



Accelerating CNS



*Multi-Function, Multi-Mode Digital Avionics
(MMDA)
Certification Methodologies Assessment*

**ACAST Workshop
Report Presentation**

August 24, 2004



Accelerating CNS

Agenda



■ Introduction

– Study Team:

- » CNS
- » ViaSat Government System(Mike Kocin)
- » AvioniCon (Cary Spitzer)

■ SOW Tasks and Report

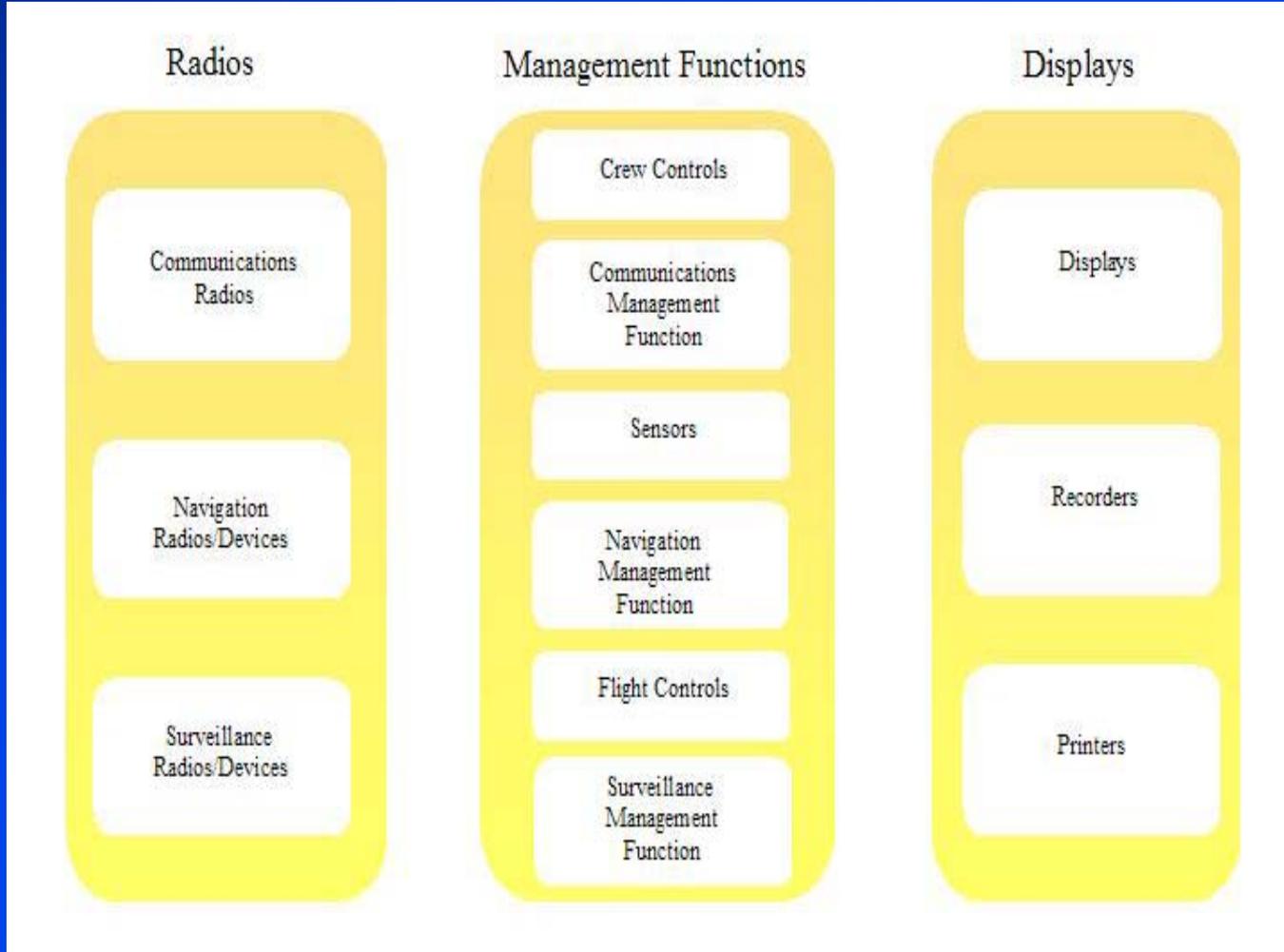
■ Recommendations

SOW and Report Roadmap

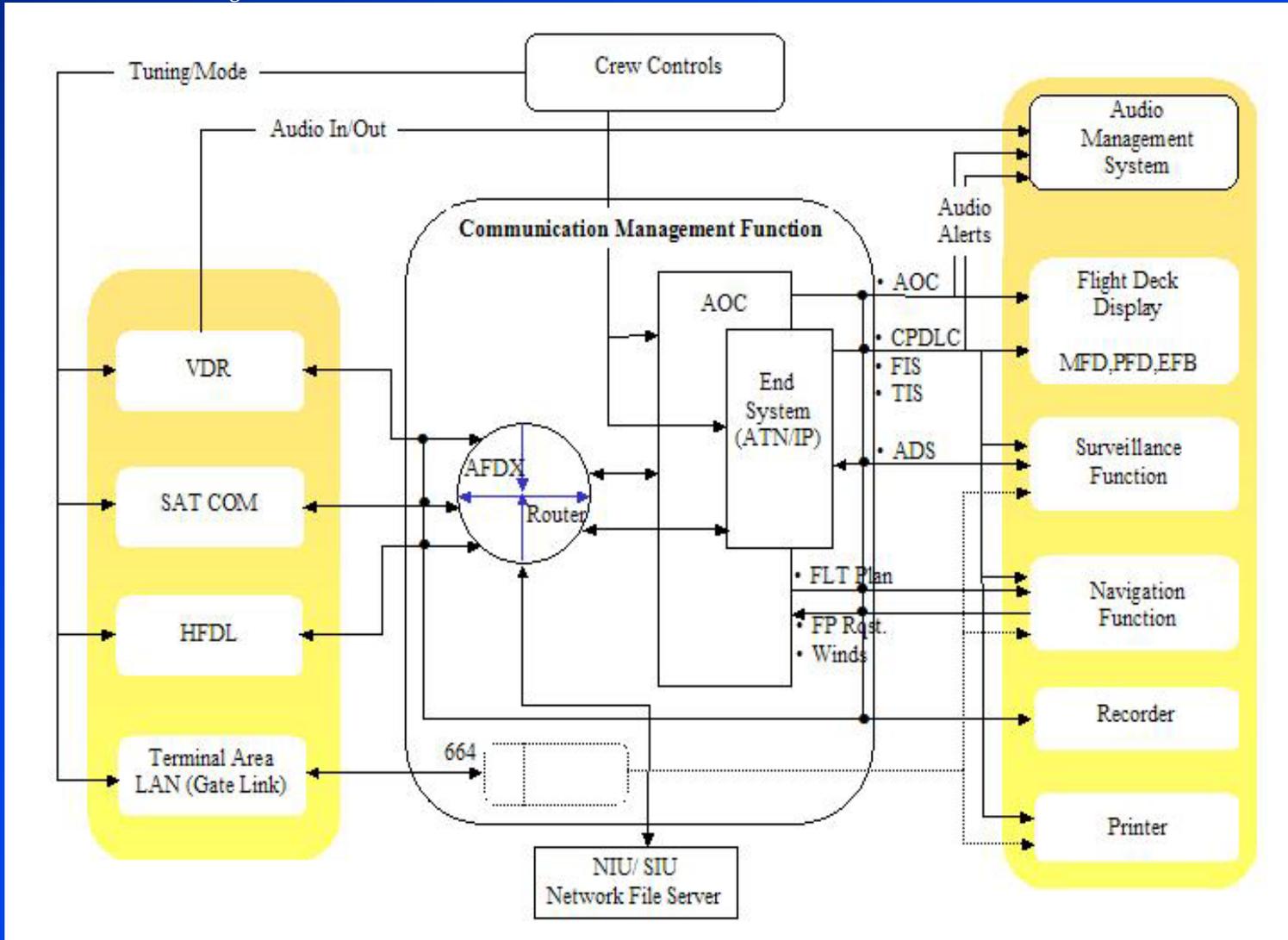
- **I. Survey and summarize certification by commercial companies [Report Task 3, 4, 5 & 6]**
- **II. Assess aspects of re-configurable avionics:**
 - Standard Software architecture and OS
 - Open Systems Standards
 - Re-usable code
 - Standard Hw platforms
 - Re-configurable or software-defined Hw/components [Report Task 2 & 7]
- **III. Assess certification aspects and NEXCOM standards [Report Task 8]**

Report Content

- **Executive Summary**
- **Survey & Assessment**
 - **Task 2: Current and Near Term CNS Architecture**
 - **Task 3: Methodologies Used for Avionics Certification**
 - **Task 4: Life-cycle Reference Model for Airborne Systems and Certification Methodologies**
 - **Task 5: Survey Companies Engaged in Producing MMDA**
 - **Task 6: Summarize Approaches to Certification**
 - **Task 7: Assessment Methodologies and Challenges to Certification**
 - **Task 8: Assessment of Avionics Compliance with NEXCOM**
- **Relevance of the IMA Development Process to the NASA MMDA Program**
 - **Standard Software architecture and OS**
 - **Open Systems Standards**
 - **Re-usable code**
 - **Standard Hw platforms**
 - **Re-configurable or software-defined Hw/components**
- **Conclusions/Recommendations**



Communication Functional Architecture



Certification Methods Reviewed



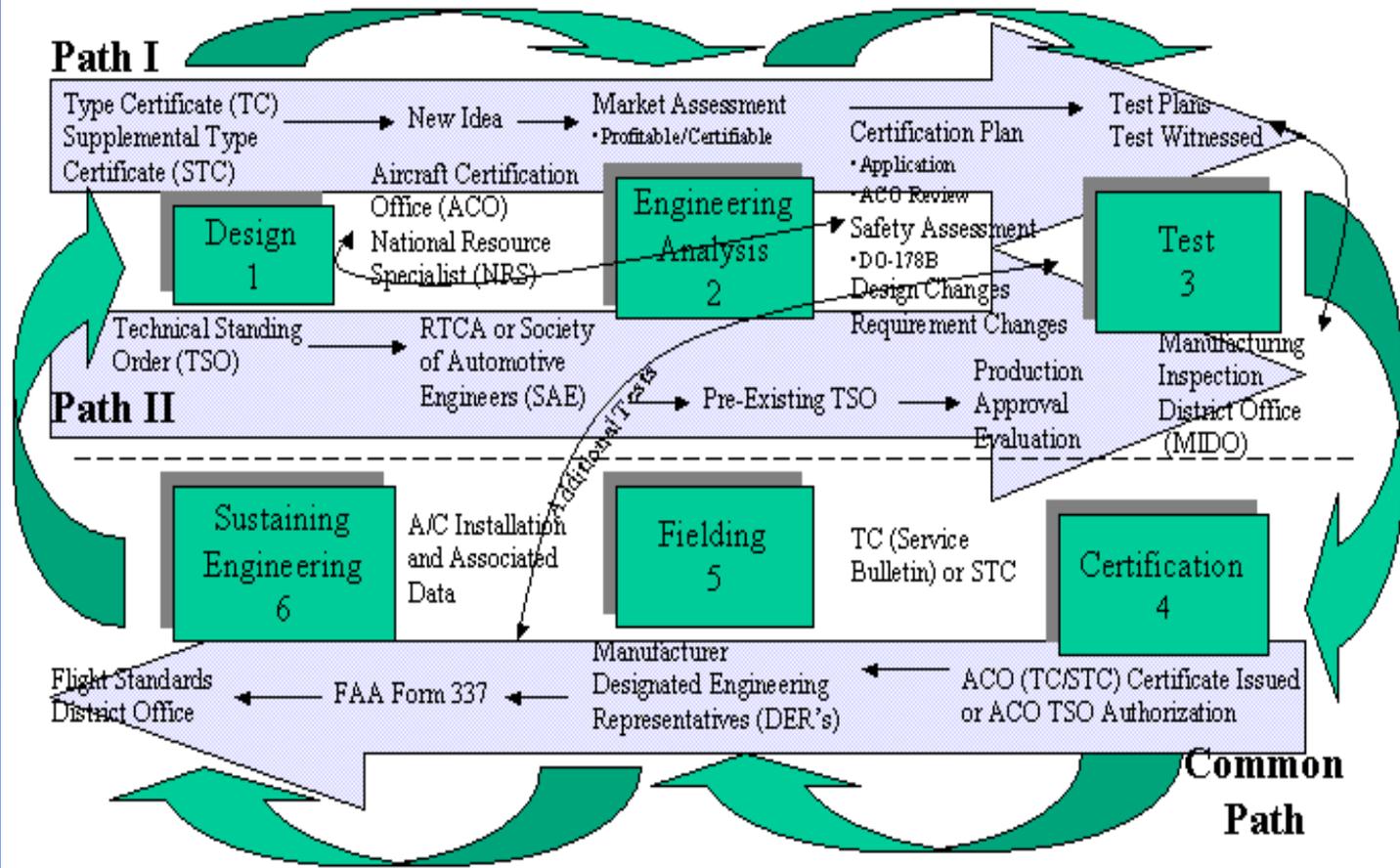
Accelerating CNS



- **Current FAA Practices**
- **Military Approaches**
- **SC-200 IMA proposed methodology**

Life-Cycle Model

Airborne Systems and Certification Methodology





Accelerating CNS

Certification Overview



- **Basis: Safety Driven = Deterministic, Reliable, Available and Performing an intended function**
- **FAR/JAR 25.1301: concept of “intended function”**
 - **1309: covers requirements for equipment, systems, and installations.**
 - » All systems included embedded system must comply.
 - » Covers performance under foreseen operating conditions
 - » Considered separately and in relationship to other systems
- **Safety assessment – functional hazard assessment defines and classifies hazards (develops fault –tree)**
- **Then software critically can be defined: not straight forward process but done on a case by case basis with FAA until consistent practice across DO-254, ARP 4751 & ARP 4761 is determined.**
- **Once criticality is defined (5-levels), the software development DO-178B is a systematic process.**
- **Process has worked for multiple processors in a system and multi-mode radio (e.g. AIMS -777) – now RTCA SC-200 is defining the methods for the simultaneously shared processor.**
- **Don’t forget DO-160 requirements**



Accelerating CNS

Survey Inputs



- **General Questions**
- **Follow-up**
- **Report contains summary of responses**

Conclusions

- There is not a “clear” path to certification of MMDA – SC-200 IMA is working to chart this path
- Individual Company processes and practices follow a range of activities as necessary to meet interpretations of FAA inspectors
- Failure to obtain early agreements on proposed certification plans can cause problems and delays
- Clear communications with the FAA are needed to establishing both the intent and use of the product
- ARINC 653 is being considered as a recommended approach by SC-200 for the IMA software architecture

Conclusions/Recommendations



Accelerating CNS



- **Provided the start of a project certification roadmap under RTCA SC-200**
- **24 recommendations**
- **Organized results into three classes**
 - **Type I. Process Class**
 - » Methodology and Procedures
 - **Type II. Systems and Components Class**
 - » Design architecture
 - » Specific aspects of hardware and software
 - **Type III. Other**
 - » Related to specific practices

Summary of Key Recommendations



Accelerating CNS



- **Develop a clear path to certification**
 - Tailor efforts to make sense under the TRL 3-6 goals.
- **Develop the higher system level architecture for the MMDA approach (needed to support functional hazard assessment)**
- **Clearly identify the intended use (needed to determine hazard levels)**
- **Develop a certification plan recognizing relevant TRL 3-6 steps**
 - Consider early discussions with FAA
 - Tailor to funding and schedule (i.e. for steps not relevant to TRL 3-6 perform analysis and do an internal review)
- **Encourage use of standards and TSO'd products**
- **Support ongoing efforts for SC-200 and other related documents upgrades**



Relevance of IMA Development Process

Accelerating CNS



Reference: NASA MMDA Program TRL 3-6

IMA Development Process	Relevance to NASA MMDA Program
1. Resource (e.g., modules and platform) development, qualification, and demonstration of compliance	Relevant for modules only.
2. Development of tools for application development, resource configuration, application configuration and integration	Not relevant
3. Development of configuration data (table) for a specific configuration load	Not relevant
4. Development and verification of software applications	Relevant.
5. Integration and verification of the individual applications on the IMA platform	Not relevant
6. Final system integration and test for each aircraft function (independent from each other)	Not relevant
7. Final system integration and test with all aircraft functions implemented at aircraft level	Not relevant

Sources Used: SC-200 draft materials

Reference: NASA MMDA Program TRL 3-6



Accelerating CNS



Detailed Steps Required to Implement IMA Development Process No. 1	Relevant.	Rel., Res. Ltd.	Optional	No
1. Plan the qualification process(es) to meet all of the applicable certification requirements.	X			
2. Develop minimum performance specifications for the module and demonstrate compliance with module requirements or specification.	X			
3. Demonstrate compliance of resource intrinsic properties, such as: time and space partitioning, determinism, latency, resource configurability, and application parameters.			X	
4. Verify compliance of resource properties with established requirements in terms of characteristics and performance, interfaces, services, safety and integrity objectives, and robustness to faults/errors.				X
5. Develop the basic software (e.g., operating system, application process interface, and core services) and hardware elements, as relevant to the module. Show compliance with the DO-178/ED-12, DO-254/	X			
6. ED-80, DO-160/ED-14, and other means of compliance, e.g., HIRF, as appropriate.				
7. Develop and make available the module qualification data for certification authority approval.				X
8. Provide users of the module with sufficient information to properly integrate and interface the module to the platform and system, e.g., user's guidelines and module data sheet.				X
9. If the module is a platform, integrate modules and components.			X	
10. Qualify verification and development tools, i.e., tools used to automate or replace some aspect of the module qualification effort, as needed.				X
11. Implement quality assurance, configuration management, integration, validation, verification, and certification liaison for the module qualification.			X	
12. Manage the configuration of the module so that correct applicability of the version of the module is assured. User data should include module configuration applicability information (e.g., part number, version number). Modules should contain a means for the users to determine configuration (e.g., physical part number, electronic part number / version, software identifiers)			X	

Sources Used: SC-200 draft materials



Accelerating CNS

Contact Information



Computer Networks & Software, Inc.

7405 Alban Station Ct., Suite B-215
Springfield, VA 22150
703.644.2103
www.CNSw.com

Chris Wargo
443.994.6137 (cell)
chris.wargo@CNSw.com

ViaSAT Government Systems

6155 El Camino Real
Carlsbad, CA 92009
760) 476-2200
www.ViaSat.com

Mike Kocin
760.476.2342
mike.kocin@viasat.com

AvioniCon

3409 Foxridge Road
Williamsburg, VA 23188

Cary Spitzer
757.221.8031
cspitzer@avionicom.com



Accelerating CNS

Specific Topics



- **Standard Software architecture and OS**
- **Open Systems Standards**
- **Re-usable code**
- **Standard Hw platforms**
- **Re-configurable or software-defined Hw/components**

Type I Process - Recommendations



Accelerating CNS



- **1. The development of a MMDA under the ACAST project should be accompanied by a developed certification plan. The plan would conform to RTCA SC-200 IMA and would specify certification activities to be performed, partially performed or deferred.**
- **2. NASA should support the finishing of the RTCA SC-200 IMA committee task.**
- **3. NASA GRC may consider the training of a GRC DER.**
- **4. Although additional investigation is required, NASA GRC could develop additional product design and software development productivity tools related to the certification process.**
- **5. NASA could foster additional research to establish a “ISO-9001 like” company certification approval process. Then the FAA would focus on test results and flight testing .**

Type II Systems and Components Class -1/4



Accelerating CNS



- **1. For any MMDA certification planning to proceed a higher level avionics architecture needs to be understood.**
- **2. NASA could sponsor, develop and furnish additional “qualified” or TSO’ed components.**
- **3. NASA GRC should support the upcoming revision of DO-178D (178C – Early 2005)**
- **4. NASA GRC could support the revision of ARP 4754 and ARP 4761**
- **4. NASA should support the update of ARINC 653-3 currently underway**

Type II Systems and Components Class – 2/4



Accelerating CNS



- **5. Specific to Standard Software Architectures and Operating Systems:**
 - NASA could develop a plan to build a library of technology modules for MMDA insertion
 - NASA could develop an industry certified platform/operating system
 - Develop a level of critically for MMDA components
 - Develop the MMDA architecture certification plan
- **6. Specific to Open software standards:**
 - Use Open Standard Application Programming Interface (API) tailored for specifics
 - » IEEE POSIX 1003.1-2001
 - » ARINC 653-2
 - Linux can be used if security enhancements are made
 - OpenGL used in certified ground systems but unknown use in avionics systems?

Type II Systems and Components Class – 2/4



Accelerating CNS



- **7. Specific Software Re-use:**
 - The use of C++ Object Oriented Programming is acceptable depending on source code compiler
 - Participate in FAA/NASA-LaRC “Object Oriented Technology in Aviation (OOTiA)” project
 - Establish Software Libraries and Tool Qualification data
 - Develop Configuration Items, software plans and standards

- **8. Specific to standard hardware platforms**
 - Cost factors determine hardware selection as well as MMDA type identification
 - Use IMA approach where CPU has specific traits suitable for certifying (example: Apple OS 7 type hardware)
 - Or, Develop portable and extensible hardware platform

Type II Systems and Components Class – 2/4



Accelerating CNS



- **9. Specific to reconfigurable or software defined hardware/components**
 - **Develop waveforms for MMDA**
 - **Develop Configuration program for hardware lifecycle**
 - **Develop architecture and certification plan for hardware**
 - **Insure architecture is expandable and portable**