SAE Aerospace
An SAE International Group

AEROSPACE INFORMATION REPORT

AIR4366	REV. A
Issued 1996-05	
Cancelled 2007-08	
Superseding AIR4366	

Issues and Concerns Associated with Electronic Propulsion Control System Partitioning

RATIONALE

The AIR4366 subject material has been superseded by another standard work produced by the RTCA SC200 which has now published D0-297. An assessment of the content of AIR4366 against DO 297 was made and summarized in a matrix, see attachment 08.air4366 from the September 06 meeting. Quoting from the September 06 minutes, “The matrix shows what each of the documents is trying to achieve and then provides a comparison between them. ……. in the vast majority of areas, the SC200 document covers all points contained with the AIR in a more detailed and robust manner.” In would be a pointless exercise to update the AIR4366 since a much more comprehensive document already exists, hence it is suggested that AIR4366 be cancelled.

CANCELLATION NOTICE

The document has been declared "CANCELLED" as of August 2007. By this action, this document will remain listed in the Numerical Section of the Aerospace Standards Index.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

SAE Aerospace
An SAE International Group

AEROSPACE INFORMATION REPORT

AIR4366	REV. A

Issued 1996-05
Cancelled 2007-08

Superseding AIR4366

Issues and Concerns Associated with Electronic Propulsion Control System Partitioning

FOREWORD

Traditionally engine controls have been a dedicated part of an engine. The interfaces between the engine controls and the airframe have been straight forward, generally consisting of throttle linkage, fuel lines, and electrical connectors.

As technology has progressed, electronic controls have supplanted hydromechanical systems. Control system logic has become more sophisticated, and engine-airframe interfaces for an optimum system are no longer clearly evident. Distributed systems, in which "the propulsion control" is no longer an identifiable entity, are now possible and may offer significant advantages in aircraft performance, cost, weight, reliability, etc., for some applications.

This AIR, prepared by the Electronic Engine Control Committee's Panel on System Partitioning, is not intended to discourage the distribution or partitioning of propulsion control systems, but rather to ensure that all the issues are properly considered to avoid new and perhaps subtle problems which may lie ahead.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

TABLE OF CONTENTS

1. SCOPE 3

2. REFERENCES 3

2.1 Military Publication 3
2.2 FAR Publications 3
2.3 ARINC Publication 3

3. ISSUES AND CONCERNS 3

3.1 System Definition and Design 4
3.1.1 System Requirements 4
3.1.2 Conceptual Design 5
3.2 Development 6
3.2.1 Sequence and Scheduling 7
3.2.2 Component Design 8
3.2.3 System Validation 9
3.3 Certification/Qualification 9
3.3.1 Certification Plan 9
3.3.2 Test Definition 10
3.4 Configuration Control 10
3.4.1 Responsibilities 10
3.4.2 Software 11
3.4.3 Hardware 11
3.5 Maintainability/Support 12
3.5.1 Fault Isolation 12
3.5.2 Test Equipment 13
3.5.3 Support Personnel 13
3.5.4 In-Service Problems 13
3.6 Warranty and Liability 14

4. SUMMARY 14

1. SCOPE:

This SAE Aerospace Information Report (AIR) enumerates areas of concern which need to be addressed when the aircraft propulsion control system functions are distributed. Distributed items may include electronic control sensors, electrical or hydraulic power sources, computer hardware and software, etc. This report identifies many factors which should be considered to determine the best system architecture for any given application.

2. REFERENCES:

2.1 U.S. Government Publication:

Available from DODSSP, Subscription Services Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.

MIL-STD-1553B

2.2 FAR Publications:

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591.

FAR 23
FAR 25
FAR 27
FAR 29
FAR 33

2.3 ARINC Publication:

Available from Aeronautical Radio, Inc., 2551 Riva Road, Annapolis, MD 21401.

ARINC 629

3. ISSUES AND CONCERNS:

The topics contained in the main body of this report are labeled "Issues and Concerns". They represent those items which, as seen by the engine control community, can present problems if not properly addressed up front. They are by no means considered insurmountable obstacles, and offer great opportunities for cooperative, creative solutions to the technical challenge.

The main body is organized to follow the flow of a program. It begins with (1) system definition and design, followed by (2) development, (3) certification/qualification, and finally addresses (4) configuration control, (5) maintainability/supportability, and (6) warranty/liability issues. However, it is important that all issues be addressed in the system definition phase.

3. (Continued):

A propulsion control system consists of those components such as sensors, control units, actuators, and computation means which maintain the commanded level of propulsive performance provided to the airframe by the engines.

3.1 System Definition and Design:

Presented within this section are general considerations which should be addressed as partitioning of the propulsion control system is defined. Although top level requirements are not influenced by partitioning, subsystem requirements and interface definitions take on new significance depending upon system configuration.

3.1.1 System Requirements: System requirements must be defined which specify system performance that is necessary to achieve real-time execution of control algorithms for the control of fuel flow, stator vanes, bleeds, and other variable geometry. Consideration should also be given to requirements for additional secondary functions, such as engine condition monitoring, instrumentation, and other data.

System performance should be defined in terms of the dynamic response and accuracy required from the various elements of the control system - input commands, sensors, computers, actuators. These requirements will in turn lead to the definition of additional requirements regarding computational cycle times, data update rates, etc.

Criticality of control system functions dictate the system reliability and safety requirements. Based on these requirements, needs for fault tolerance will be developed, including possible redundancy of sensors, computational resources and actuation systems. Consideration must be given to the level(s) of redundancy - dual, triple, quad, dual-dual, etc. System redundancy can result from communication of data between computers. An important consideration is the provisions made for redundant sources of electrical power, to ensure continuity of supply to achieve specified requirements.

System integration and resource sharing must be partitioned in such a manner as to maintain independence between engines in multi-engine applications in order to prevent faults from propagating between engines.

Failure modes of the control system should be defined in terms of observable end results, e.g.:

a. No observable effect for a single failure

b. Fail fixed

c. Fail to a predefined condition

d. No large uncontrolled thrust or power changes

3.1.1 (Continued):

Control system design should minimize the effects of and/or provide graceful failures consistent with system requirements for major, hazardous, or catastrophic events including, but not limited to:

a. Loss of all communication between the engine and aircraft

b. Total loss of electrical power

c. Common mode failures

3.1.2 Conceptual Design: In the conceptual design stage, system requirements are allocated to the specific elements of the propulsion control system.

Some concerns in system partitioning which must be addressed during conceptual design are:

a. Preliminary definition of system performance requirements at the selected interfaces.

b. Ability to define and test subsystem performance.

c. Ability to isolate and troubleshoot system/subsystem performance.

d. Method of computation/communication.

e. Means of providing system and subsystem built-in-test.

f. Allocation of reliability, weight, size, and power.

g. System performance and/or cost benefits from shared hardware or data.

h. Determination of environmental requirements.

i. Dedicated or shared (with nonpropulsion control system) computer resources.

j. Central or distributed processing.

k. On versus off engine mounting - thermal, vibration, EMI, and lightning, plus EMP and radiation hardening in some military applications.

l. Data bus structures and communication rates between computers.

m. Software design to separate propulsion control from other functions in a distributed system.

n. Life cycle cost, including testability and maintainability.

o. Dynamic system interactions.

3.1.2 (Continued):

Allocation of dedicated sensors and actuators is often self-evident from the system requirements. However, an important consideration may be whether the system is to use dedicated sensors, or to derive signals such as air temperature, altitude, airspeed, etc., from another aircraft system.

Similar considerations may apply to input command signals from the airframe - dedicated hard-wired inputs to the propulsion control system, or supplied from other equipment via the data bus.

In fact, all shared resources must be identified and a plan developed, at the integrator level, to detect and avoid resource contention. Within an integrated system, examples would be real time usage and memory, if the CPU is to be shared between subsystem tasks, as well as communication bus bandwidth.

At this stage of the design, fundamental decisions about software need to be made, such as the degree to which different levels of software criticality will be integrated or segregated.

In establishing the system conceptual design, all pertinent parties should be involved as early as possible. In the initial design stage, the airframe and engine manufacturer must obviously be involved, and so may the end user. However, as soon as possible, the manufacturers of major elements of the various control systems also need to be included, to get the benefit of their particular expertise. Flexibility in partitioning decisions should be maintained until the inputs of all parties have been considered. Arbitrary definition of partitioning and interfaces can result in compromised performance and excessive system costs.

The design task is complex, requiring total understanding of the interface between functional blocks. Systems built from components supplied by different vendors are prone to greater development problems. More planning, coordination, and emphasis on interface definition in the early design phase can minimize these problems, as can early simulations and analysis. In any event, "firm" interface documents are required early.

3.2 Development:

Conventional approaches to development of engine control systems result in a development program for the control that is relatively independent of outside influences. In other words, there is often little interaction other than between the engine manufacturer and the control system supplier. As the control system is partitioned, both in hardware and software, the approach to a development program may require modification. The development program must be tailored to the degree of partitioning of the systems under design. Hence, the degree and method of system partitioning will influence not only the approach to development, but also the relationship of the participants. This can vary from a conventional relationship to one requiring much greater communication and coordination of development program efforts.

3.2.1 Sequence and Scheduling: The sequence and the schedule of a development program for a partitioned control system can require special attention. In general a top-down approach to the development cycle will be necessary, which may not substantially differ from the conventional approach at the prime contractor level. However, it will be necessary, dependent on the method of partitioning the system, to involve subtier contractors at an early point in the program. Open communication between several levels of contractors may be appropriate to define system issues and approaches. Since this approach requires early identification of suppliers, such a level of cooperation may be required even in the proposal stage.

Analysis - During any development program several analyses may be required. Generally they can be limited in scope to relatively independent components. Such analyses then address just those components, with propulsion system concerns addressed by the propulsion system supplier. In the case of a partitioned control system, the component supplier will provide definitive analyses of his component, and there will likely be a migration upward of system level analysis responsibility. It is conceivable that responsibility for complete analysis results will fall on the system integrator, with supporting analyses from subtier contractors. The following points should be considered:

a. Analyses should be defined early in the program.

b. Reliability failure analysis and dynamic performance simulations must be included.

c. Related and supporting efforts required of different contractors for analyses must be defined.

d. Areas of communication required between analysis contractors must be defined and accommodated.

Test - Development program test requirements must be defined at an early stage in any program; however, with a partitioned system approach this is more critical. the test program may involve components that cannot be tested as stand-alone units, thus requiring supporting test equipment not common in conventional programs. In the case of control software installed outside the unit under test, a means of providing that software function must be available for the test. This may require definition of test support hardware in which to install that software and thus the external functions.

Interface - When the system design is implemented in a partitioned manner the definition of subsystem and/or component requirements becomes more critical. Of particular concern is the appropriate definition of the interface between these and other portions of the system. Since the unit by design may not be a "stand alone" unit, the interface definition will require consideration of the interaction of the unit and the overall system. Thus the interface definition may, in addition to being a performance specification, include a partial definition of related components or systems. This presents a complication of the definition and configuration control processes.

3.2.1 (Continued):

Since all proper hardware will likely not be available when "needed", there is a risk of having to repeat development tests or make system modifications/design changes to accommodate differences when proper hardware/software becomes available. This can be a further complication to program scheduling.

3.2.2 Component Design: Component design in a partitioned system will proceed in a relatively conventional manner. Given an adequate definition of the design requirements, including the interface and test requirements mentioned, no major changes will be called for in the design approach. However, if in the design process alterations must be addressed, communication of the required alterations and update of the respective documents will be a more complicated undertaking. The interface definition documents will likely be more complex with a partitioned system. This will require attention to the following:

a. Cooperative efforts among all parties to adequately define the system interface requirements.

b. Negotiation at an early stage of development of areas involving interface requirements. These areas may be impossible to resolve without the involvement of all participants in the program.

c. A more complex specification required to relate the interface requirements to the necessary participants. In fact, a new tier of Industry Standards may be needed to accommodate partitioned systems.

(Business issues, which also may be quite complex, are not addressed in this document.)

Update of these interface documents will be particularly critical, and more complicated due to the increased complexity of the requirements. Interface changes can have major impacts on component or subsystem design. Key issues will be similar to those related above, with timely communication of updates most important.

During the design process, with a partitioned system, items of information supporting higher system level analyses may not be available until the design process is underway. It is expected that this will be more frequent in a partitioned system, and may even require a cooperative effort for certain types of analyses. Although this has been the convention for reliability (and similarly approached) analyses, many engineering analyses will also require such an approach. The means and schedule for communicating this information should be defined early in the development program.

3.2.3 System Validation: Particular concerns at the system level relate mainly to the resolution of difficulties that arise during the test program. In a partitioned system, operations during a test may involve several (no longer independent) subsystems or components. The system level test plan should address the means of resolving items in contention or lack of availability of proper hardware. This may take the form of further involvement of subcontractors during the test, provision for development test support equipment sufficient to determine where the difficulty lies, etc.

Simulations required are a challenge similar to analyses in a partitioned design situation. For conventional simulation needs, it may be necessary to communicate data relating to the simulation at an earlier stage, or at least in a form more complex than normal, since there may be greater interdependence between subsystems. This can produce both technical and data rights problems. Another concern in a partitioned system is that simulation may become necessary to achieve appropriate design verification/validation where hardware is unavailable when needed.

3.3 Certification/Qualification:

Conventionally a propulsion control system is shown to comply with the appropriate engine certification requirements, e.g., FAR 33, and the aircraft manufacturer will use data and analyses from the engine manufacturer in order to satisfy the appropriate sections of the aircraft certification requirements, e.g., FAR 23, 25, 27, or 29. Where sections of the engine control are located or integrated with the aircraft system, special attention should be given to the impact of those function/hardware aspects on certification. This could be affected by indirect effects and by reliance on a specific hardware standard not necessarily procured by the engine manufacturer. In fact, it is probable that some significant changes to the current method of certifying engines would be necessary.

The following points should be considered relative to certification.

3.3.1 Certification Plan: The initial issue to be addressed is whether it is necessary to certificate on the basis of a unique engine/aircraft combination or whether a generic engine can be certificated with a propulsion control system which is functionally representative of a system to be provided in the final application. The tasks for the certification of a propulsion control system may be shared between the engine and the aircraft manufacturer. The certification plan should identify the distribution and responsibilities for these tasks including the definition of the physical and functional interfaces.

Where a function of the propulsion control system resides in another piece of equipment, the scope and responsibilities of all applicable analyses, including all dispatch limitations, should be defined. In particular: the interface definition, the behavior under abnormal conditions, and how the possibility of common mode failures should be addressed.

3.3.1 (Continued):

Documentation is a vital part of the design and certification process and a clear division of the documentation responsibility needs to be established. Software documentation should follow the requirements presented in RTCA document DO178B.

Where changes are made to equipment performing multiple tasks, procedures should be established to ensure that the certification standard of apparently unrelated functions is protected. In particular, specific procedures must ensure that changes in one area cannot change form, fit, function, or logistics of any other area without invoking the full change procedures for all the applicable tasks/functions.

3.3.2 Test Definition: The test configuration must include all aspects associated with partitioning to ensure that the design requirements are demonstrated to be valid over the whole operating envelope. For example, failures of those elements not forming part of the propulsion control system must be shown to have no adverse effect.

Testing conventionally follows a process of design verification and validation through rigs, engine tests, and flight tests. Each of these processes needs to be carefully assessed relative to the hardware used and the relevance/applicability of the results. The hardware may range from:

a. Emulations

b. Functionally equivalent unit

c. Production standard hardware for the applicable partitioned functions excluding the rest of the partitioned unit

d. The complete production standard hardware unit which may embrace those functions not directly associated with engine control

3.4 Configuration Control:

During the lifetime of an aircraft, its systems undergo changes either as a result of the discovery and correction of unwanted interactions or as the result of efforts to improve the operational efficiency. The control and identification of these changes has implications both for safety and for logistics support of the fleet. If a partitioned control system includes the use of a common computing resource for several subsystems, important new issues are raised concerning configuration control.

3.4.1 Responsibilities: In the past, the responsibility, costs, and liability for configuration control have been distributed amongst the various manufacturers of LRU's. Class 1 and Class 2 changes were implemented and tested independently with little concern for interaction except at the system level.

3.4.1 (Continued):

Distribution of control results in the migration of responsibility for configuration control from subsystem manufacturers to the airframer. This will be the case if the airframers choose to become subsystem integrators. Even if the subsystem supplier implements his/her controls with standardized modules, configuration control will fall to the airframer if these modules are subsequently integrated into a centralized computing resource. For any change in a system using a common computing resource, configuration control must include system design methodologies which insure that each subsystem retains its critical computer resources, namely real time and input/output resources. Accidental contention for output resources between unrelated subsystems could result in unsafe conditions or premature wear out of mechanical systems.

Both airframers and end users must have the configuration control mechanisms in place to address these challenges.

3.4.2 Software: Software partitioning and configuration control are significant concerns if a common computing resource is used for multiple subsystems. Adequate software partitioning is required to avoid costly recertification of all software when software for one subsystem is updated. This is especially true if memory boundaries are moved, forcing the recompilation of all code.

Design tools are a possible solution to ensure sufficient software partitioning. This would reduce human error in the change process but would require rigorous validation of the design tools. The generation of software must offer ways of:

a. Enforcing strict control of intersystem communication

b. Certifying the effects of recompilation on unrelated code

c. Accurately predicting real time usage between subsystems under worst case conditions

d. "Top-down" or "specification to implementation" method for code generation

e. Automatically identifying resource contention and real time overflow and scaling conditions

Software configuration control should be integrated into the heart of these design methodologies. Configuration control would have to take into account the possibility of the permutations of various configurations of subsystems.

3.4.3 Hardware: Hardware configuration control for common computing resource systems is not unlike that of the current LRU systems except for the increased potential for unplanned intersystem interactions.