system development need to be more tightly co-designed, integrated earlier and the roles and responsibilities of stakeholders and key players, e.g. aircraft integrator, system integrator and basic module developer, are changing and evolving
- Objectives
  - Brief Review of the history of Functional Safety Management (FSM) standards
  - Review the history of Quality and Risk Management and its relevance to FSM
  - Discuss the worldwide civil aircraft and systems development FSM guidelines with ARP4754A and ARP 4761 as the current aircraft centerpiece guidance documents
  - Examples for Uber Elevate Air Taxis, GoFly Individual Flying Machines, and University Rocket Launch Space Challenge

Brief Overview and History of Functional Safety Management Methods

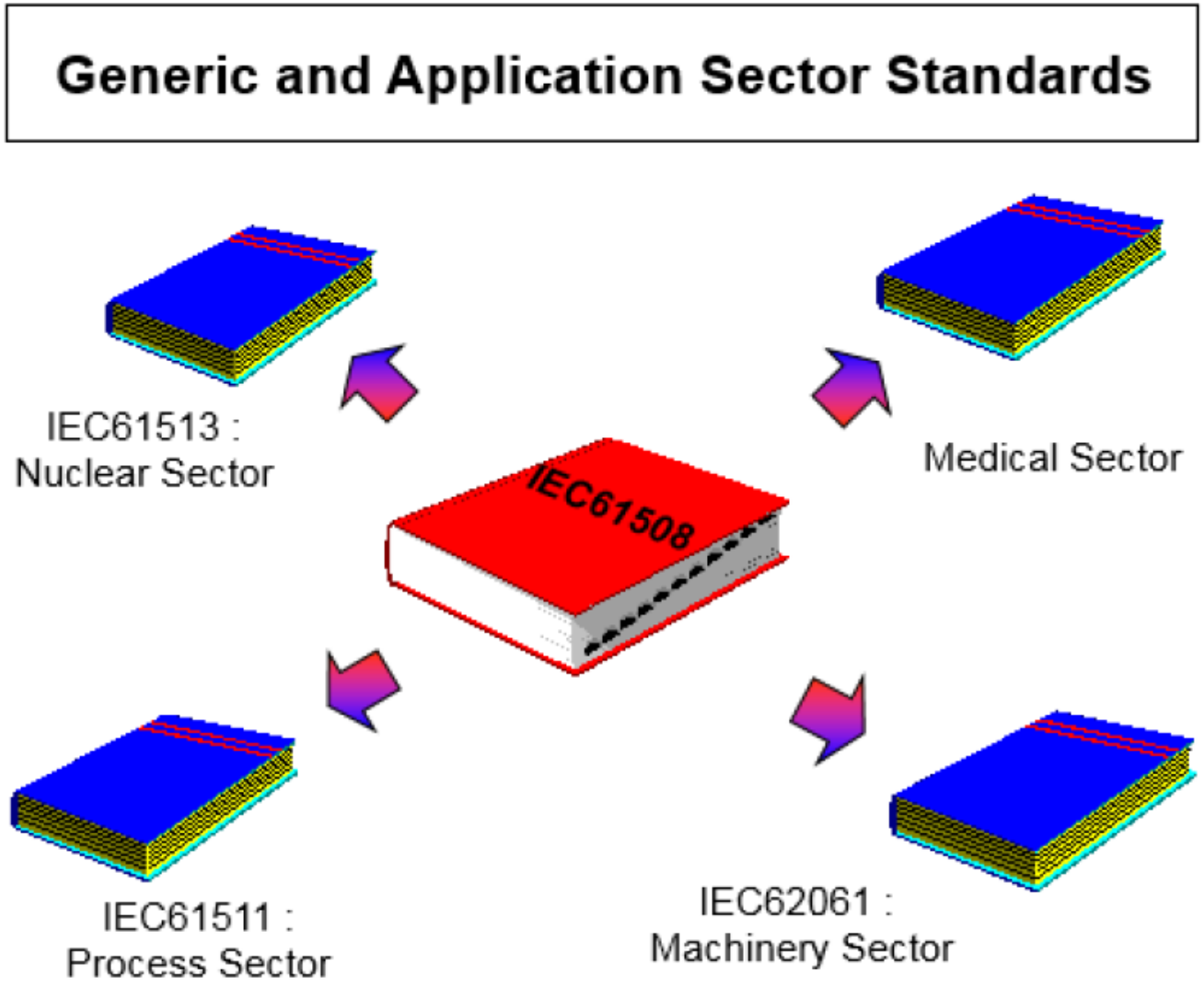
(Functional Safety Management: As Easy As Safety Integrity Level (SIL) 1, 2, 3)

- **Functional safety** seems to have been **shrouded in mystery for many years** – even the term itself is mysterious. In this context functional safety **deals with the application of "safety instrumented systems" as part of a company's overall risk management strategy**.
- **The standards for functional safety are relatively new**. **IEC 61508 was first released in 1998 followed by IEC 61511 in 2003**. These standards are both very detailed and specific and yet they aim to establish generic frameworks that apply over a wide range of applications.
- Some of the language used seems to be ambiguous and difficult to interpret. **Users have found it challenging to interpret and to apply these standards**.
- The functional safety standards **deal with *managing the risk of both random failures and systematic failures***. It is relatively straightforward to apply the mathematics of probability to characterize **random failures**. It has been **significantly more difficult to manage the risk of systematic failures**. This is **primarily to do with how we apply engineering methods and techniques**.

Review of Functional Safety Methods

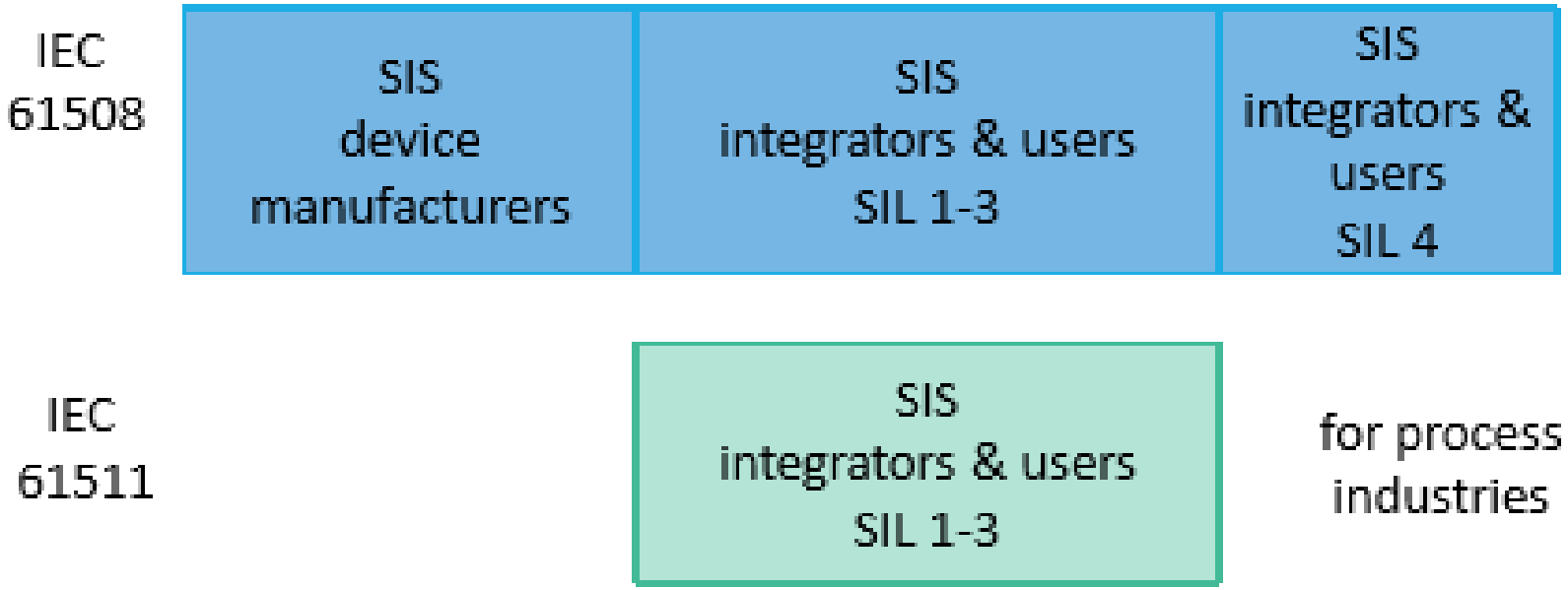
- **Functional safety** is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of *likely operator errors*, *hardware failures* and *environmental changes*.
- **Functional safety is intrinsically end-to-end in scope** in that it has to treat the function of a component or subsystem as *part of the function of the whole system*.
- **Early functional safety standards focused on Electrical, Electronic and Programmable Systems (E/E/PS),** the end-to-end scope meant that in practice functional safety methods have to extend to the non-E/E/PS parts of the system that the E/E/PS actuates, controls or monitors. *Functional safety is achieved when every specified safety function is carried out and the level of performance required of each safety function is met*.

Functional Safety Standards are in Many Sectors; Transition to Aviation, initially in DO-178B in 1990s



Functional Safety Management: As Easy As (SIL) 1, 2, 3

IEC 61508 or IEC 61511



Integrators & users in the process industries can use either IEC 61508 or IEC 61511

IEC 61511 is generally simpler to apply

Functional Safety Management interface with System Development Management (Fig 1, IEC 61508)

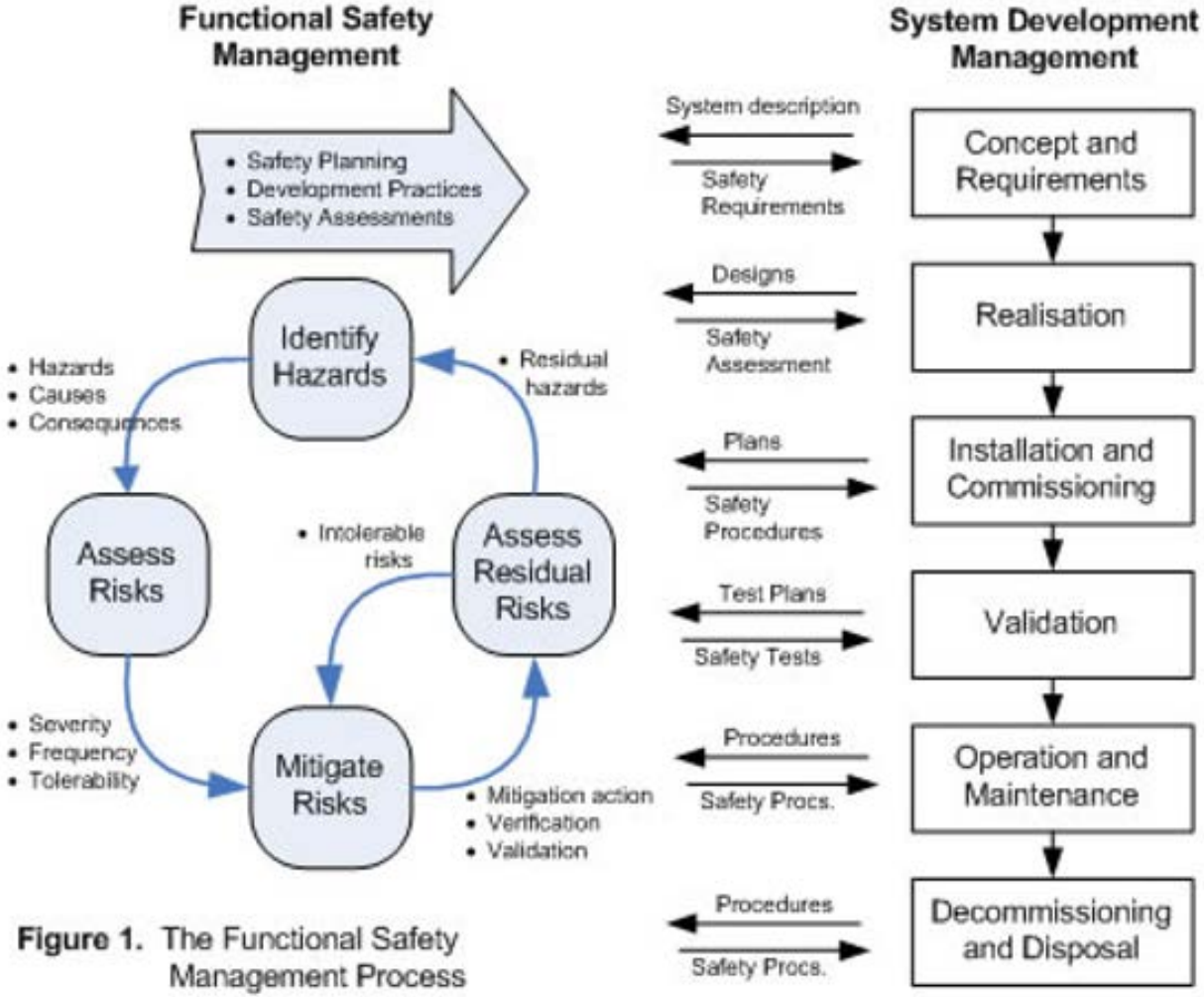


Figure 1. The Functional Safety Management Process

Functional Safety Management: As Easy As (SIL) 1, 2, 3

- Engineering companies and operations companies that apply functional safety **have struggled to reconcile their long established work practices with the relatively new standards**. At best compliance has been "partial".
- The good news is that it really is not that difficult to comply. There is nothing particularly new or onerous. **The principles are essentially the same as in *quality management and risk management***.
- The first step in achieving compliance is to **prepare and to implement a "Functional Safety Management Plan".**

Development of Quality and Risk Management

- **In the 1980s industry experienced similar difficulties in understanding and adopting quality management for lean manufacturing**. The ideas behind managing quality are quite abstract and **were embraced and articulated by the Japanese under the *Total Quality Management (TQM)* Umbrella** with the **need for implementing it through *Concurrent Engineering* for Just In Time and Lean Manufacturing. Similarly, the concepts of *Six Sigma* for risk management were introduced.**
- **Quality is primarily about understanding and satisfying a *customer's expectations***. This includes implicit expectations, as well as explicit expectations. The techniques of specification, inspection and testing **only make sense in a wider context** which also addresses ***Risk*** and ***Uncertainty***.
- **Formal risk management was developed in the late 1980s and throughout the 1990s**. Risk management principles are now widely understood and applied.
- **Functional safety management simply applies quality management to systems that are designed to control risk** through a ***Development Assurance (DA)* process**.

Development of Quality and Risk Management

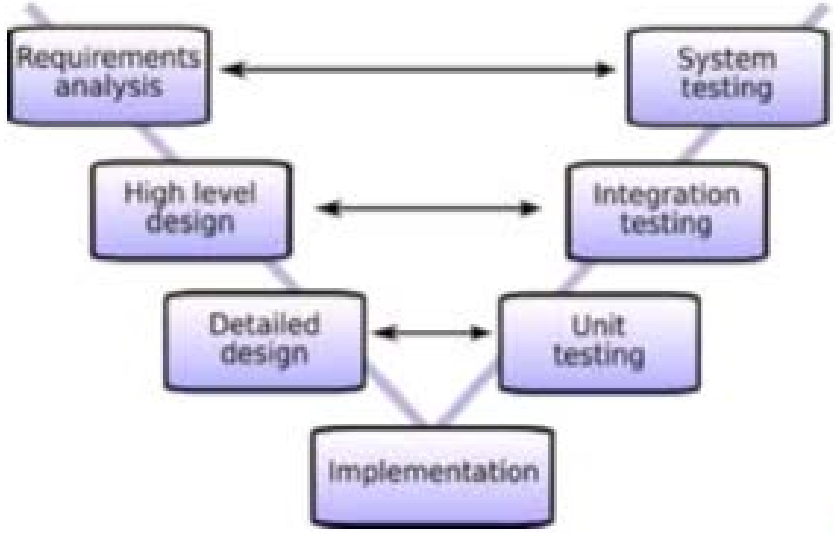
- **In the early days of quality management the focus seemed to be on "Quality Control" or "Quality Assurance".** Emphasis was placed on inspection and testing. Quality was about conformance to specification. Non-Conformance Reports were seen as representative of quality control.
- Our **understanding of quality management has evolved**. Quality management principles are now better understood and include the use Robust Design Techniques, such as Taguchi's Robust Design Simulation
- **Quality begins with executive management taking overall responsibility**, setting policies and implementing strategies.
- It requires taking a **Development Assurance** approach early in System Development vice a **Quality Assurance** approach later on, often too late

Development of Quality and Risk Management

- **Quality management principles** include:
  - Resource management (including competence, training and awareness)
  - Management of product realization
  - Measurement, analysis & improvement
  - Monitoring
  - Documentation
- Quality and Risk Management have evolved into the need for **Concurrent Engineering** (specifically **Integrated Product & Process Development**) and **Development Assurance**

Development of Quality and Risk Management

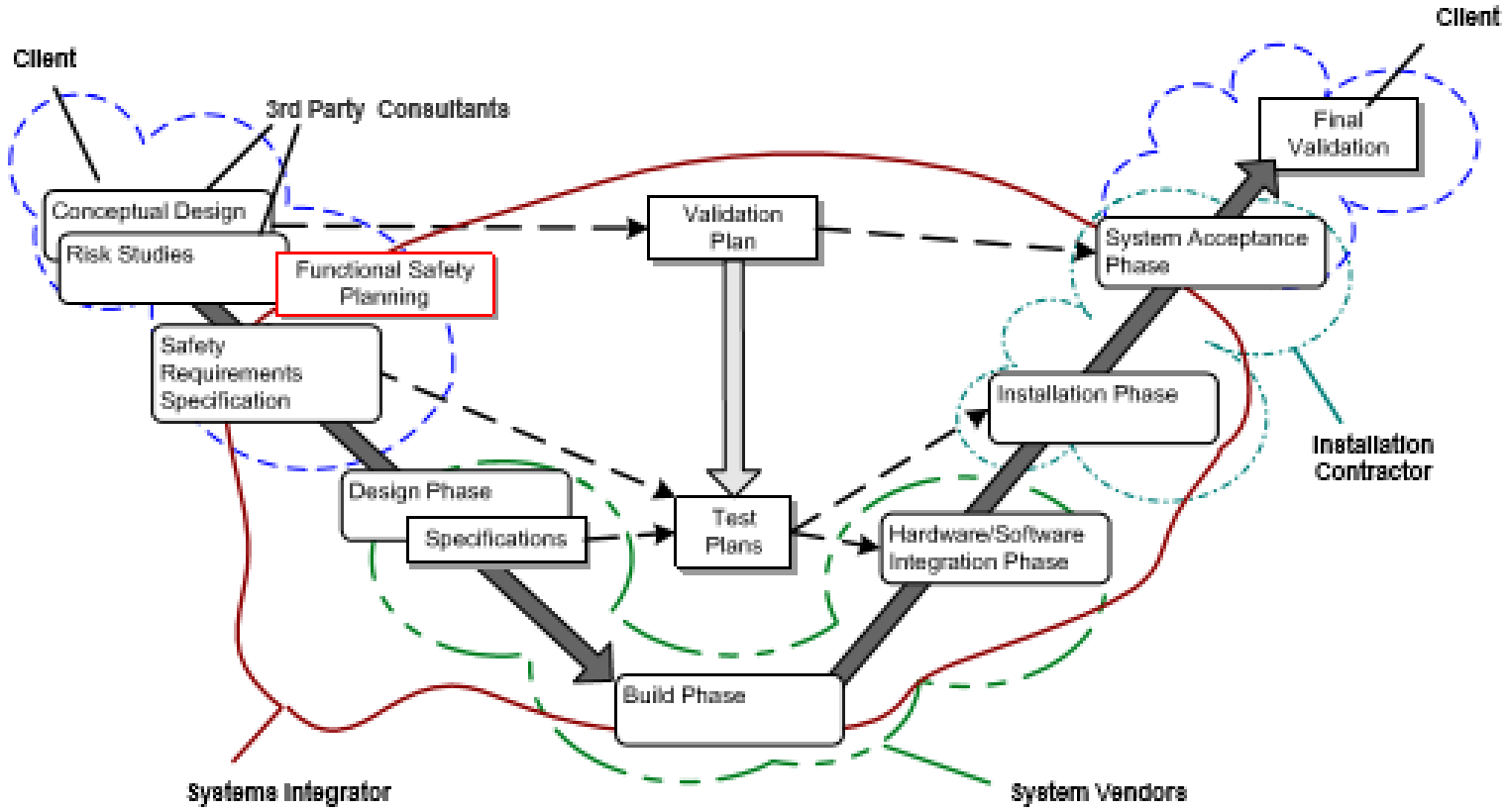
- **The core of quality management is in "Product Realization". It includes these main elements:**
  - Establishment & review of requirements
  - Design and development
    - inputs
    - outputs
    - review
    - verification
    - validation
  - Change control
  - Purchasing



- These same elements **form the core of functional safety management**.
- Functional safety management **can be seen as a specific application of quality management**

Development of Quality and Risk Management

- Functional safety management **follows the same classic systems engineering "V-model" which is central to quality management**:



Evolution of Functional Safety Management for Civil Aircraft and Systems to its Current Global Application

Dr. Daniel P. Schrage
Professor and Director, Vertical Lift
Research Center of Excellence (VLRCOE)
School of AE, Georgia Tech

Civil Aviation Functional Safety Management History

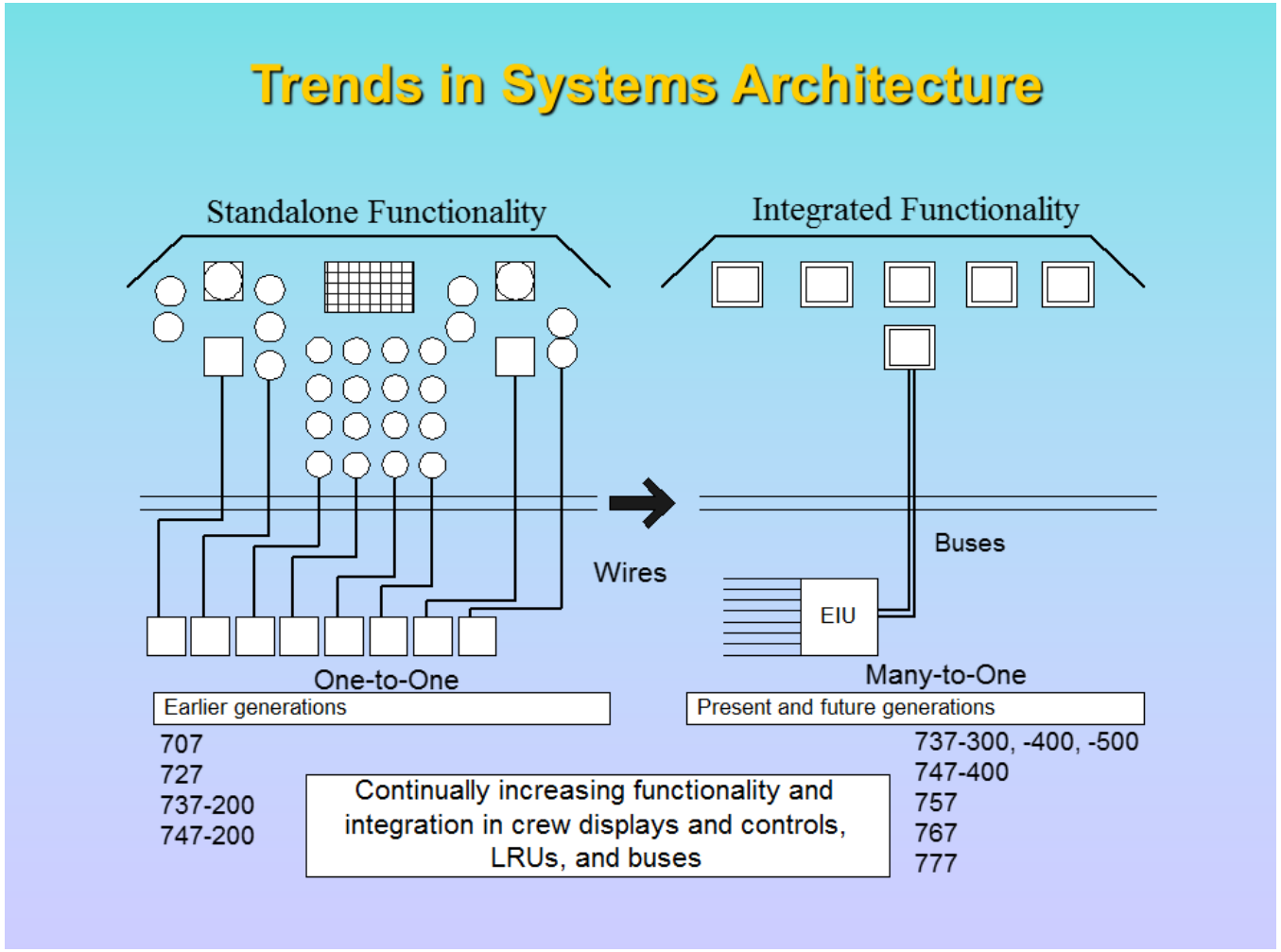
- **Started in the early 1990s with the development of DO-178A/B for *Software Development for Aviation Systems***; closely followed by the development of SAE ARP 4754 and ARP 4761 in the mid 1990s.
- The **Concept of Development Assurance Levels (DALs) was introduced**; somewhat as a parallel to the Safety Integrity Levels (SILs), as identified in IEC 61508 and IEC 61511. Both DO-178A/B and ARP 4754 use DALs, although with slight differences in definition and application.
- The **tight coupling of *Civil Aircraft and Systems Development*, AR4754, with ARP 4761**, *Safety Analysis Assessment Methods* has proven to be very beneficial for assessing Development Assurance with Safety Analysis and Risk Management. A contiguous example, S-18 Aircraft, in ARP 4761, is beneficial.
- Later, a new **Document Order (DO) 254 for *Electronic Hardware Development for Aviation Systems*** was developed and introduced.
- In the 2000s Boeing and Airbus moved from *federated to integrated, distributed avionics architectures* for new civil aircraft, such as the Boeing 777/787 and Airbus 380/350, which has required the **introduction of DO 297 for *Integrated Modular Avionics (IMA) for Civil Aircraft***
- In 2010 the U.S. and Europe issued a new ARP 4754A/ ED 79, which **brought together a common description of the DAL from the Aircraft Level**, down to IMA and Item levels, e.g. Electronic Hardware and Software.
- However, with the *continued acceleration of integrated software solutions for even more complex civil aircraft,* there is **work underway to update ARP 4754A and ARP 4761 to include a contiguous example between them and perhaps the DOs**; also there is work underway by the civil avionics/FBW/FBL community to include an update or new DO 297 to **include the need to address reconfiguration and shared functionality on multi-core processes**.

Aviation Functional Safety Management Guidance

- Aviation is among the safest industries in the world and it applies Functional safety in many areas, including for example the automated flight control system.
- The two-axis autopilot system controls the pitch and roll of the aircraft and controls heading and altitude, all of which are programmed to respect certain Functional safety parameters, activating alarms and other measures when they are breached
- Initial aviation functional safety management was documented in DO 178B, “Software Considerations in Airborne Systems and Equipment Certification”
- Initial aviation function safety management approach expanded to a set of interrelated DOs and ARPs accepted in US and Europe through consensus
- With the movement to full authority Fly By Wire (FBW) in modern civil and military aircraft avionics and flight controls are now being fully integrated into adaptive Air Vehicle Management (AVM) and Integrated Modular Avionics (IMA) systems.

Boeing View of Trends in Systems Architecture

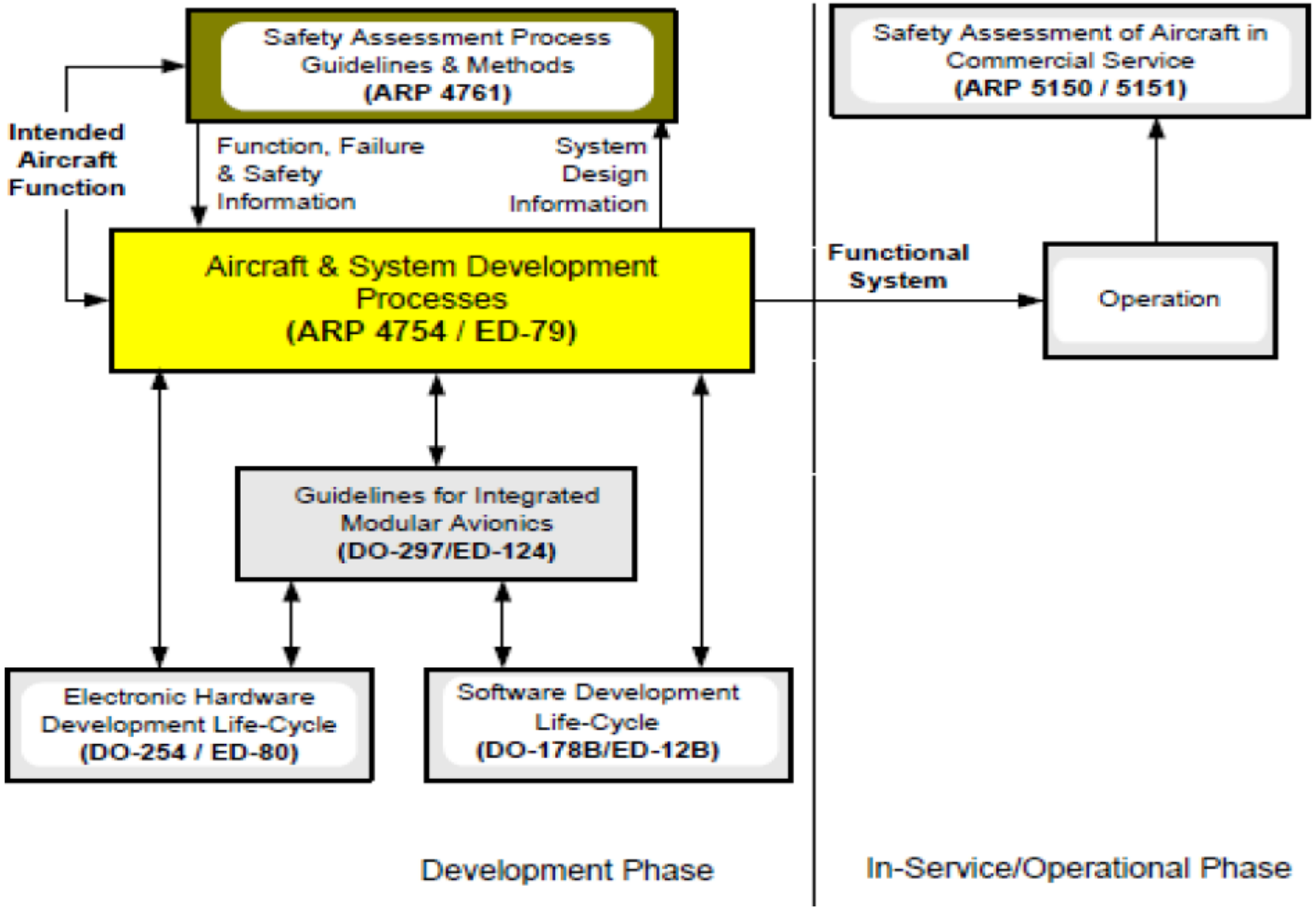
(John Dalton, Chair, SAE S-18 Committee, AEROTECH 2012)



Systems Evolution

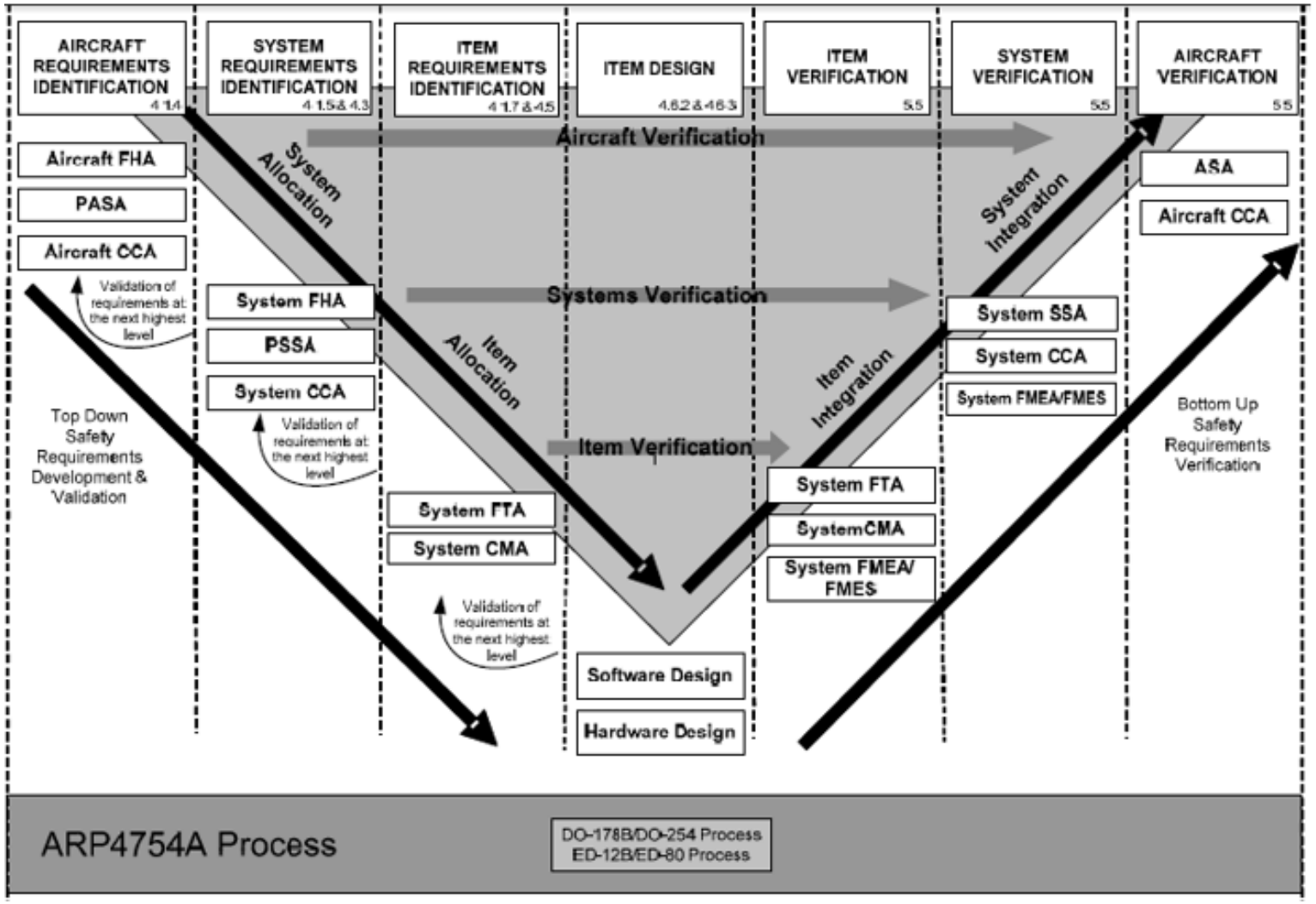
B707/B727	Little integration, brick wall system. Flight engineer for real-time systems integration
B737-100/-200	Simplified systems - brick wall, analog systems. 2-crew real-time systems integration
B757/B767	Digital systems, traditional architecture. Moderate integration in design
B777	Digital systems, new architecture. Interdependent systems, highly integrated design
B787	New materials, new architecture,

The 2010 Issuance of ARP 4754A/ED-79 provided a Global Functional Safety Standard, included component hardware, software and IMA for Aircraft Synthesis –Still an Evolving Process



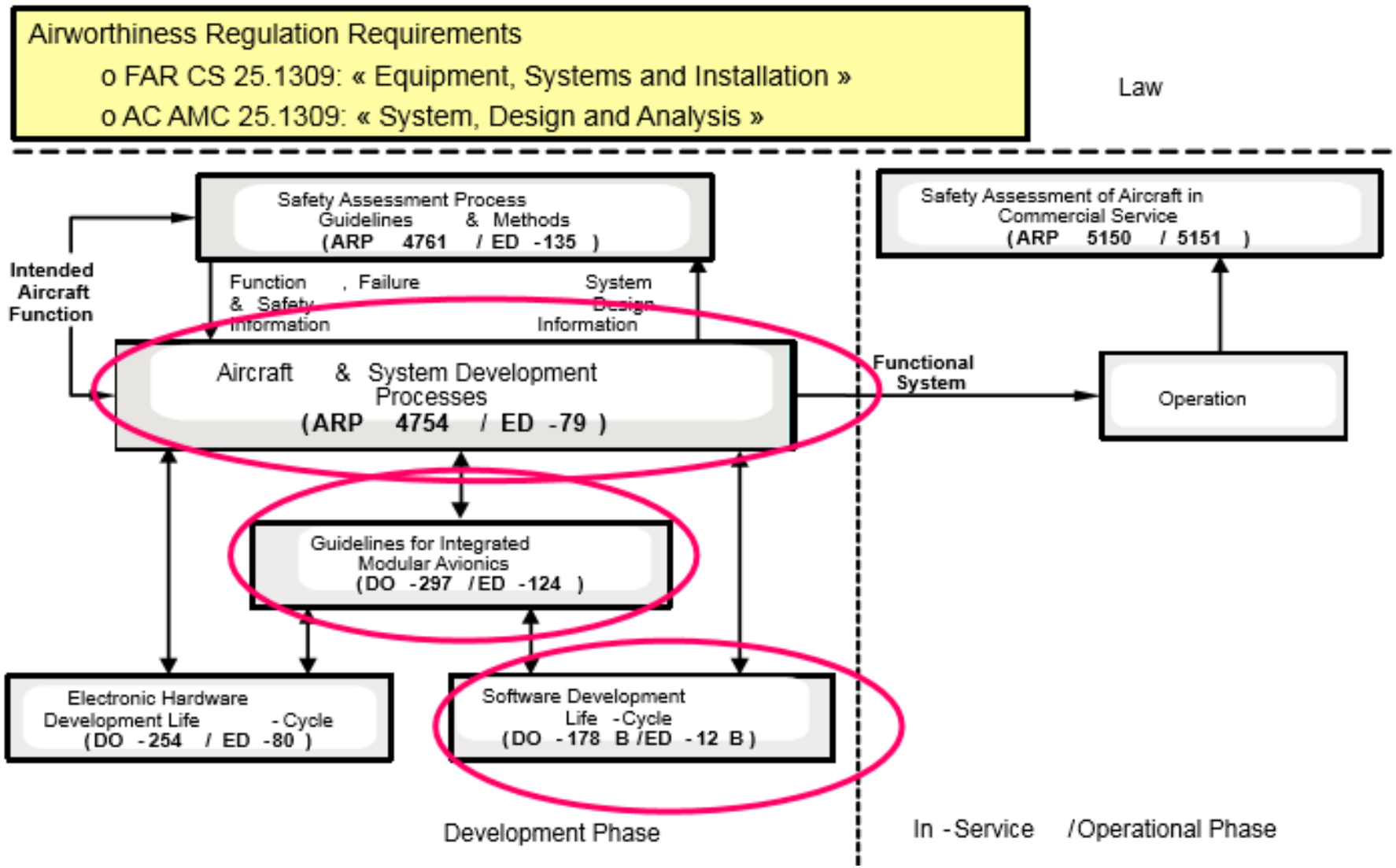
Civil Aviation has Moved from a QA to DA Approach
(SAE ARP 4754A, 2010)

DEVELOPMENT ASSURANCE (DA)



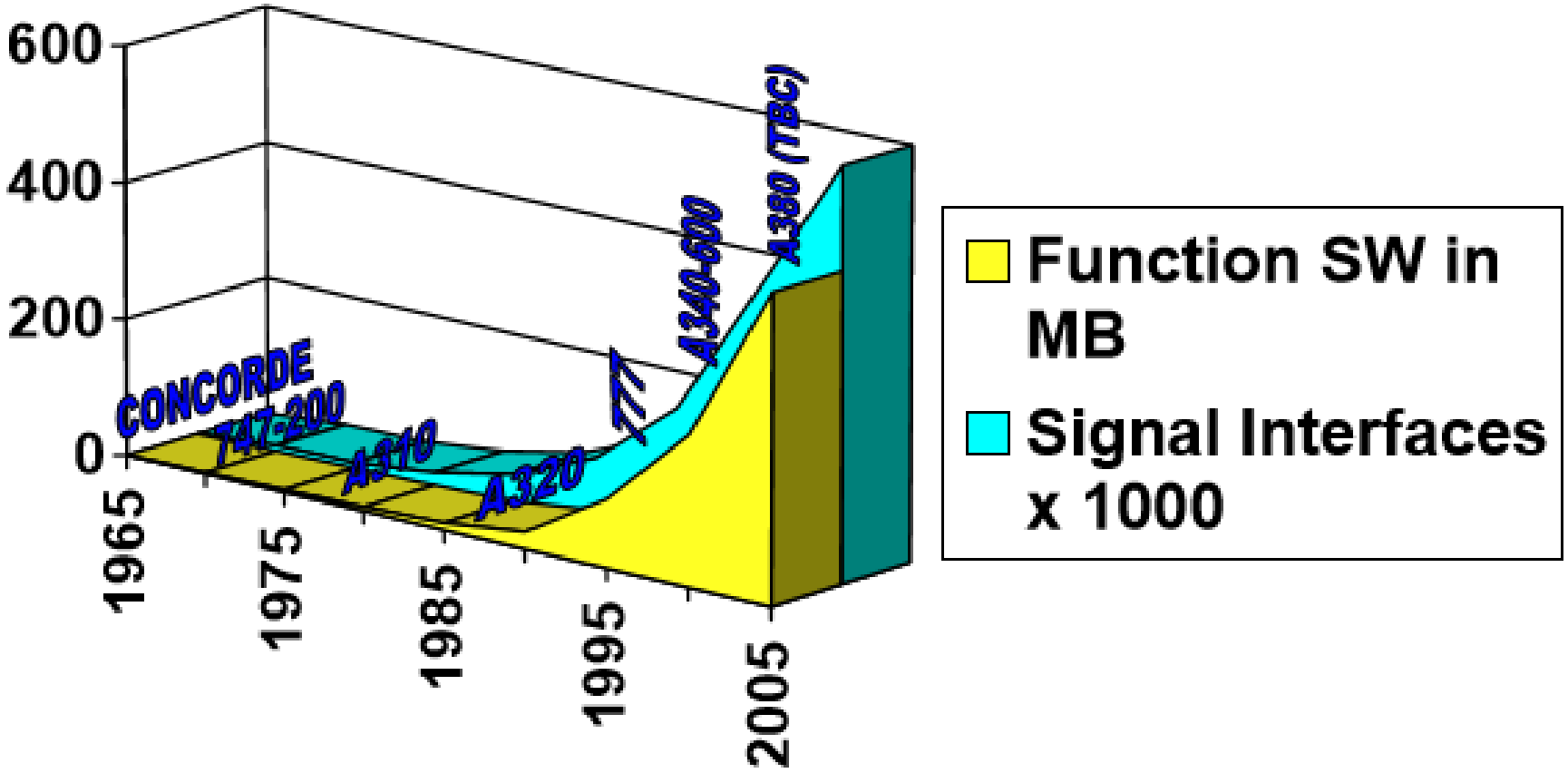
QUALIFICATION ASSURANCE (QA)

Avionic safety standards

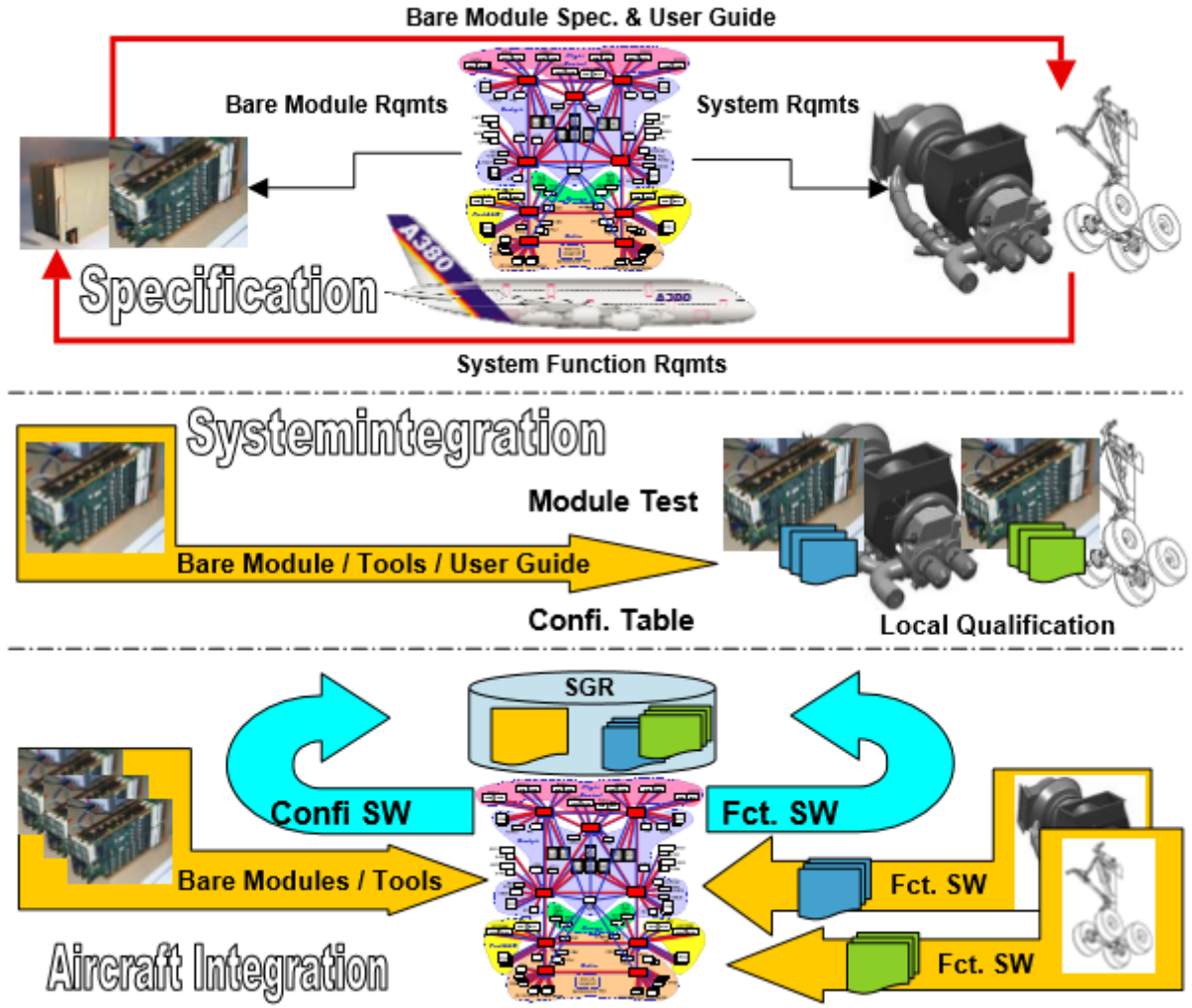


Installed Function SW and Signal Interfaces on board Commercial Aircraft require Integrated Modular Avionics (IMA)

(Butz, H., "Open Integrated Modular Avionic (IMA): State of the Art and future Development Road Map at Airbus Deutschland")

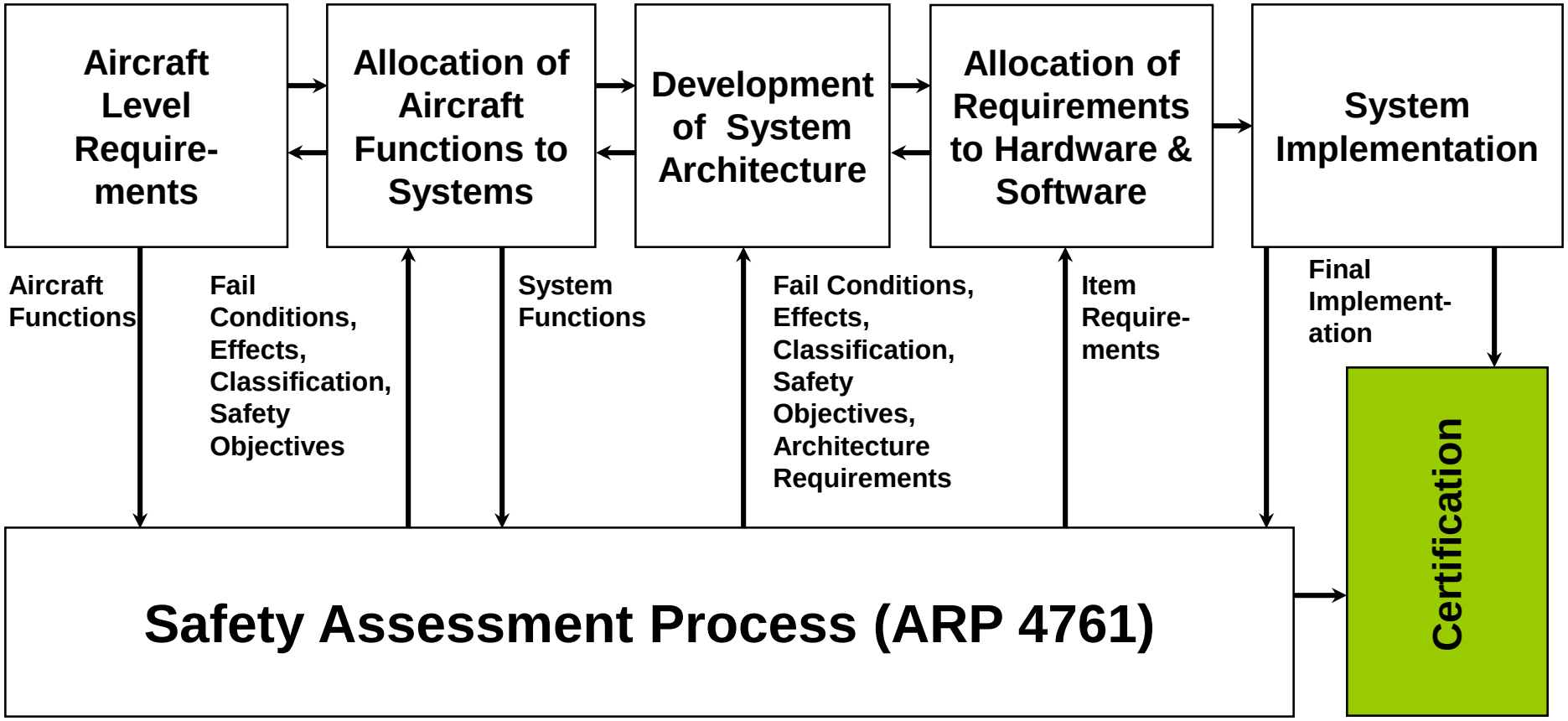


Development and Function to IMA Network Integration Processes Requires a New Integration Approach (Butz, H., ibid)



Commercial Manned Aircraft System Process Development Model Interactions with Safety Assessment Processes per ARP 4754A & ARP 4761- Assumes Transportation ConOps

System Development Process (ARP 4754A)



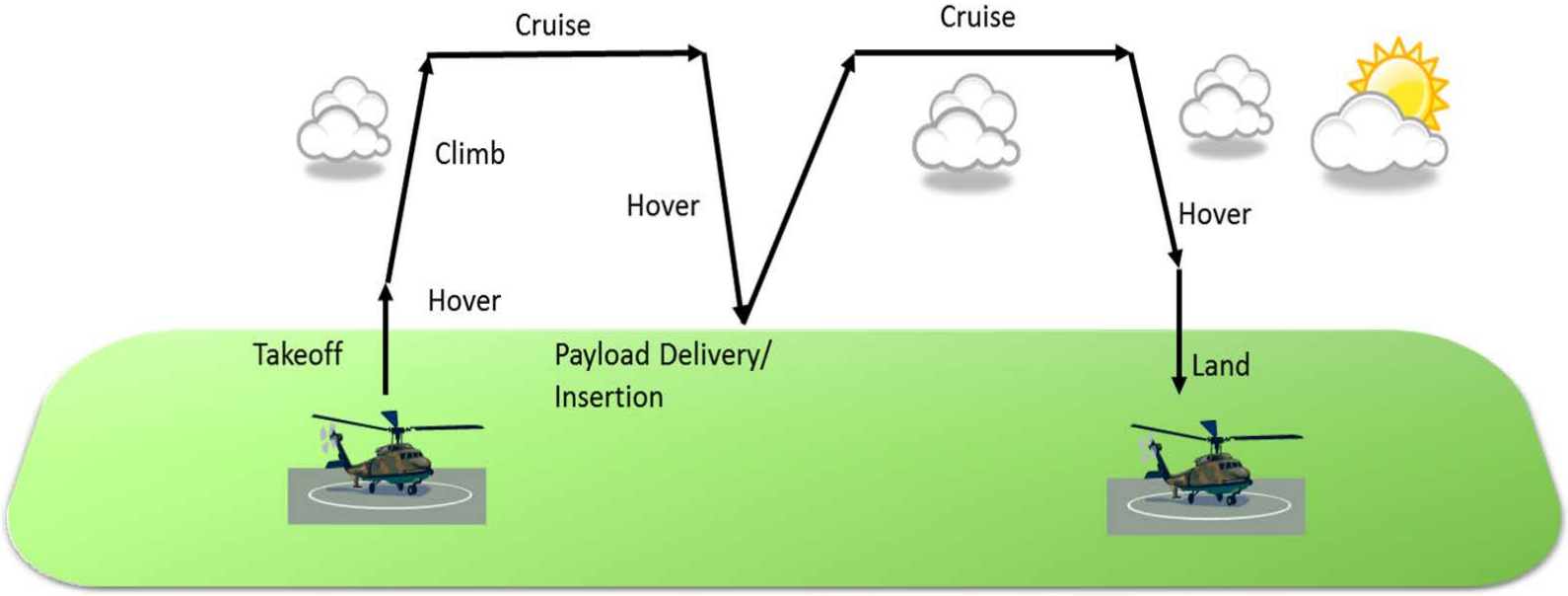
Mission Profiles Define Functions for System Effectiveness Criteria

Systems Effectiveness **is a measure of the extent to which a system may be expected to achieve a set of *specific mission requirements***

Capability (Performance):
Takeoff Distance/Hover Capability
Climb Rate
Cruise Speed
Descent Rate/Landing Distance

Availability (Readiness):
Reliability (MTBF)
Maintainability (MTTR)
Logistics Support

Dependability (Safety):
Flight Safety (FDAL)
Survivability (P_S)
In Flight Shutdowns



$$\text{VBA Metric} = \frac{\alpha(\text{Capability}) + \beta(\text{Availability}) + \gamma(\text{Dependability})}{\phi(\text{Life Cycle Cost})}$$

Functional Hazard Assessment

FHA

Relationships

- Independent of Hardware
- Provides criteria against which the other analyses will be assessed.
- Provides the FTA Top Events in the Form of Events of Concern (Failure Conditions)

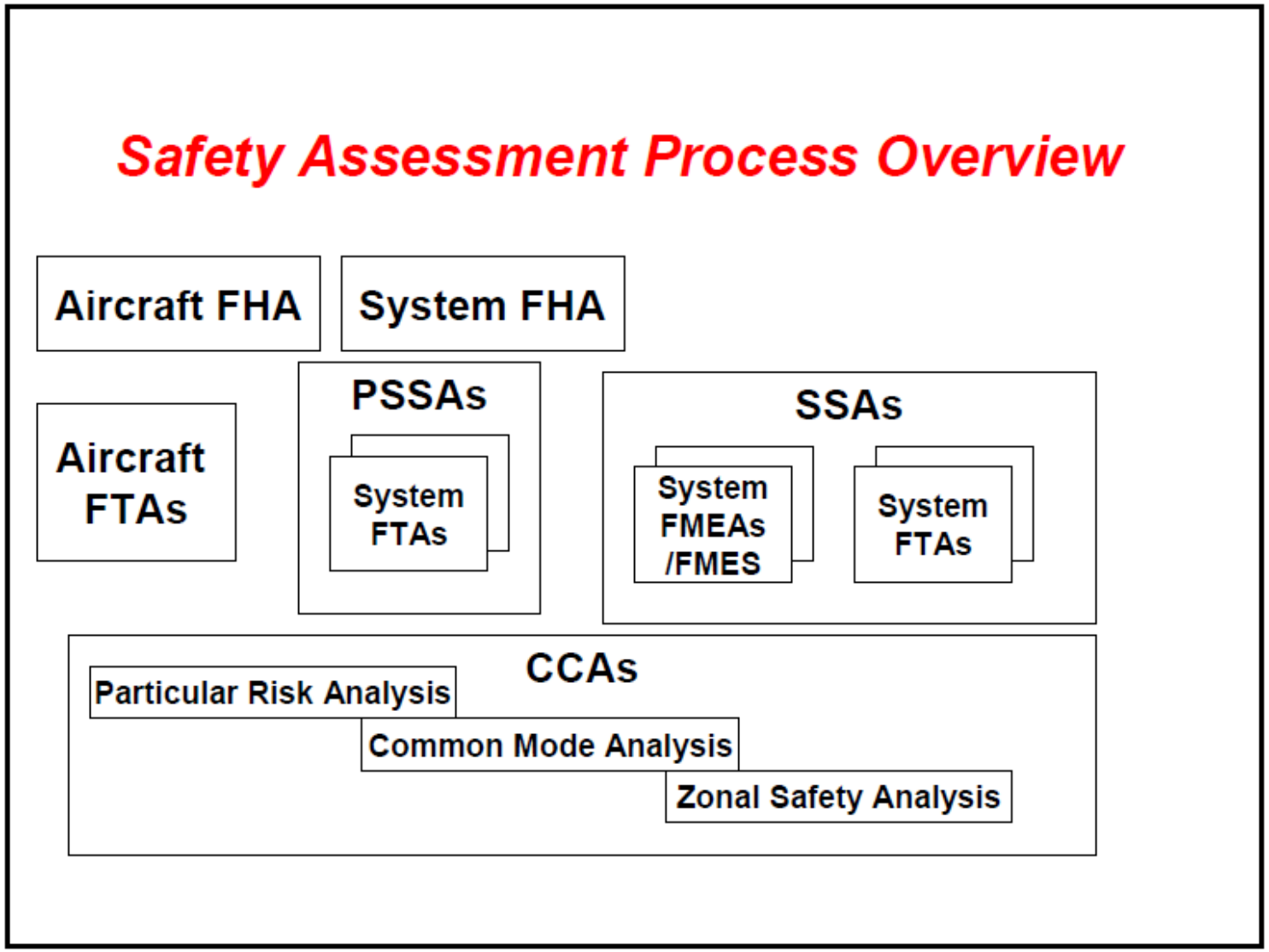
Functional Hazard Assessment

FHA

SUMMARY:

- Provides the Top Level Design Criteria
- Determines the Depth of Further Analyses
- Allows for Derivation of the System Architecture
- Independent of Hardware and Software

SAE ARP 4761: Guidelines and Methods of Performing the Safety Assessment Process on Civil Airborne Systems and Equipment



Random Failures and Development Errors

- A system behaviour can be affected by
  - Random failures of its components
  - Errors introduced during development process
- Random failures: The metrics used to estimate the random failure occurrence and decide of their acceptability are based on probabilities calculations: Failure rates, MTBF, reliability evaluation, probability of occurrence evaluation
- Development errors: The probabilistic approach is not used (non appropriate) to evaluate development errors occurrence. The decision that development errors have been sufficiently removed from a product are base on an evaluation of the quality level of the product development process.
- The quality level of a Development process is measured by what is called “Development Assurance Level” (DAL).

Difficulties with Applying Integrated Civil Aircraft and Systems Development with Safety Assessment Process for other Aviation Systems, e.g. General Aviation, Military and UAS

- The Civil Aircraft Integrated Approach is driven by large Commercial Transport Manned Aircraft (led by Boeing and Airbus) **who help set the aviation standards which then sets the safety bar** for other aviation systems
- Difficult, if not impossible, for General Aviation and Civil Rotorcraft to comply with the same Failsafe and DAL levels, **either economically or due to single point failures**
- Difficult for Military Aircraft to apply early integrated development and safety assessment as **sufficient funds are often unavailable** until after Milestone B; Also, **need a military aircraft level standard, like ARP4754A, for implementation** – Not **sufficient new starts** to affect new CPVS Development Assurance on its own – Remember IDA vs UML as a software language?
- Unmanned Aerial Systems (UAS), both small and large, **have broader Concepts of Operations (ConOps) which must be functionally defined**, some which may be simpler and easier to certify and some which may be more complicated than manned aircraft systems

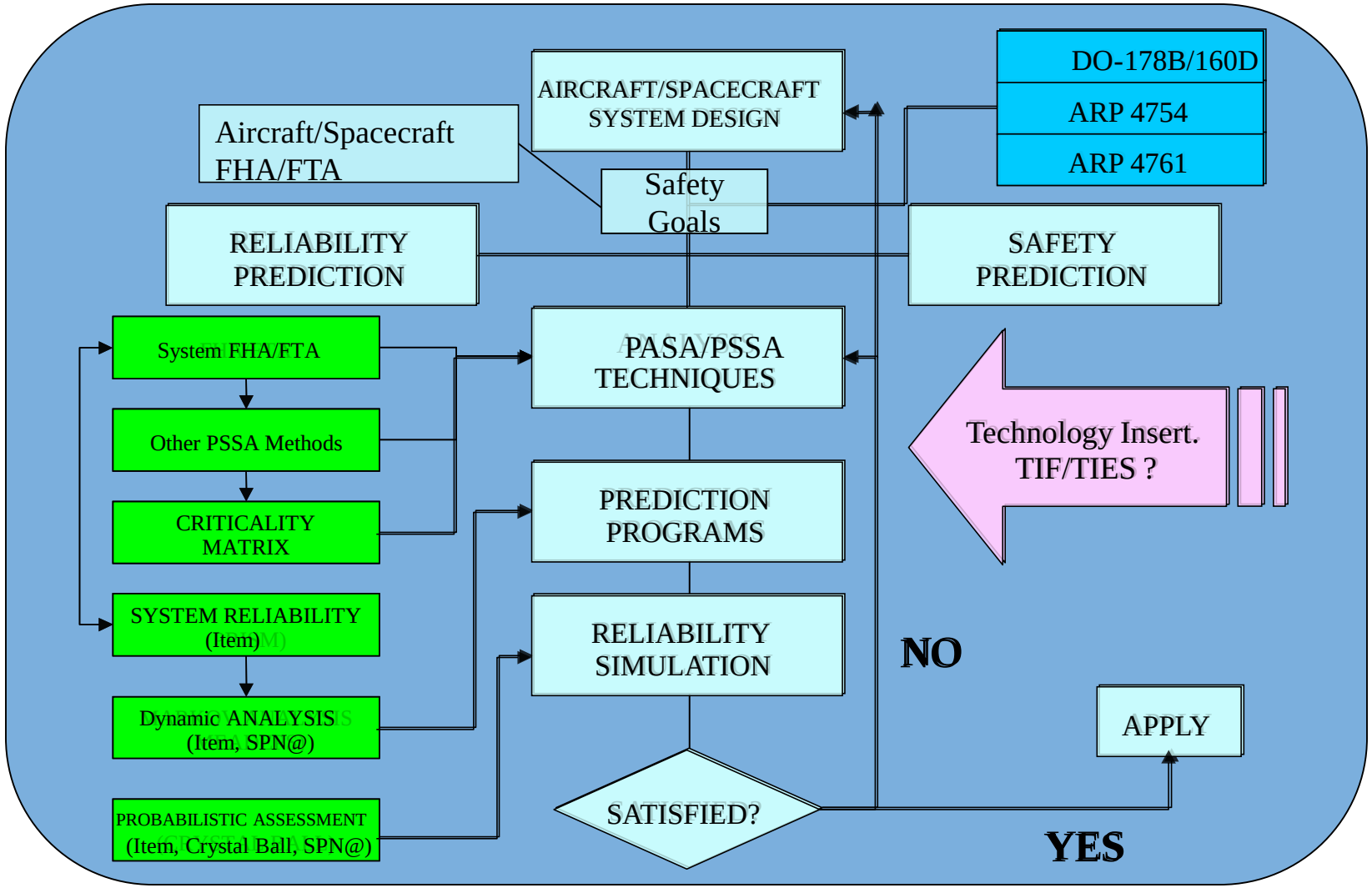
Example Case Studies from Safety By Design and Flight Certification Course – Using the ARP4754A Aircraft and Systems Development Guidance Approach

Dr. Daniel P. Schrage
Professor and Director, Vertical Lift
Research Center of Excellence (VLRCOE)
School of AE, Georgia Tech

Georgia Tech AE6362 Graduate Course: Safety By Design and Flight Certification

- Has been taught on an annual basis since 1995 and has used the Civil Aircraft and Systems Development Guidelines in ARP 4754/4761 on all types of aircraft systems, spacecraft and UAS
- Has been updated in recent years to address the changes incorporated in ARP 4754A and the updates in DO 178C, DO 297
- A set of tutorials are given, along with a quiz, on probabilistic methods and reliability engineering is provided to bring all students, both on campus and distance learning, up to basic level of understanding for conducting a Preliminary Aircraft Safety Assessment (PASA) and Preliminary System Safety Assessment (PSSA)
- ITEM Software Tools have been used in recent years. Other safety analysis methods and tools have been used in the past. Abridged Petri Nets (APN) by Dr. Vital Volovoi, a former co-instructor of the course, are also introduced and used by the students on their projects.
- Student Project Teams are required to use one dynamic state-based safety analysis method, e.g. Markov Chains or Stochastic Petri Nets (SPNs)

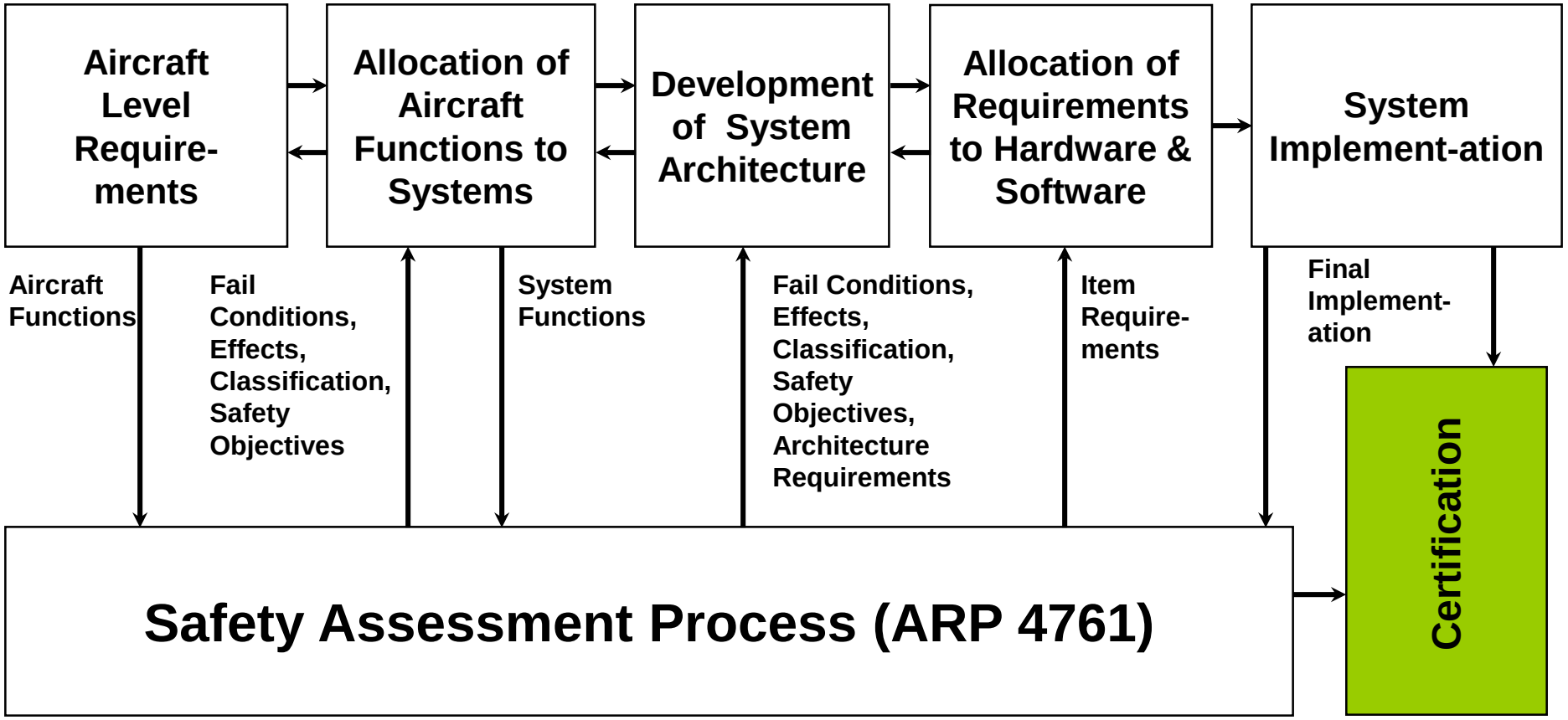
Georgia Tech SBD: Overall Approach



Dr.Daniel P. Schrage
School of AE
Georgia Tech

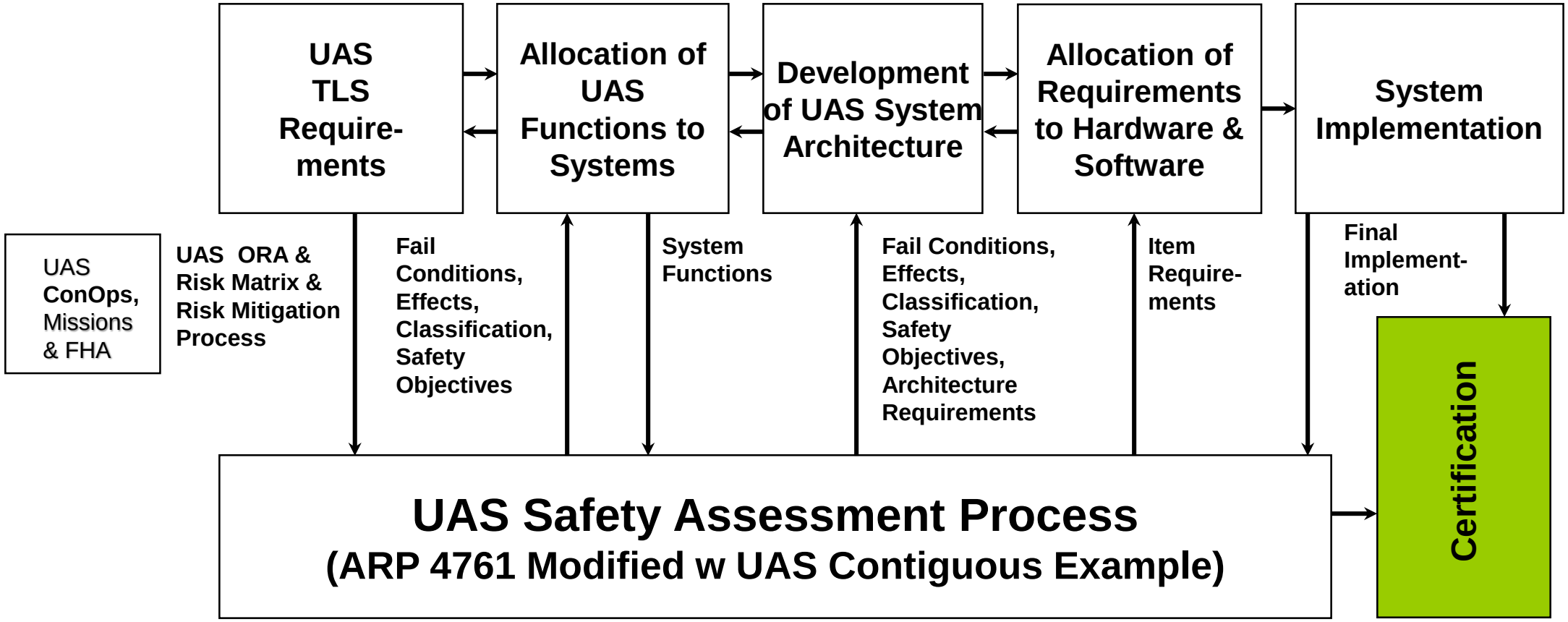
Commercial Manned Aircraft System Process Development Model Interactions with Safety Assessment Processes per ARP 4754A & ARP 4761

System Development Process (ARP 4754A)



Proposed UAS Process Development Model Interactions with Safety Assessment Processes for a Potential UAS FSM Standard & ARP 4761 Modified (sUAS Case Study included as Appendix)

System Development Process (UAS FSM Standard)



2018 AE6362 SBD Projects

Topic	Application
• Uber Elevate Air Taxi Safety Assessment & Certification	Support for Uber Elevate Air Taxi Initiative
• Yellow Jackets Space Program (YJSP) Safety Assessment for Potential Launch of Karem 1 Rocket	Relevant for Recent Announced Base 11 Space Challenge
• Preliminary Aircraft and System Safety Analysis for Boeing 777X Integrated Modular Avionics	Assessing an IMA Upgrade for a Commercial Transport
• Preliminary Aircraft and System Safety Analysis for AHS Competition Stopped-Rotor Concept Vehicle	Supports DoD Next Generation Umanned Aerial Systems (UAS)

Summary and Conclusions

- A Functional Safety Management Approach is the only viable way to certify CPVS and Complex Engineered Systems in an Economic and Rationale Way
- This presentation addresses how civil aviation aircraft and systems development guidance can be used as an appropriate FSM Approach for other complex engineered systems
- Examples of different relevant complex engineered systems from the Georgia Tech AE636218 Course: Safety By Design (SBD) and Flight Certification (FC), e.g. Air Taxis, Next Gen UAS, Rocket Launch and Individual Flying Machines are given as examples
- FSM approaches can and need to be tailored or further developed for CPVS certification