



Procedures and Guidelines

DIRECTIVE NO. 573-PG-8700.2.2
EFFECTIVE DATE: 08/27/1998
EXPIRATION DATE: 08/27/2003

APPROVED BY Signature: original signed by
NAME: John Deily
TITLE: Branch Head

Responsible Office: 570/Guidance, Navigation, and Control Center

Title: Design of Flight Component Embedded Software

1 PURPOSE

This procedure establishes guidelines for the design of Guidance Navigation and Control (GN&C) component embedded software for space flight use. Employees will use this process in support of the design, verification, and review of GSFC products.

2 REFERENCE

GPG 8730.4, The GSFC Quality Manual
GPG 8700.1, Design Planning and Interface Management
GPG 8700.2, Design Development and Configuration Control
GPG 8700.3, Design Validation
GPG 8700.4, Technical Review Program
570 8700.2.4, Design of Non-Flight Embedded S/W
570 8700.2.5, Analytical Design of S/C Missions
570 8700.3.5, GN&C Component Verification Testing
570 8700.2.6, Analytical Design of sub-Orbital Missions
570 8700.2.7, Design of S/C Propulsion Systems

3 SCOPE

This procedure defines the guidelines for the design of Flight GN&C Component Embedded Software. These guidelines apply to any Product Design Team members providing spaceflight embedded software support to GN&C projects covered by the scope of the GSFC Quality Management System.

4 DEFINITIONS

- 4.1 Flight Component Embedded Software includes software at the circuit board and box levels. This includes any of the following modules: operating system software, software bus, memory management, data storage, housekeeping, scheduling, task management, failure detection and handling, command and interface software, telemetry, models, serial I/O, and math libraries. These components are defined below. This software is intended to be used in or beyond earth orbit: either on attached/free-flying shuttle missions, on attached/free-flying space station missions, or on expendable launch vehicle missions. The term does not refer to ground embedded software.
- 4.2 Operating System Software includes processor and peripheral hardware initialization, processor exceptions, processor interrupts, and processor mode transitions and logging.
- 4.3 The Software Bus is a layer of software that provides communication between the operating system and other system processes.
- 4.4 Memory Management includes memory reads, memory writes, and calculating memory checksum data.
- 4.5 Data Storage involves sending packets of data to memory for caching purposes.
- 4.6 Housekeeping includes data collection, monitoring events, and watchdog circuitry.
- 4.7 The Scheduling software is responsible for coordinating the run sequence of all events.
- 4.8 Task Management administers, supervises, and regulates all system tasks.
- 4.9 Failure Detection and Handling controls the detection of and automatic actions in response to system exceptions.
- 4.10 Command and Interface software handles reading and sending commands to the appropriate system destination.
- 4.11 Telemetry software includes all software responsible for the collection and downlink of telemetry.
- 4.12 The Models software propagates standard or custom models specific to the system.
- 4.13 Serial I/O is responsible for the interfacing between internal and external devices contained within the system.
- 4.14 The Math Library includes any math routines.

5 AUTHORITIES & RESPONSIBILITIES

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov/gdms> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

- 5.1 AETD Employees: All AETD employees are responsible for adherence to this procedure.
- 5.2 Product Design Lead: Because many steps of this procedure are noted as being optional, it is the responsibility of the Product Design Lead, in partnership with the customer, to determine and document in the design plan (see GPG 8700.1 and GPG 8700.2) which specific steps will be executed. Furthermore, guidelines contained herein may be waived at the discretion of the Product Design Lead and the customer due to extenuating circumstances such as limitation on time and/or resources, or by customer request. These procedures may also be waived in favor of existing contractor ISO 9000 procedures. Such waivers must be documented.

6 IMPLEMENTATION

Note: All procedure steps are the responsibility of the Product Design Lead unless stated otherwise. The implementation procedures in sections 6.3 through 6.9 will normally be repeated iteratively, as needed, to support the design plan. This list is not intended to represent a required order of execution.

6.1 Requirements Definition

Generate a mutual understanding between the project, users, designers, and customer of the initial definition of the software to be developed. Agree on the requirements with the customer and generate a written requirements document.

6.2 Initial Planning

- 6.2.1 The Product Design Lead ensures that the Product Design Team is composed of individuals, both civil servants and contractors, with the required discipline skills.
- 6.2.2 Identify high-risk items and develop a risk mitigation plan (optional, per design plan).
- 6.2.3 Identify any long lead items (such as compilers)
- 6.2.4 Identify required Ground Support Equipment (GSE).
- 6.2.5 Develop a build plan
- 6.2.6 Develop a budget and a schedule for review and approval by functional management and the customer.

6.3 Functional Design

- 6.3.1 Propose how the system will perform the required functions (at the highest level) and develop a functional design document.
- 6.3.2 Define project formats such as programming language(s), design methodology, naming conventions, and component prototypes.
- 6.3.3 Develop a Software Development Plan (SDP) which includes the previously defined project formats and build plan.
- 6.3.4 Develop interface control documents (ICDs).
- 6.3.5 Develop a block diagram of the system, which illustrates all software subsystems, I/O devices, special purpose hardware, and the flow of all data throughout the system.

6.3.6 Define and document any engineering test unit (ETU) interface differences (optional, per design plan).

6.4 Procurement

6.4.1 Order any long lead items (such as compilers).

6.4.2 Ground Support Equipment is incorporated from existing stock with or without modification, is procured, or is fabricated.

6.4.3 Identify and order any other required items.

6.5 Detailed Design

6.5.1 Refine the functional design into a complete, detailed system plan (at the lowest level) and develop a detailed design document.

6.5.2 Refine the functional design block diagram.

6.5.3 Develop a set of algorithm documents

6.5.4 Define project formats such as I/O files and records, output products, global storage areas, inter-task communication packets, interactive user language, and any other software constructs other than actual code.

6.6 Functional Reviews

6.6.1 Perform one or more Peer Reviews of the functional and detailed designs (see GPG 8700.4)

6.6.2 Perform a preliminary review of command, telemetry, memory, and processing requirements against intended system capacity.

6.7 Test Plans

Generate and execute test procedures for module, build, and integration testing (as required by the design plan).

6.8 Flight Software Reviews

6.8.1 Participate in the project Preliminary Design Review (per customer requirements).

6.8.2 Participate in the project Critical Design Review (per customer requirements).

6.8.3 Participate in Pre-Environment Review (per customer requirements).

6.8.4 Participate in Pre-Shipment Review (per customer requirements).

6.8.5 Participate in Safety Review (per customer requirements).

6.9 Flight Software Development

6.9.1 Perform coding of ETU software (optional, per design plan).

6.9.2 Generate (or modify) ETU test procedures (as required by the design plan).

6.9.3 Perform coding of software modules based on design methodology employed.

6.9.4 Integrate modules into builds.

DIRECTIVE NO. 573-PG-8700.2.2

EFFECTIVE DATE: 08/27/1998

EXPIRATION DATE: 08/27/2003

6.9.5 Generate any user, operations, and maintenance manuals needed.

6.9.6 Load any fixed embedded flight software into the component's non-volatile memory.

6.10 Flight Software to Spacecraft/Instrument

The Product Design Lead and Product Design Team participate, possibly significantly, in the development and execution of the embedded flight software to spacecraft/instrument integration and test procedures. This includes the fabrication of test laboratories as well as dynamic simulations and acceptance testing (optional, per design plan).

7 FLOW DIAGRAM

N/A

DIRECTIVE NO. 573-PG-8700.2.2

EFFECTIVE DATE: 08/27/1998

EXPIRATION DATE: 08/27/2003

CHANGE HISTORY LOG

Revision	Effective Date	Description of Changes
Baseline	08/27/1998	Initial Release