TTTech

Part 4:

Processes and Certification Standards

with an Aerospace focus

Aerospace System Design and Safety Assessment Processes

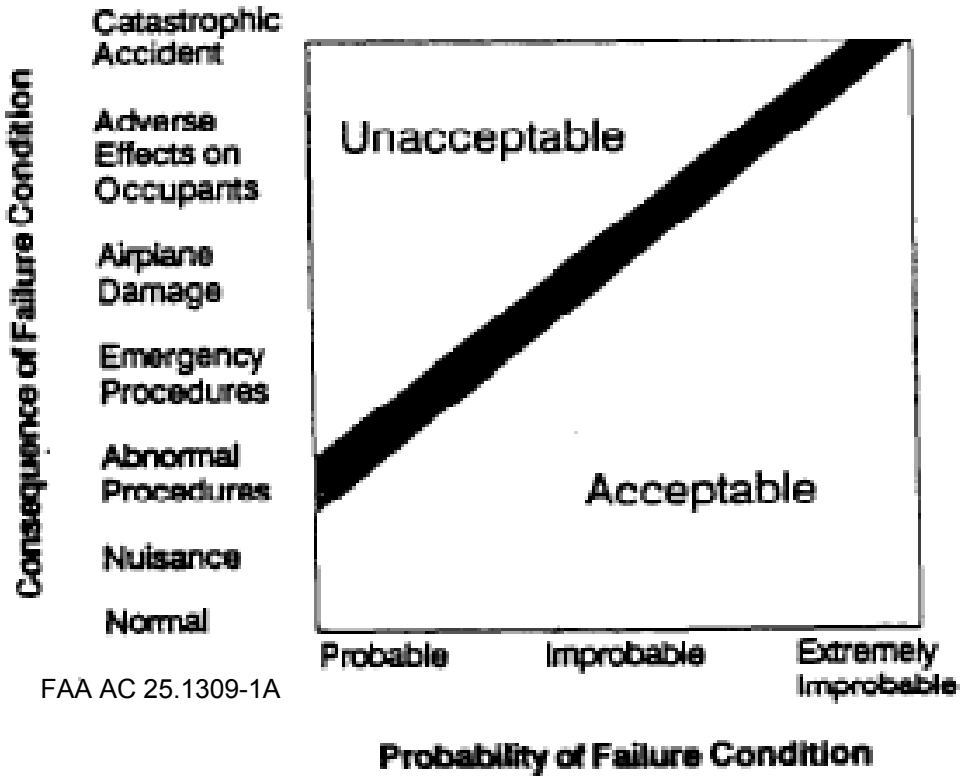
Federal Aviation Regulations (FAR) Part 25.1309, FAA Advisory Circular (AC) 25.1309-1A, SAE Aerospace Recommended Practice (ARP) 4754, SAE Aerospace Recommended Practice (ARP) 4761

This chapter will introduce:

- Primary Safety Objective (Probability vs. Consequences of Failure Conditions)
- System Design and Analysis Process
- Certification Considerations of Simple vs. Complex Systems
- System Safety Assesment and Development Assurance Levels

Probability vs. Consequences of Failure

Figure 1: Probability vs. Consequence Graph



FAA AC 25.1309-1A

The primary safety objective is to achieve an inverse relation of severity to probability.

Consequences of Failure Conditions

- **No Safety Effect:** Failure Conditions that would have no effect on safety. [...]
- **Minor:** Failure Conditions which would not significantly reduce airplane safety. [...]
- **Major:** Failure Conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions. [...]
- **Hazardous:** Failure Conditions which would lead to a large reduction in safety margins or functional capabilities, physical distress or excessive workload on the flight crew, or serious or fatal injury to a relatively small number of the occupants. [...]
- **Catastrophic:** Failure conditions which would result in multiple fatalities, usually with the loss of the airplane. [...]

(AC) 25.1309-1A

Probability of Failure Conditions

- **Probable** failure conditions are those anticipated to occur one or more times during the entire operational life of each airplane.
  (Average Probability per Flight Hour: $p > 1 \times 10^{-5}$)

- **Improbable** failure conditions are those not anticipated to occur during the entire operational life of a single random airplane. However, they may occur occasionally during the entire operational life of all airplanes of one type.
  (Average Probability per Flight Hour: $1 \times 10^{-9} < p < 1 \times 10^{-5}$)

- **Extremely Improbable** failure conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type.
  (Average Probability per Flight Hour: $p < 1 \times 10^{-9}$)

Note: Definitions of failure condition and probability classes vary slightly between standard documents and certification authority regulations.

System Design and Analysis Process

- **Functional Hazard Assessment (FHA)**
  - Identifcation of aircraft-level hazardous failure conditions
  - Classification of failure conditions according to the severity of their consequences
- **System Design & Analysis**
  - Required level of rigor increases with severity of failure consequences
  - Minor/Major/Catastrophic Failure Conditions map to requirements for qualitative and/or quantitative assessments according to flow chart
  - Credit for product service experience may be claimed for simple devices.
  - Also considers flight crew work-load and required ground crew actions

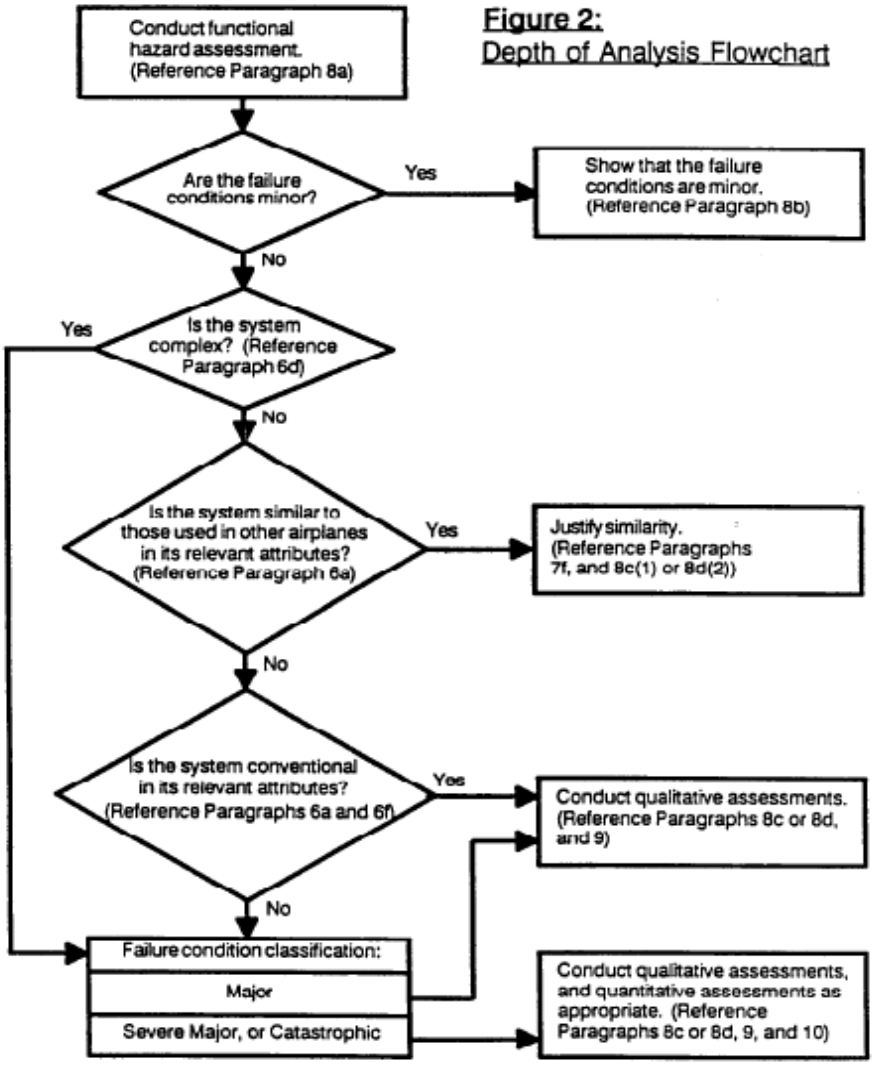


Figure 2:
Depth of Analysis Flowchart

FAA AC 25.1309-1A

System Design Obligations

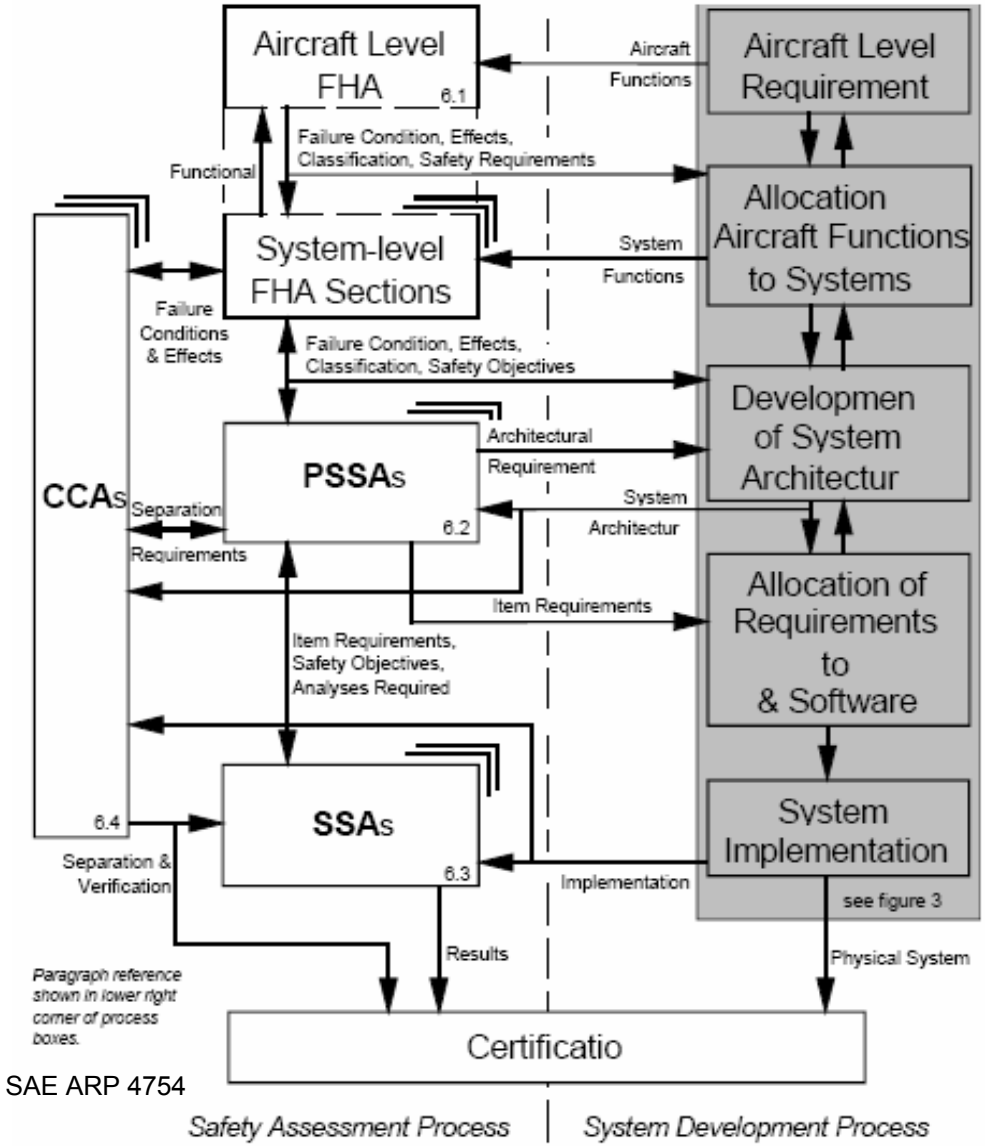
- **Minor Failure Condition**
  - Isolation of system must be shown
- **Major Failure Condition**
  - Must be shown to be improbable ($p<10^{-5}$)
  - For conventional (non-complex) system, reference similar systems or service history
  - Otherwise, conduct qualitative assessment (i.e. engeneering judgement, supported e.g. by Failure Mode and Effects Analysis (FMEA), Fault-Tree Analysis (FTA), Reliability Block Diagrams, etc.)
  - Analysis of redundant systems is complete, if isolation between redundant system channels is shown and reliability for each channel is satisfactory.
- **Hazardous/Catastrophic Failure Condition**
  - Must be shown to be extremely improbable ($p<10^{-9}$)
  - Appropriate combination of qualitative and quantitative analysis or substantial service experience of identical or very similar system
  - Probability analysis by means of quantitative FMEA, FTA, or Reliability Block Diagram, which also include numerical probability information. Primary failure rates can be determined from service history or acceptable industry standards.

Considerations for Complex Systems

- **Simple/conventional/non-complex systems**
  - Can be shown to be implemented correctly by exhaustive testing (def. DO-254) and fail *statistically* with the combined probabilities of their physical constituent parts.
  - Random component failure can be mitigated via redundancy strategies and can be analyzed by methods like FTAs and FMEAs.
- **Complex systems**
  - Systems too large for exhaustive testing (includes almost all SW-based systems)
  - May fail *systematically* due to the increased chance of residual *design errors,* which lead to certain failure under specific (but a priori unknown) operating conditions.
  - No probability numbers can be assigned to „the likelihood of design error“ in a product
  - Lacking accepted methods to demonstrate the absence of design error in a product, current certification regulations require rigorous development process assurance to qualitatively minimize the likelihood of design errors instead.
  - Consequently, increasing development assurance burden is assigned with relation to the safety effect of the implemented function in the form of ***Development Assurance Levels*** defined for complex HW and SW subsystems.
  - Process objectives to meet these levels are defined in DO-178B and DO-254

Development Process of Complex Systems

- Aircraft level functional requirements are allocated to **aircraft systems**
- Iterative analysis with **Functional Hazard Assessment (FHA)**
  - Determines severity of failures
- Development of **System Architecture**
  - Allocation, Redundancy, Partitioning, etc.
- **Preliminary System Safety Assessment (PSSA)** of design, iteratively (top-down)
  - Determines Safety Requirements and
  - Development Assurance Levels
- Allocation of requirements to **hardware** and **software items**
- HW/SW item development according to DO-254 and DO-178B, respectively
- ***System Safety Assesments*** **(SSAs)** analyze implementation (bottom-up)



SAE ARP 4754

Common Cause Analysis

- **Common Cause Analysis (CCA)** targets design errors that may invalidate subsystem *failure independence assumptions* required by the (P)SSA.
  - **Zonal Safety Analysis:**
    should examine each physical zone of the aircraft to ensure that equipment installation and potential physical interference with adjacent systems do not violate the independence requirements of the systems.
  - **Particular Risk Assessment**:
    should examine those common events or influences that are outside the system(s) concerned but which may violate independence requirements. These particular risks may also influence several zones at the same time, whereas zonal safety analysis is restricted to each specific zone.
  - **Common Mode Analysis:**
    provides evidence that the failures assumed to be independent are truly independent. The analysis also covers the effects of design, manufacturing, and maintenance errors and the effects of common component failures.

Considerations in Airborne Systems and Equipment Certification

RTCA DO-178B

and

Design Assurance Guidance for Airborne Electronic Hardware

RTCA DO-254

This chapter will introduce:

- Overview of DO-178B/DO-254 compliant life-cycle processes and process objectives
- Example: TTTech‘s Software Development Life-Cycle

RTCA DO-178B

- Industry consensus document for software certification in 3rd edition (1992), recognized by the international certification authorities as *applicable means of compliance*.
- Suggests software life cycle processes, but does *not* prescribe a preferred software life cycle. Rather a set of seperate processes which may be implemented in most life cycles is presented.
- Defines explicit process objectives to be met for each life cycle process.
- DO-178B compliant life cycles generally create evidence, that the objectives of each software process have been met, are verifiable and can be reproduced.
- DO-178B recognizes *Development Assurance Levels* labeled from A (highest) to D (lowest), where certain process objectives are waived with decreasing level.
- Processes may be automated, but tools used may require tool qualification, too. (distinction between Development Tools and Verification Tools)

RTCA DO-254

- Industry consensus document on complex hardware development in 1st edition (2000).
- Only recently recognized by the internation certification authorities as applicable means of compliance.
- Counterpart of DO-178B for hardware certification and *very* similar in spirit.
- DO-254 shares many process objectives with DO-178B

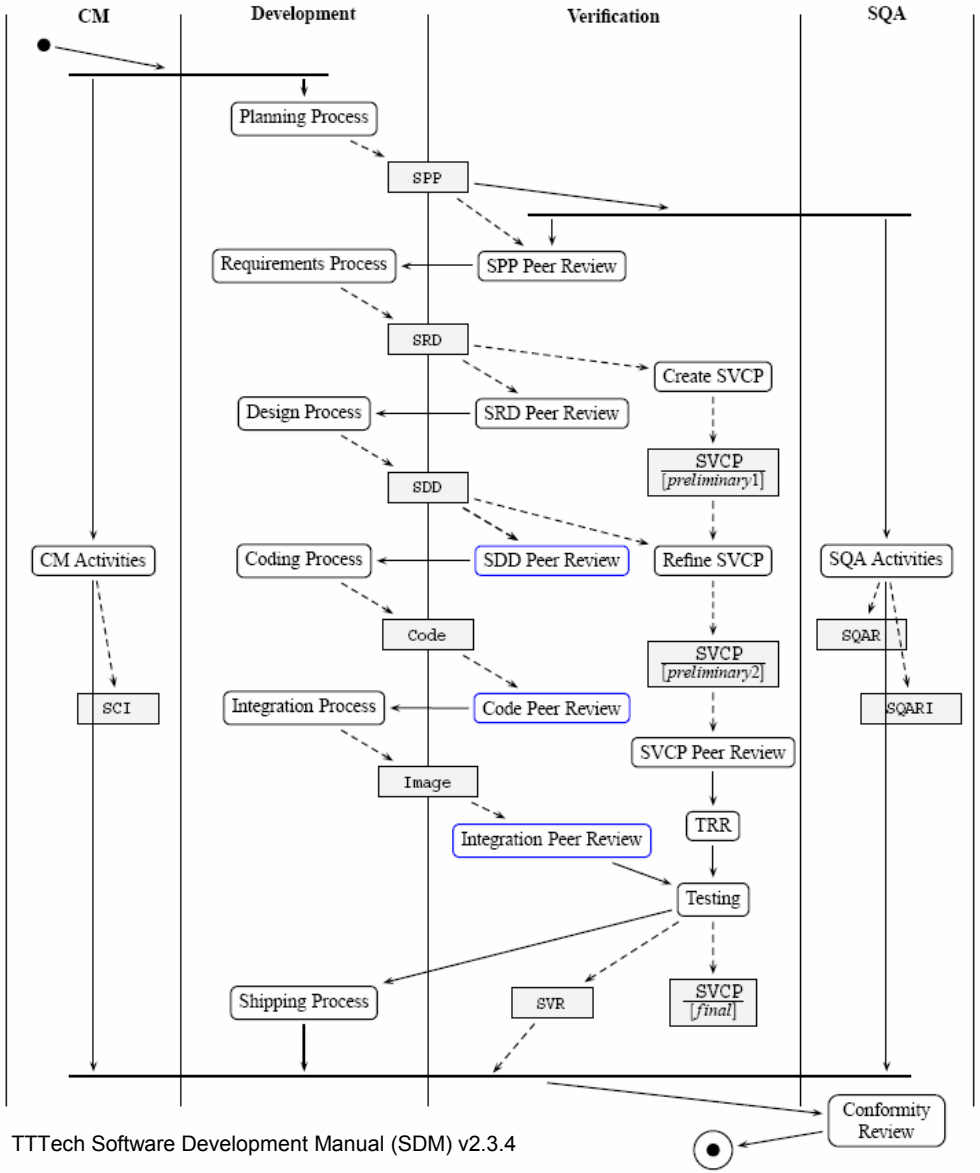
The following slides will review DO-178B and DO-254 processes and their objectives jointly.

Hardware/Software Life Cycle

- DO-254/DO-178B compliant HW/SW life cycles should comprise of the following processes:
  - **Planning Process**
  - **Development Process**
    - **Requirements Process**
    - **Conceptual Design Process**
    - **Detailed Design (HW) / Coding Process (SW)**
    - **Implementation (HW) / Integration Process (SW)**
  - **Verification and Validation Process**
    - **Reviews and Analyses**
    - **Testing Process**
  - **Configuration Management Process**
  - **Process/Quality Assurance Process**
  - **Certification Liaison Process**

Integral Processes

Example: TTTech´s Software Life Cycle



TTTech Software Development Manual (SDM) v2.3.4

- The flowchart to the left shows how software processes are implemented at TTTech.
- Each development process creates an artifact as output (documents or code).
- *Software Verification Cases and Procedures (SVCP)* are developed in parallel to the refinement steps of the development process.
- All development, planning and verification artifacts are *peer reviewed* prior to release.
- The Testing Process creates the *Software Verification Results (SVR)* as objective evidence for the correct implementation of all high- and low-level requirements.

Processes and Objectives

- Planning Process Objectives
  - Definition of development and integral processes activities (incl. CM, QA, Problem Tracking, etc.)
  - Definition of organizational roles and verification independence
  - Definition of transition criteria, interrelationships and sequencing among processes
  - Definition of life cycle environment (languages, compilers, other tools etc.)
  - Definition of applicable HW/SW development standards (mandatory rules to observe when writing requirements, code, etc.)

Processes and Objectives

- Development Process Objectives
  - Development of high-level requirements from system level requirements
  - Feedback of *derived* high-level requirements back to (P)SSA process
  - Development of software architecture/conceptual design
  - Development of low-level requirements from high-level requirements and architecture
  - Feedback of *derived* low-level requirements back to (P)SSA process
  - Traceability between system-level, high-level, and low-level requirements, code and test cases.

Note: DO-178B/DO-254 give further, more specific objectives for the lower-level Requirements, Design, Coding and Integration Processes.

Processes and Objectives

- Validation and Verification Process Objectives
  - The allocated system requirements have been developed into high-level requirements that satisfy those system requirements.
  - The high-level requirements have been developed into an software architecture (SW) or conceptual design (HW) and low-level requirements that satisfy the high-level requirements.
  - The conceptual design or software architecture and low-level requirements have been developed into Source Code (Detailed Design) that satisfies the low-level requirements and Software Architecture (Conceptual Design).
  - The Executable Object Code/Hardware Implementation satisfies the requirements.
  - The means used to satisfy these objectives are technically correct and complete.

- Means of verification are peer reviews, analyses and comprehensive tests.
- With lower *Development Assurance Level*, lower *test coverage criteria* have to be met (e.g. no low-level testing, no decision coverage for Level D software)

Processes and Objectives

- Configuration Management Process Objectives
  - Provide a defined and controlled configuration of all configuration items throughout the life cycle
  - Provide the ability to consistently replicate all configuration items and ensure secure physical archiving and recovery
  - Provide controls that ensure problems receive attention and changes are recorded, approved, and implemented.
  - Provide evidence of approval of the by control of the outputs of the life cycle processes.

Processes and Objectives

- Process/Quality Assurance Process Objectives
  - Development processes and integral processes comply with approved plans and standards.
  - The transition criteria for the life cycle processes are satisfied.
  - A conformity review of the product is conducted.

- Certification Liaison Process Objectives
  - Communication between applicant and authority is established
  - Means of compliance is proposed and agreement is established
  - Compliance substantiation is provided.

Integrated Modular Avionics (IMA)

Development Guidance and Certification Considerations

RTCA document DO-297,
EUROCAE document ED-124

This presentation will introduce:

- The motivation for a new, modular approach to avionics systems certification
- Basic IMA certification terms and their relationships
- Key characteristics of IMA Platforms and Applications
- The Time-Triggered Architecture (TTA) as an example of a real-world IMA Platform
- IMA Certification Tasks and required Module Acceptance Data
- IMA Change and Reuse Requirements
- IMA System Safety Assessment

IMA and its motivation

- IMA: Integrated Modular Avionics

  Boeing 777 first plane to deploy IMA implemented by Honeywell, 1992 (SafeBus)

  TSO C153 (Type Standard Order for re-usable Hardware) first FAA acknowledgement of IMA

  SC 200 WG 60 design and development guidance for IMA

- Motivation for IMA

  Functional integration for improved services

  Reduced number boxes and cabling to save weight

  Hardware transparency and obsolescence support

  upgradeability

Integrated Modular Avionics (IMA)

"IMA is a shared set of flexible, reusable, and interoperable hardware and software resources that, when integrated, form a platform that provides services, designed and verified to a defined set of safety and performance requirements, to host applications performing aircraft functions."

(DO-*297*/ED-124 Glossary Definition of IMA)

- Current certification regulations only allow for certification of an aircraft as a complete system. Only few subsystems (engines and propellers) are accepted independently without reference to any specific aircraft type.
- Reuse of e.g. hardware or software between aircraft types is only informal, ad-hoc, and requires re-inspection and potential amendments at every instance.

Integrated Modular Avionics (IMA)

- The complex relationships of suppliers and sub-suppliers and their roles are not recognized by certification authorities. Only certification applicants (aircraft manufacturers) are “visible” to them.
- The need for a more modular approach of system certification thus became apparent and lead to the formation of RTCA Special Committee SC-200 and EUROCAE Working Group WG-60 in 2002 with the task to prepare a Development Guidance and Certification Considerations document for Integrated Modular Avionics.
- The SC-200/WG-60 committee is expected to complete the document in fall 2005.
- EASA and FAA are expected to formally recognize this document as acceptable means of compliance in Europe and the USA soon thereafter.

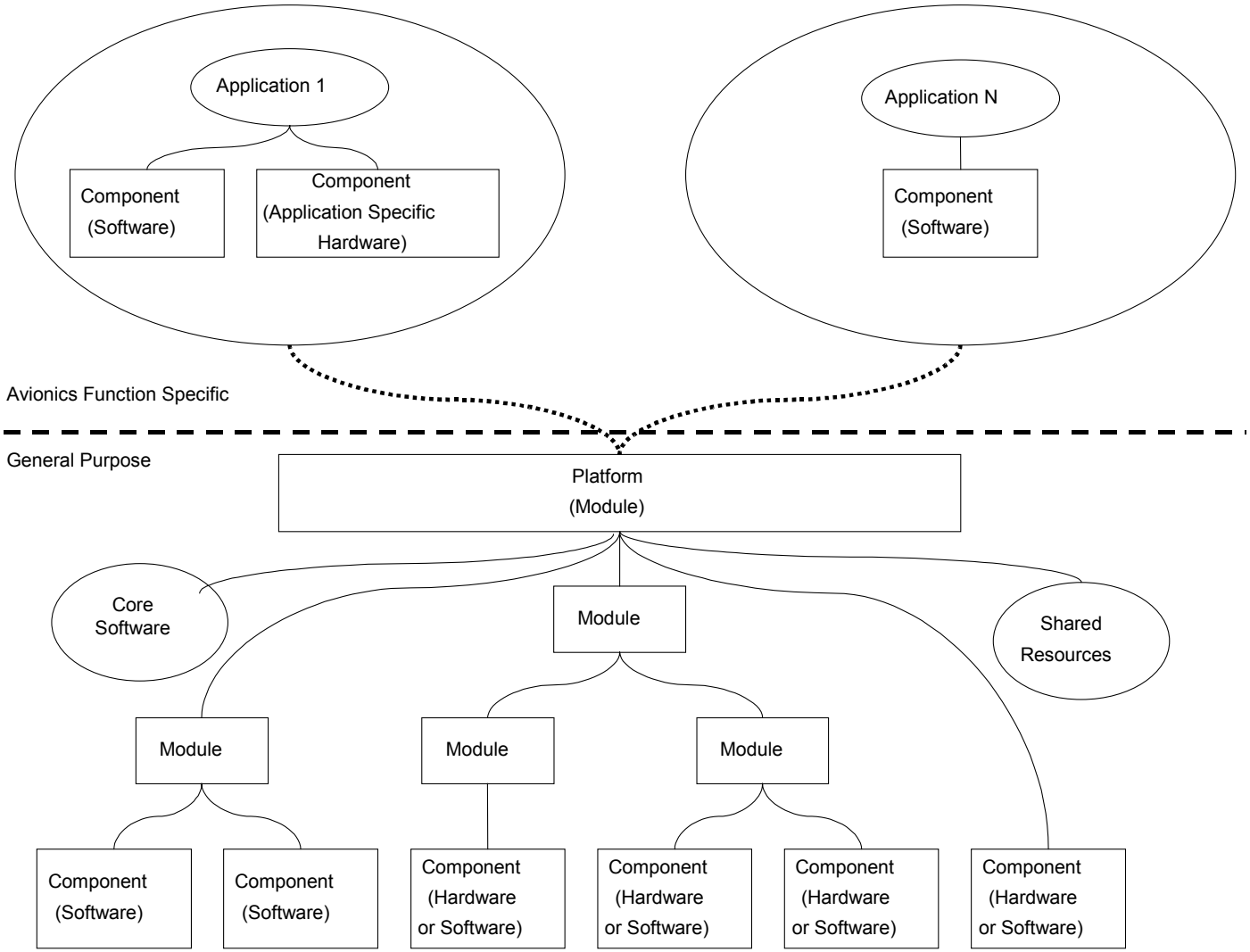
IMA Certification Terminology

Component - A self-contained hardware part, software part, database, or combination thereof that is configuration controlled. A component does not provide an aircraft function by itself.

Module – A component or collection of components that may be accepted by themselves or in the context of IMA. A module may also comprise other modules. A module may be software, hardware, or a combination of hardware and software, which provides resources to the IMA-hosted applications. Modules may be distributed across the aircraft or may be co-located.

Platform - Module or group of modules, including core software that manages resources in a manner sufficient to support at least one application. IMA hardware resources and core software are designed and managed in a way to provide computational, communication, and interface capabilities for hosting at least one application. Platforms, by themselves, do not provide any aircraft functionality. The platform establishes a computing environment, support services, and platform-related capabilities, such as health monitoring and fault management. The IMA platform may be accepted independently of hosted applications.

IMA System Structure



IMA Key Characteristics

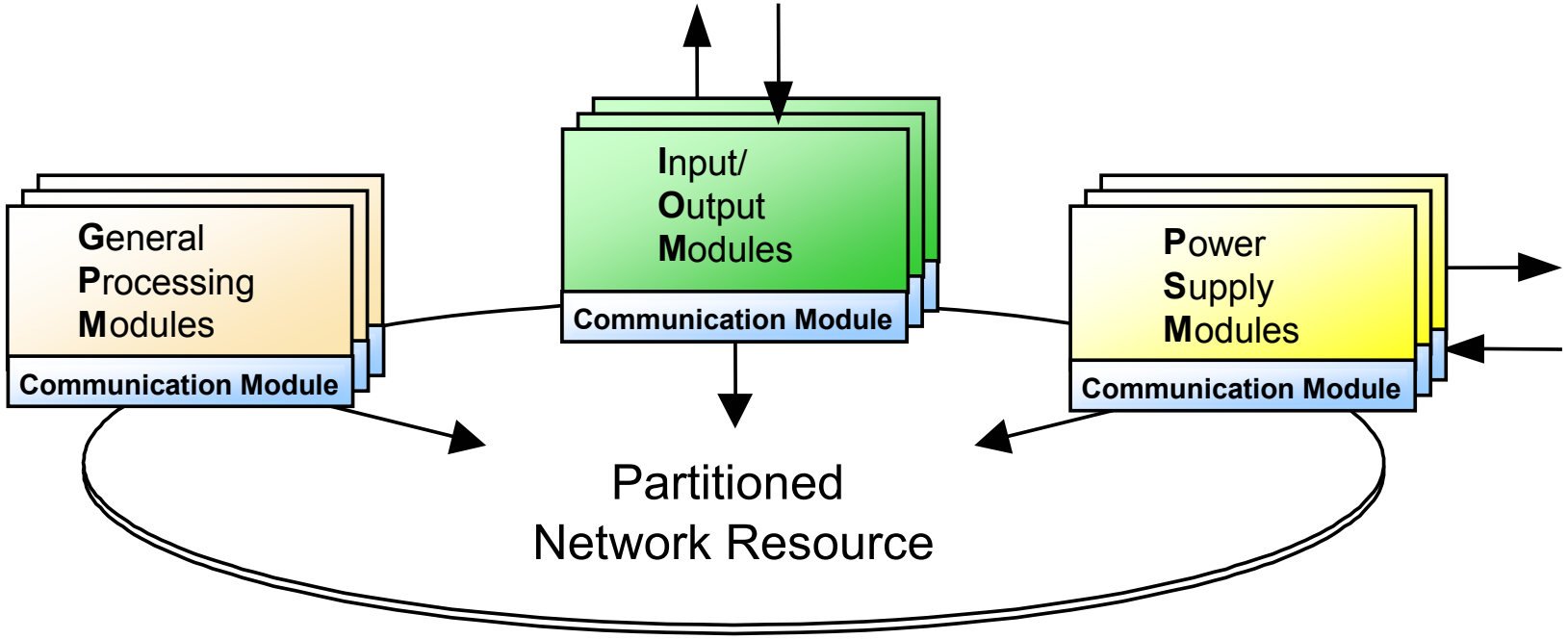
- Platform Characteristics
  - Platform resources are shared by multiple applications
  - An IMA platform autonomously provides robust partitioning of shared resource
  - An IMA platform only allows hosted applications to interact with the platform and other hosted applications through well defined interface
  - Shared IMA platform resources are configurable to support reuse of the platform

- Application Characteristics
  - An application may be designed independent of other applications and obtain incremental acceptance on the IMA platform independently of other applications
  - Applications can be integrated onto a platform without unintended interactions with other hosted applications
  - Applications may be reusable
  - Applications are independently modifiable

IMA Key Characteristics

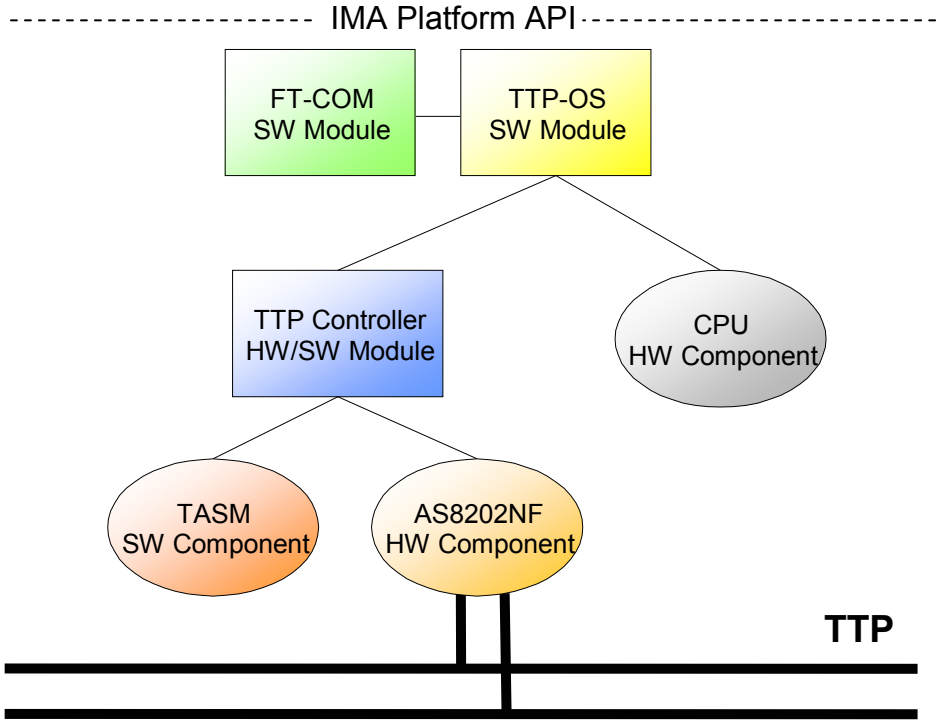
- Shared Resources
  - Each shared resource has the potential to become a single point of failure that can affect all applications using that resource. Accordingly, an IMA platform has to apply appropriate mitigation techniques as determined by the system safety assessment process.
- Robust Partitioning
  - A mechanism for assuring the intended isolation of independent aircraft functions and applications residing in IMA shared resources in the presence of design errors and hardware failures that are unique to a partition or associated with application specific hardware.
- Health Monitoring and Fault Management
  - The IMA platform provides health monitoring and fault management capabilities for the platform and hosted applications. The IMA system may have to provide higher level (aircraft function) health monitoring and fault management capabilities to support availability and integrity requirements.

Example: Time-Triggered Architecture



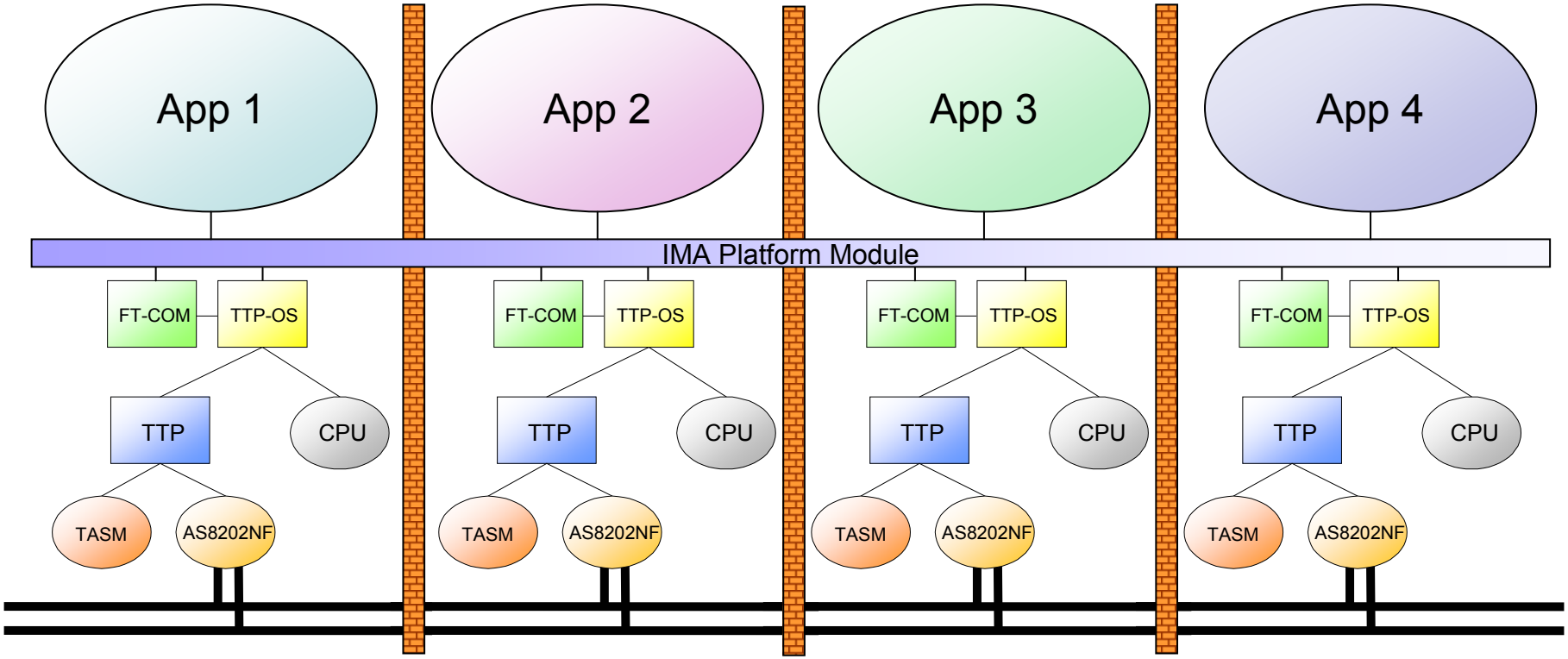
- **Processing Modules (LRUs):** Multitude of *general-purpose LRUs* on which applications can be integrated to perform aircraft functions. May contain application-specific hardware.
- **Communication Modules:** *TTP communication controllers* robustly partition access to the shared network resource. That resource may either be a dual-redundant bus- or star-topology. The star topology may include an additional *Central Bus Guardian module* to provide even stronger partitioning and fault-containment claims (not shown).
- **IMA Platform:** The integration of (a subset of) these modules forms a general-purpose IMA Platform, called the ***Time-Triggered Architecture (TTA)*** by TTTech.

Example: Decomposition into IMA Modules



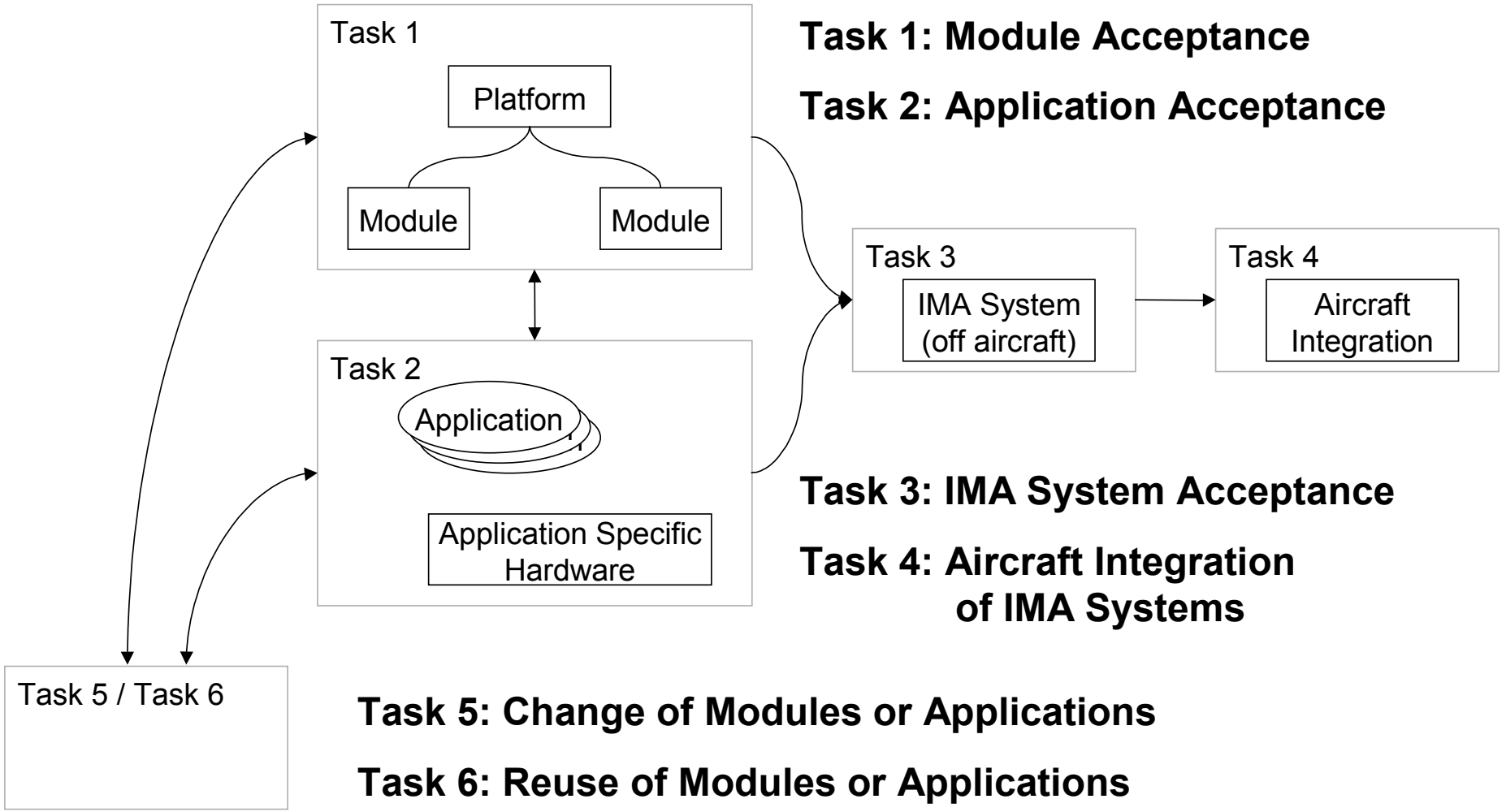
- **TTP Controller Module:** This reusable module is comprised of the *AS8202NF chip HW component* executing the *TASM SW component*. This module governs access to the *communication channel*, which is *shared* among multiple components of this type. It also provides a global reference time.
- **Robust Partitioning** of the *shared communication channel* is ensured by the autonomous execution of a static *TDMA schedule*, which cannot be influence in any way by IMA applications using this service.
- **Health Monitoring** is implemented by a *Group Membership Service* executed by the *TTP Controller*.
- **Fault Management** tasks are divided between the *TTP Controller Module* and *FT-COM SW Module*.

Example: TTA as IMA Platform



- **TTP-OS** is a reusable software module which *integrates* on the TTP Controller Module and a CPU component. It executes a static task schedule in synchrony with the global reference time provided by the TTP Controller Module.
- The **FT-COM** module is implemented as local tasks in TTP-OS. It reduces redundant messages from replicated applications to single, agreed values before they are presented to the local application.
- **Robust Partitioning** between applications is ensured by the static TDMA bus access schedule *enforced* by the *TTP Controller Module* (or, optionally, Central Guardian Modules)

IMA Certification Tasks



Task 1: Module Acceptance

Task 2: Application Acceptance

Task 3: IMA System Acceptance

Task 4: Aircraft Integration of IMA Systems

Task 5: Change of Modules or Applications

Task 6: Reuse of Modules or Applications

IMA Certification Tasks and Certificates

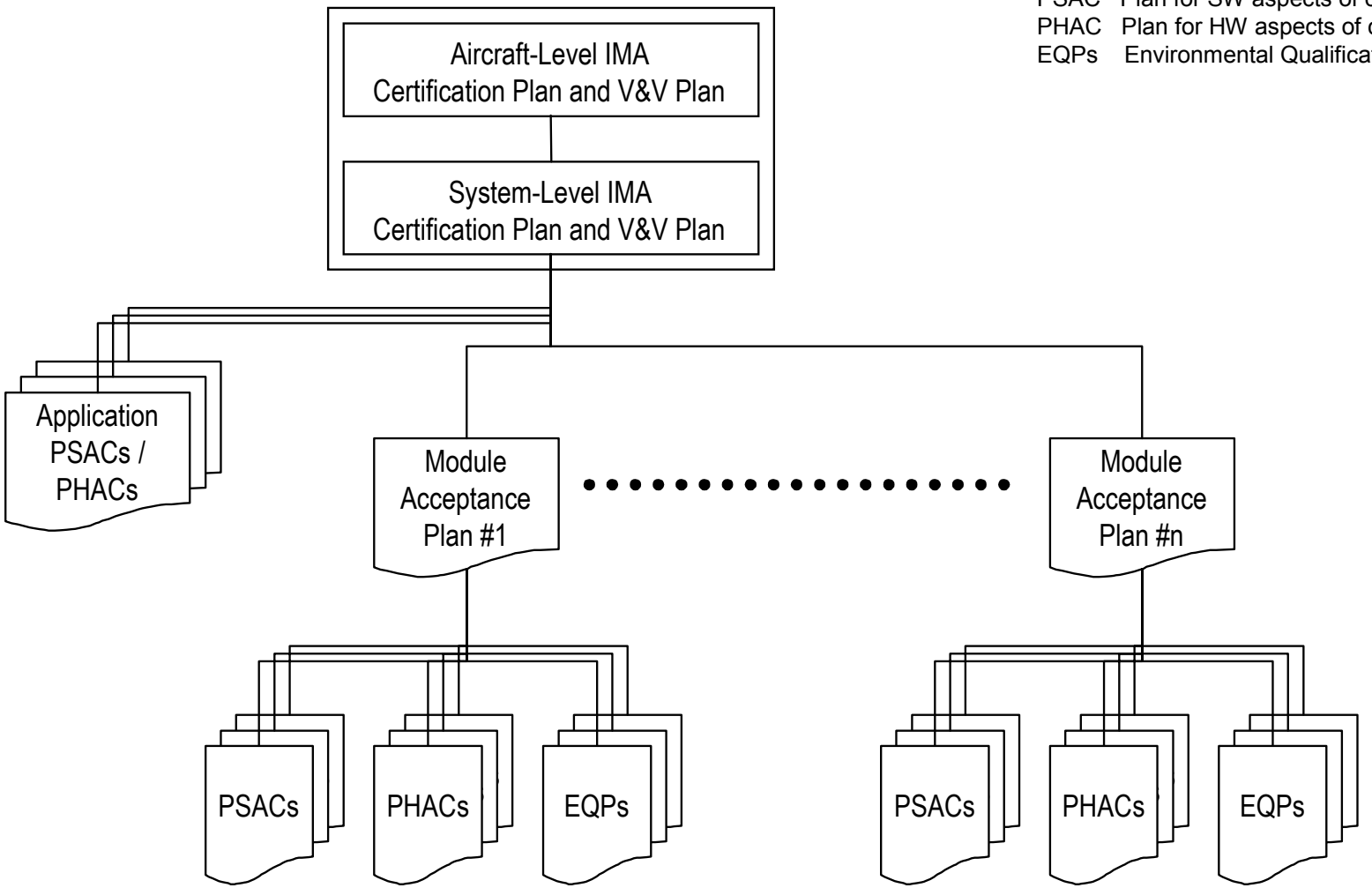
- **Task 1: Module Acceptance**
  - Integrate components and/or modules to form a platform
  - Acceptance letter, approved module acceptance data package
- **Task 2: Application Acceptance**
  - Integrate a single application with the platform
  - Acceptance letter, approved IMA platform-hosted application compliance data
- **Task 3: IMA System Acceptance**
  - Integrate multiple applications with the platform(s) and one another
  - Acceptance letter or stamped data sheet, Accepted or approved compliance data package
- **Task 4: Aircraft Integration of IMA Systems**
  - Integrate IMA system with aircraft and its systems
  - (classic) Type Certificate (TC), Supplemental TC, Amended TC, Amended Supplemental TC
- **Task 5: Change of Modules or Applications**
  - Identify changes and their impacts, and need for re-verification
  - Same as Task 1 if change of module , same as Task 2 if change of application
- **Task 6: Reuse of Modules or Applications**
  - Identify and use IMA components on other IMA systems and installations
  - Same as Task 1 if reuse of module, same as Task 2 if reuse of application

Recognition of Stakeholder Roles

- **In the context of an IMA project, the following typical stakeholder roles are recognized by the document:**
  - Certification Authority
  - Certification Applicant
  - IMA System Integrator
  - Platform and Module Suppliers
  - Application Supplier
  - Maintenance Organization
- **Clear interfaces between roles through required IMA document structure**
- **Organizations may assume one or more of these roles**
- **Each role is assigned a specific IMA certification task and is involved in the integral system assesment process.**

Planning data for IMA system

PSAC Plan for SW aspects of certification
PHAC Plan for HW aspects of certification
EQPs Environmental Qualification Plans



Module Acceptance Data

- **Module Acceptance Plan (MAP)**
  - System Overview / Module Overview
  - Acceptance Criteria
    - Software/Hardware design assurance Levels
    - Hardware Environmental Qualification Level
    - Safety requirements allocated to module/effects of module on system safety
  - Module Life Cycle and output documents (Module Life Cycle Data)
    - Requiremens, Design, Implementation, and Verification processes
  - Certification Schedule
  - Tool Qualification
  - Module Reuse Considerations
    - Justification for reusability
    - List of data supplied to applicant
    - Prior credit being claimed, further credit claimed and open activities
    - Interface data, reuse guidance, limitations, instructions for completing partial credits, etc.

Module Acceptance Data

- **Module Requirements Specification (MRS)**
  - Functional, operational and performance requirements, with attention to safety.
  - Safety and protection requirements, potential failure conditions.
  - Interface requirements and definitions
  - Fault Management and health monitoring requirements.
  - Resource management, scheduling procedures and inter-processor/inter-task communication
  - Requirements for robust partitioning, including identification of allowed interactions between module partitions, and requirements for the methods and means of preventing partition breaches, detecting partition violations, and recovering from partition violations.
  - Description of deactivated features or mechanisms (for future reconfiguration), if appropriate.
  - References to DO-178B/DO-254 life cycle data as appropriate

Module Acceptance Data

- **Module Validation and Verification (V&V) Data**
  - Module V&V data is the evidence of the completeness, correctness, and compliance of the module with its requirements, as defined in the MRS. It provides assurance that the module has been developed to its requirements, correctly produced, validated and verified, and the acceptance criteria has been achieved. Data includes procedures and results for module reviews, analyses, simulation and testing.
  - **SW**: Software verification cases, procedures, and results (see DO-178/ED-12), as appropriate to the software level *when software is part of the module.*
  - **HW**: Traceability data, review and analysis procedures and results, test procedures and results, and test acceptance criteria (see DO-254/ED-80, Ref. [6]), as appropriate to the design assurance level *when complex hardware is part of the module.*
  - **EQ**: Data, which includes the environmental qualifications form, level(s) of testing, test plan, test procedures, and results of the tests (see DO-160/ED-14). Not all testing can typically be done at the module level. Certain types of tests can only be done when the module is integrated within the system and/or aircraft.
  - **Module integration V&V cases and procedures and results**, when modules are integrated on the module. Review and analysis procedures, Test cases, and Test procedures.
  - **Module traceability data.** Module traceability establishes a correlation between the requirements, detailed design, implementation and verification data that facilitates configuration control, modification and verification of the module.

Module Acceptance Data

- **Module Quality Assurance (QA) Records**
  - The results of the module QA process activities are recorded in QA records. These may include QA review or audit reports, meeting minutes, records of authorized process deviations, or conformity review records.
- **Module Configuration Index**
  - The MCI identifies the configuration of the module and the module life cycle environment. This index is written to aid reproduction of the module, including its life cycle environment for regeneration, re-verification, or modification.
- **Module Acceptance Configuration Management (CM) Records**
  - The results of the module CM process activities are recorded in CM Records. Examples include configuration identification lists, baseline or library records, change history reports, archive records, and release records.
- **Module Acceptance Accomplishment Summary (MAAS)**
  - Compares the Module Acceptance Plan with actual accomplishments and explains and differences.
  - Lists remaining activities for the user of this module.

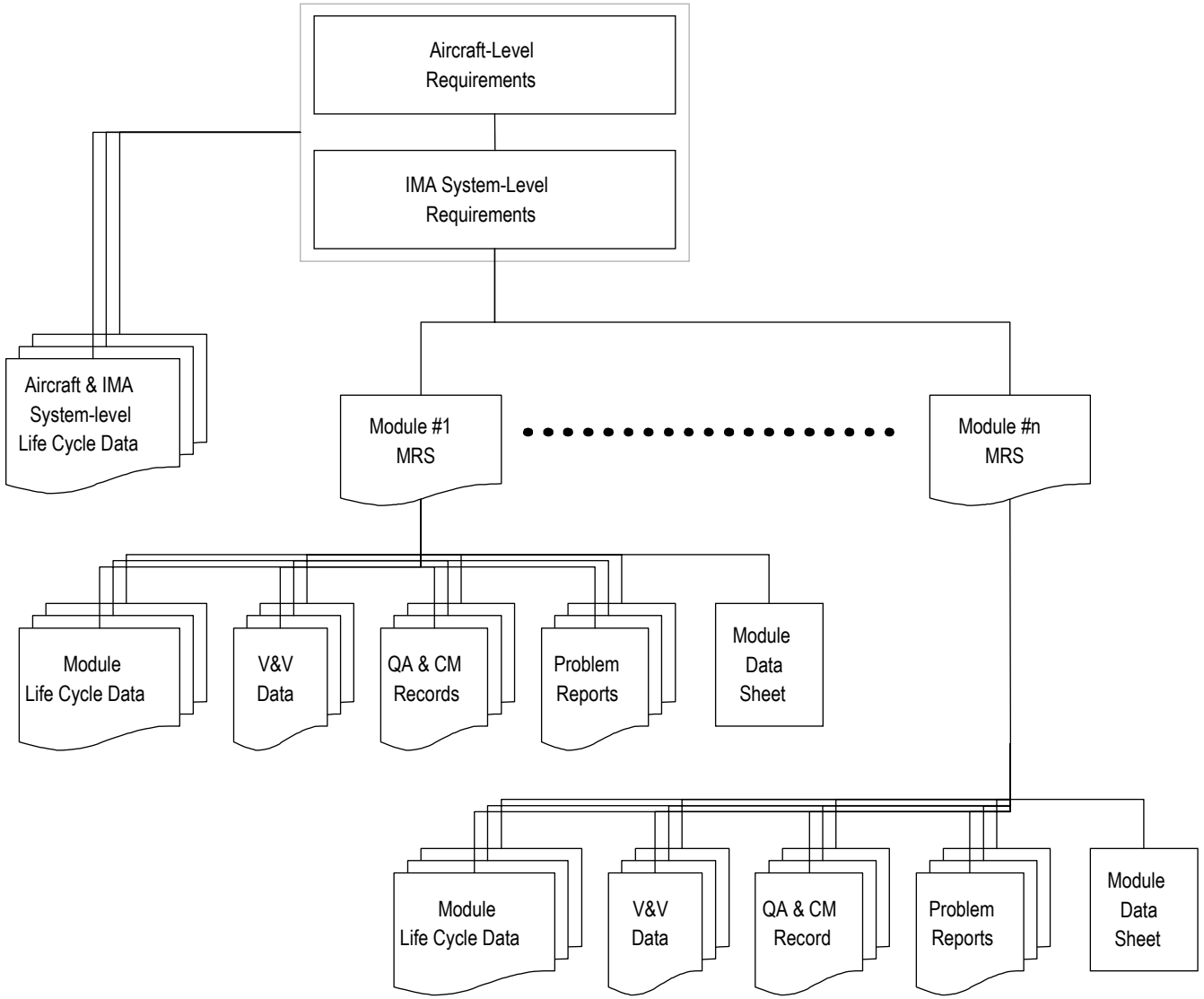
Module Acceptance Data

- **Module Accpetance Data Sheet (MADS)**
  - Module part number(s), should include modification and revision status.
  - Reference to the final Module Configuration Index (with revision status).
  - Software level(s) and hardware design assurance level(s)
  - Environmental qualification test levels achieved.
  - Physical connection information for hardware
  - Power requirements and dissipation
  - Size and weight
  - Special installation information (e.g. dataloading, grounding, airflow...)
  - Safety assessment information that may affect installation
  - Tool requirements as applicable for software development, verification, and system configuration
  - Usage domain of the module.
- **Module Problem Reports**
- **Additional Module Acceptance Life Cycle Data**

IMA Application Acceptance Data

- **For the certification of IMA *applications,* the established certification processes apply in general:**
  - DO-178B processes for Software
  - DO-254 processes for Hardware, and
  - DO-160E for Environmental Qualification
- **If application reuse is planned, the PSACs/PHACs must address:**
  - Justification for reusability
  - List of data supplied to applicant
  - Prior credit being claimed, further credit claimed and open activities
  - Interface data, reuse guidance, limitations, instructions for completing partial credits, etc.

Typical Life Cycle Data for an IMA System



Further IMA Acceptance Data

- **IMA System Acceptance Data**
  - IMA System Certification Plan (IMASCP)
  - IMA System Validation and Verification Plan (IMASVVP)
  - IMA System Configuration Index (IMASCI)
  - System-level IMA Accomplishment Summary (IMAAS)
  - Other IMA System Life Cycle Data
- **Aircraft-level IMA System Compliance Data**
  - Aircraft-level IMA System Certification Plan (IMASCP)
  - Aircraft-level Validation & Verification Plan
  - Aircraft-level IMA System Configuration Index (IMASCI)
  - Aircraft-level IMA Accomplishment Summary (IMAAS)
  - Other Aircraft-level Data

Change of Modules or Applications

- A change may involve modification to resources, modules or hosted applications, including addition, deletion, fixing or modification of IMA system components.
- In some cases, components may be changed in the modules to address obsolescence, reliability, etc. without affecting the functionality of the IMA system.
- There are a variety of types of changes that may occur, such as a
  - new application being hosted on the IMA platform,
  - modification to an existing hosted application,
  - new supporting software and processing hardware,
  - a modification to existing supporting software or hardware
  - addition of new network infrastructure.
- Changes will require re-acceptance or approval by the certification authority.

Change process objectives

- **An IMA system design should address the following objectives:**
  - Minimize the impacts of an IMA system component change on the IMA system and aircraft certification as a whole.
  - Only the changed modules or applications should require re-acceptance or re-approval.
  - The main goal of the change process within the IMA system is to bound changes in such a way that their effects are known and can be fully verified and validated.
- **The specific objectives of the change process are to:**
  - Develop a change management process and coordinate it with all stakeholders. The process should identify how the various levels of developers, suppliers, integrators, and certification applicants will coordinate and address changes.
  - Perform changes using the approved change management process.
  - Conduct and document the change impact analysis.
  - Reintegrate the changed component into the IMA system. Perform all necessary verification, validation, and integration activities (regression testing) to obtain acceptance of the modified module or application and to ensure that the change has no adverse impact on affected, but unchanged modules and applications.
  - Maintain configuration control of all life cycle data related to the change

Reuse of Modules or Applications

- **Goals of reuse process:**
  - Main goal is to be able to use previously assured and accepted, module or application life cycle data with minimal need for oversight by the certification authority.
  - Reuse must be planned during the initial development process.
  - Modules are accepted with the intent of being reused in multiple systems.
- **Objectives after initial acceptance:**
  - Ensure life cycle data is unchanged from previous acceptance
  - Ensure documented limitations, assumptions, etc. are addressed in subsequent installation.
  - Perform a usage domain analysis to establish that the subsequent installation characteristics fall within the usage domain. (including V&V)
  - Evaluate any open problem reports to ensure that the they do not adversely impact safety, functionality, performance, or operations.
  - Perform integration into subsequent installation and verify its proper functionality in the IMA system.
  - Minimize need for re-evaluation of accepted modules or accepted applications.
  - Submit necessary plans and data to the certification authority and users.

IMA System Safety Assessment

- **The high level of integration requires application of ARP 4754 and ARP 4761.**
- **The process should consider the following, as a minimum:**
  - Isolation, separation, and independence to prevent interference to safety-critical functions by functions of lower failure conditions severity
  - Protection to prevent single failures and foreseeable combinations of failures that could adversely affect multiple functions simultaneously
  - A preliminary FHA should be performed at the aircraft and IMA system levels in order to assess the intended functionality, characteristics, and capabilities of the IMA architecture.
  - Examination of the architectural design and safety-related capabilities of the IMA platform and the constraints imposed on the aircraft functional allocation and hosted applications.
  - Examination of the behavioral issues of the IMA platform, including health monitoring, resource management, and fault management capabilities provided by the platform and the types of available failure recovery or containment.
  - Examination of the performance details within the IMA platform to ensure it will satisfy the performance requirements of the hosted application(s).
  - The document allocates these responsibilites to the stakeholder roles, which shall perform FHA, PSSA, SSA, Common Cause Analysis, and FMEAs for each module and at each integration level.

Summary

- This section gave an overview of the upcoming RTCA DO-297/ED-124 document „Design Guidance and Certification Considerations for Integrated Modlar Avionics (IMA)“, prepared by SC-200/WG-60.
- It has introduced the following topics:
  - the motivation for a new, modular approach to avionics system certification
  - the basic IMA certification terms and their relationships
  - the key characteristics of IMA Platforms and Applications
  - IMA Certification Tasks and required Module Acceptance Data
  - IMA Change and Reuse Requirements
  - IMA System Safety Assesment considerations
  - The Time-Triggered Architecture (TTA) as an example of a real IMA Platform