The Engineering Society For Advancing Mobility Land Sea Air and Space®
INTERNATIONAL
400 Commonwealth Drive, Warrendale, PA 15096-0001

AEROSPACE RECOMMENDED PRACTICE

SAE ARP4714

Issued 1999-10

External Software Loading of Electronic Engine Controls

FOREWORD

Advances in electronic memory technology have now made available electrically alterable memories, suitable for use in aircraft electronic engine controls (EEC), whereby software can be loaded without disassembly of the control box. This is most commonly done using a serial data link to the EEC processor to alter the memory in the EEC. The ability to change engine control software provides economic benefits throughout the service life of a program, but it should be firmly controlled. For the reader not conversant with the equipment necessary for external software loading, a brief summary can be found in Appendix A.

TABLE OF CONTENTS

QUESTIONS REGARDING THIS DOCUMENT: (724) 772-8510 FAX: (724) 776-0243
TO PLACE A DOCUMENT ORDER: (724) 776-4970 FAX: (724) 776-0790
SAE WEB ADDRESS: http://www.sae.org

TABLE OF CONTENTS (Continued)

1. SCOPE:

This paper presents guidelines for development of a procedure for external software loading of an electronic engine control (EEC) for a commercial application, on-wing or in a qualified service shop. This paper makes the following assumptions:

a. The EEC is designed to accept external software loading.

b. The EEC is certified as part of an engine.

c. The support equipment is qualified in accordance with procedures set forth by the engine (and aircraft, if necessary) certifying authority if the EEC cannot detect an integrity violation of the loaded program.

d. The software to be loaded has been approved by the engine and aircraft certifying authorities.

e. One or more configurations of EEC hardware has been identified for each version of software which is to be loaded in the EEC.

It is appropriate to use these guidelines in the initial development phase, although the certification issues would not be applicable.

Approval as used herein means approval by the engine (and aircraft, if necessary) certifying authority. There are cases where the engine may commence certification activities and no specific aircraft application has been identified. In these cases, the aircraft certification authority should be notified of the EEC's external software loading capability when the engine's application is identified. The appropriate documentation can be delivered to the aircraft certifying authority at that time.

2. REFERENCES:

RTCA/DO-178B Software Considerations in Airborne Systems and Equipment Certification
ARINC Report 615.2 Airborne Computer High Speed Data Loader

3. TECHNICAL REQUIREMENTS:

All systems dealing with the loading of software should comply with section 2.5 of RTCA/DO-178B.

3.1 Configuration Compatibility:

All software loading should comply with RTCA/DO-178B, section 2.5.C.

3.2 Protection:

3.2.1 Mode Protection: When the software can be externally altered, then an approved interlock system should be used to prevent potential inadvertent changes from either internal or external causes. These interlocks may be internal or external.

3.2.2 Permanent EEC Memory Protection: Means should be provided to assure any memory location not intended to be modified by the external load is protected from corruption.

3.2.2.1 Loader Kernel Protection: If the software load is to be supported/controlled by the EEC processor, then means are required to protect the resident loader kernel.

3.2.2.2 Partitioned Memory Loading: If the software load is intended to modify only specified partitioned memory locations, then means are required to detect corruption of all other memory locations not included in the intended partition.

3.2.3 Protection of Loadable Software: These should be the same means to prevent unauthorized modification or alterations to loadable software. This may be in the form of proper paperwork, such as an approved Service Bulletin (SB) (see Section 5).

3.3 Support Equipment:

If support equipment can contribute to an undetected corruption of the software load, then the support equipment should be qualified to the same level (or better) of any software that is to be loaded. The following items should be considered:

3.3.1 Test: The support equipment design should be qualified and the support equipment should be subjected to the required degree of qualification testing in accordance with the approved certification planning document. The degree of qualification will be a function of the types of error that could be introduced by the support equipment and the procedures associated with the loading. In other words, the "procedures" can be part of the validation process that assures that the proper EEC software was loaded.

3.3.2 Verification After Software Load: The software loaded into the EEC requires proof of integrity. An approved method should be used after any software load to ensure the software content of the EEC conforms to the approved software version being loaded. There should be a means to provide an indication of the successful verification of the software load.

4. CONFIGURATION CONTROL:

All elements involved in facilitating the software load, including the load procedure, should be under configuration control. This could include support equipment and its software routines.

4.1 Traceability:

4.1.1 Labeling: The new software should have an integrated “label” resident in its code to aid load verification and to provide configuration information to be read on subsequent EEC interrogations. Any checks carried out after software loading and during usual EEC power-ups should indicate label corruption.

4.1.2 Records: The configuration change should be recorded in accordance with approved quality control and configuration management procedures.

4.1.3 Change Authority: Traceable authorizing documentation should be issued prior to commencing a software load. This documentation should be approved by the engine (and aircraft, if necessary) certifying authority. Acceptable combinations of hardware and software should be identified in this document to ensure compatibility.

5. CERTIFICATION:

The use of software data loading should be identified to the appropriate engine (and aircraft, if necessary) certifying authority during the development process, using the software lifecycle data required by RTCA/DO-178B (section 11) for approval. DO-178B requires the following documents to be submitted/made available for review:

5.1 Plan for Software Aspects of Certification:

This document should be used as the initial document notifying the engine (and aircraft, if necessary) certifying authority of the plan for use of software loading capability in the engine design, and is required by DO-178B to be delivered to the engine (and aircraft, if necessary) certifying authority for approval at the beginning of the engine development. It outlines the design, development, and test techniques planned.

5.2 System Requirements:

The EEC system requirements document should include the specific requirements applicable to the capability for software loading. This document should also include a description of the intended implementation of the features required for software loading, a description of the proposed procedures, and required support equipment.

5.3 Configuration Management and Software Quality Assurance Plans:

The Configuration Management Plan should include the configuration identification, configuration control, and audit procedures planned to be used during design, development, and test for the loadable software and the support software. Separate part numbers for the hardware and software are acceptable.

The Quality Assurance Plan should include any particular quality assurance procedures associated with software loading. In addition, reviews and audits should be conducted as outlined in the Configuration Management or Quality Assurance Plan to ensure adherence to configuration control requirements.

5.4 Software Test Plan, Procedures, and Results:

These data items should include the details of the test plans, procedures, and results, particularly defining the testing assurance schemes associated with software loading capability. The purpose of this is to assure noninterference and protection against corruption of data in any unintended areas.

5.5 Accomplishment Summary:

This document should outline the specific design, development, and test tasks accomplished during the program including aspects particular to software loading.

5.6 Configuration Index:

The Configuration Index reflects the part numbering scheme for the software loading capability.

5.7 Service Bulletin:

Typically a Service Bulletin (SB) is used as the change authority for the software loading of the EEC. The SB should describe the detailed software load process. Approval by the engine (and aircraft, if necessary) certifying authority is required. Configuration information should be included in the SB to indicate the acceptable software, hardware, and engine/aircraft configuration items if required.

6. NOTES:

6.1 Key Words:

EEC, external, programming, support

PREPARED BY SAE COMMITTEE E-36, ELECTRONIC ENGINE CONTROLS

APPENDIX A
TYPICAL EXTERNAL SOFTWARE LOADING BACKGROUND

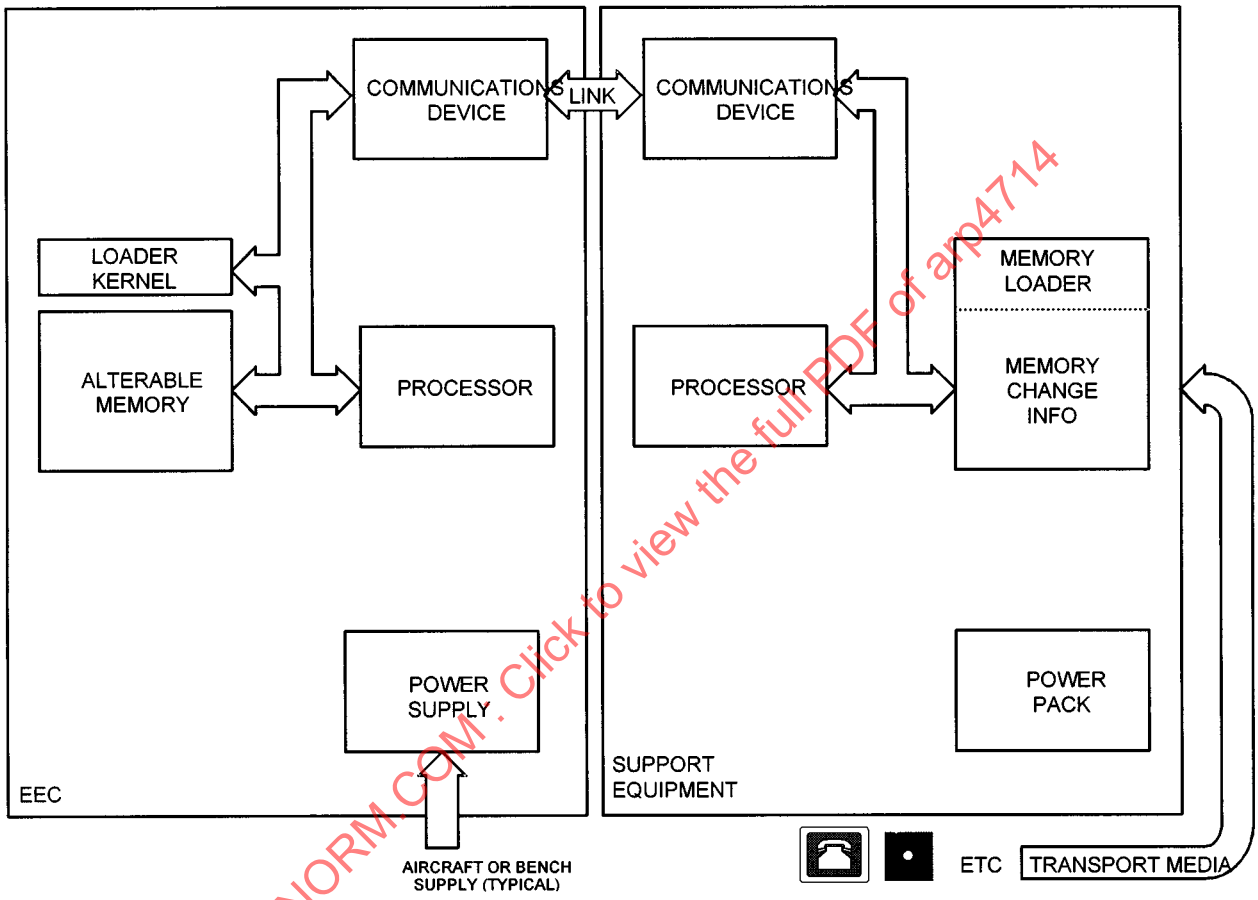

FIGURE A1 - External Loading Block Diagram

A.1 EEC:

A.1.1 Communication Device:

The EEC resident communication device allows external communication with the EEC's internal CPU bus. The device also provides the appropriate degree of isolation from the external support equipment.