13 th EUROPEAN ROTORCRAFT FORUM

5.4
PAPER No. 48

MASTERING QUALITY OF AVIONICS SYSTEM'S SOFTWARE

A. REBOUL

AEROSPATIALE HELICOPTER DIVISION
MARIGNANE - FRANCE

September 8 - 11 , 1987

ARLES , FRANCE

MASTERING QUALITY OF AVIONICS SYSTEM'S SOFTWARE

A. REBOUL

AEROSPATIALE - HELICOPTER DIVISION

1 – SUMMARY

The ever growing significance of software in avionics systems has led the Helicopter Division of Aérospatiale to set up a specific development methodology duly taking digital equipment's safety aspects into account.

A quality assurance method was defined in parallel to design activities.

This method imposes mastering software and hardware development activities performed :

- in all or part by the Helicopter Division of Aérospatiale
- in part by digital equipment manufacturers.

This method is characterized by milestones spread along the development phase.

This exposé describes :

- Aérospatiale's quality assurance organization for systems and software and the relations existing between the various departments involved with systems/software quality.
- The main activities involved and the way systems/software quality assurance actions are planned.

2 – AVIONICS SOFTWARE AND SYSTEMS

The technological advances of the last few years have been concretized as far as avionics systems are concerned by the use of digital computers as major components of on-board equipment.

Increasingly, systems have to be :

- evolutive
- functionally and operationally effective
- integrated because of digital bus connections ; the volume and complexity of software in digital equipment is perpetually increasing.

Aérospatiale Helicopter Division's exposé : «An all-encompassing approach of complex on-board systems development» has shown the need for definition methods and tools to master systems/software development.

The quality assurance methods presented herein are the formal application of the methodological principles described above. They will be specifically used to describe quality actions undertaken in parallel to design and development to ensure that pre-defined methodological dispositions are correctly applied.

This last point is especially important for avionics systems because they involve a large number of industrial development participants and require harmonization, quality assurance harmonization in particular, from the leader.

Finally, it must be emphasized that, contrarily to hardware quality assurance dispositions, systems/software quality assurance actions cannot be applied to the final product ; software quality measuring methods are not yet recognized as industrially reliable.

2.1 – QUALITY ASSURANCE METHODOLOGY

The quality assurance methodological principles set up by the Helicopter Division of Aérospatiale to develop systems including software stem from the following considerations :

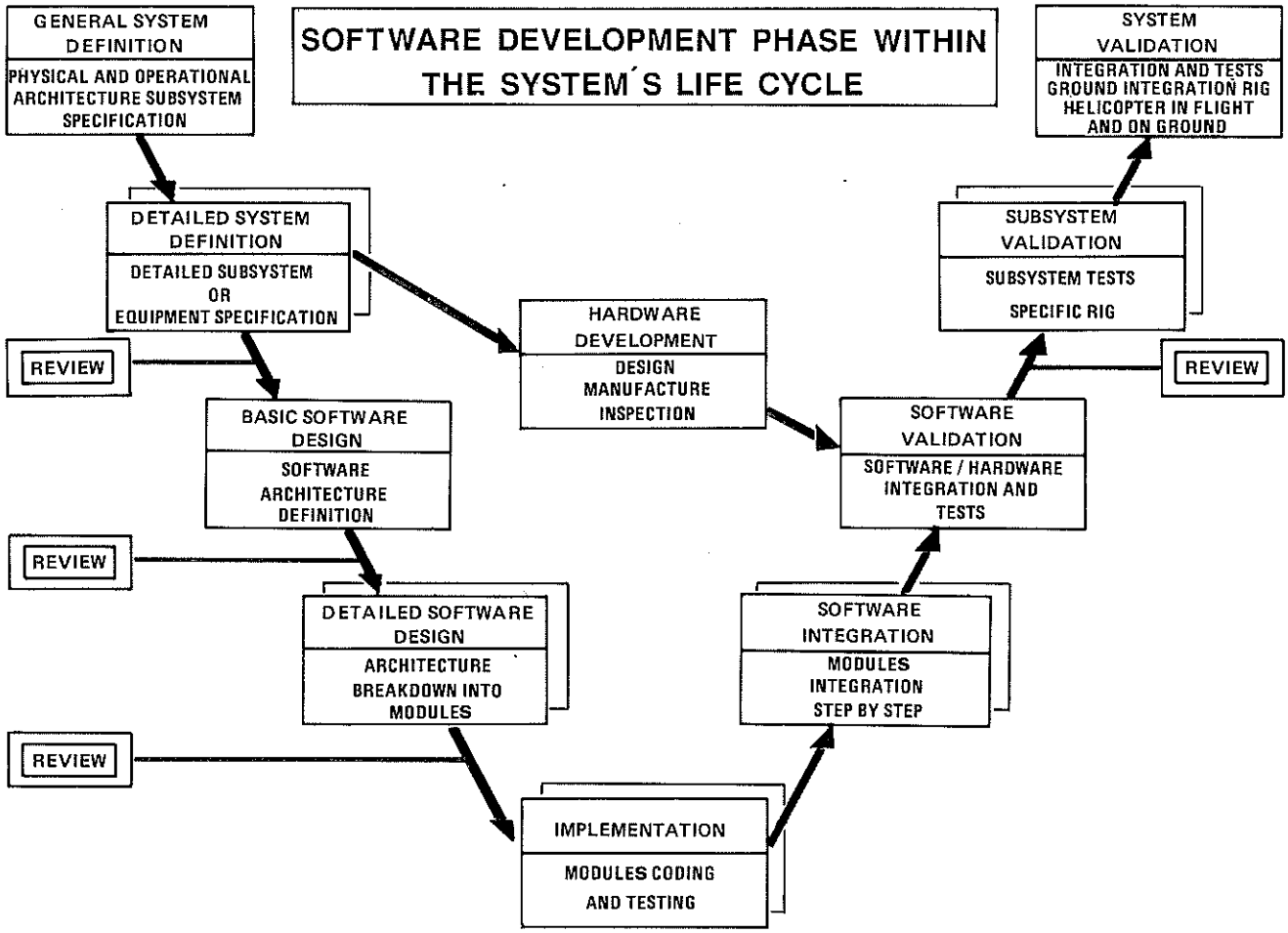
- Breaking down development process into phases delimiting technically coherent actions such as processing general technical specifications and system validation test specifications.
- Checking quality of work e.g. checking that work has been truly completed during pre-defined reviews so as not to have to change technical decisions at a later stage in the development process.
- Defining engineering, configuration management and quality assurance procedures and standards, knowing that a pre-determined, optimized framework will help master objectives and meet needs.
- Preparing and correctly structuring the documentation as the work proceeds to evaluate the system/software's product without any ambiguity as the latter is being processed.

The application of these principles is verified with milestones associated with the end of some development phases and concretized by the organization of quality assurance reviews.

System/software development phasing is presented in the following paragraph to detail the specific quality assurance operations.

2.2 – SYSTEM/SOFTWARE DEVELOPMENT PHASING

The following plan presents the development phases of an avionic system including software.



The V-shape representation mode allows emphasizing 3 points considered important from a quality assurance standpoint :

- The structured work breakdown that helps master, for complex systems/software such as avionics, the technical objectives to be reached at the system, sub-system, equipment, software, hardware pre-determined detail levels.
- The preparation from the conceptual design stage of the validation and integration activities that will be completed in parallel to the development phases e.g. software validation versus basic software design.
- The inclusion of contractual quality assurance reviews that will help define and follow up the application of development methodology directives.

3 – SYSTEM/SOFTWARE QUALITY ASSURANCE

3.1 – QUALITY ASSURANCE REQUIREMENTS

It is generally essential that quality assurance activities be performed along with the system/software development work ; this implies :

- including quality assurance actions in the definition and application of development methodology and configuration management,
- setting up quality assurance and configuration management plans as the project is being launched.

These plans are drafted by the digital equipment manufacturers at two different levels :

- Subsystem plans (set of digital equipment items providing an avionic system's operational function e.g. navigation, piloting, etc ...).
- Specific plans for software integrated to sub-system equipment.
- Monitoring the application of these plans as development is in progress.

To these general requirements can be added, depending on contractual aspects, detailed or regulatory requirements particular to the system development contract. This involves applying specific methods in accordance with national or international quality assurance or certification standards.

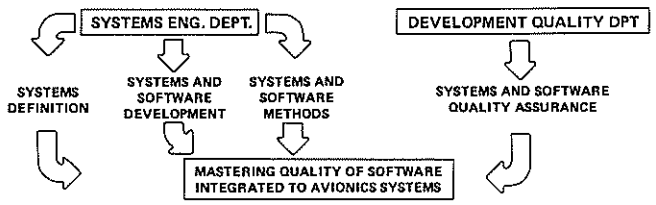
It is then up to the leader, the Helicopter Division of Aérospatiale, to point out these particular requirements to the industrialists supplying the system equipment and to ensure that they are correctly applied.

3.2 – SYSTEM/SOFTWARE QUALITY ORGANIZATION

The various Aérospatiale's Helicopter Division departments participating in an avionics system quality control are :

- The Definition and Development Departments attached to the Systems Engineering Department ; these Departments are tasked with the technical definition and follow-up of the avionics system and integrated software.
- The Methods Department attached to the Systems Engineering Department ; this Department is tasked with the implementation and application of the systems and software development methods and resources.
- The System Design Quality Assurance Department attached to Quality Management ; this Department must ensure that the methods and procedures used by Aérospatiale's Helicopter Division and equipment manufacturers will assure the quality of systems and integrated software.

This organization is summarized in the figure below :



This type of organization facilitates team work around a system development programme and ascertains that the judgements made are not biased.

A general procedure is then applied in accordance with the quality assurance requirements and the organization developed by Aérospatiale.

4 – QUALITY ASSURANCE PROCEDURE

4.1 – PRESENTATION

The system/software development work broken down into phases (see Paragraph 2.2) calls for formal actions at the milestones describes above ; these actions are :

- Examination of technical proposals made by the suppliers in reply to the functional, operational and quality assurance requirements laid out by Aérospatiale's Helicopter Division upon completion of the system definition.
- Examination for approval by Aérospatiale of the industrial measures enforced by the suppliers prior to digital equipment/software definition and development work.
- Analysis and approval by Aérospatiale of the technical files drafted during the basic software design phase ; these include basic design documents as well as software validation test plans.
- Analysis and approval by Aérospatiale of the technical files drafted during the detailed software design phase ; these include detailed design documents, integration test plans as well as internal software test procedures.
- Examination of software test results ; these include internal, integration and validation tests as well as reports of internal audits to be undertaken by the suppliers during software coding, integration and validation tests.
- Following up sub-system/system validation tests in a simulated (integration rig) or real (helicopter in flight or on the ground) environment.

To these specific system/software actions must be added analysis of programmes and results of qualification and acceptance tests for digital equipment. Since the latter are specifically related to electronic equipment quality, they are not discussed here.

4.2 – EXAMPLE OF APPLICATION

The software methodology and quality assurance examination procedure set up by the supplier is detailed below to specify the quality assurance approach adopted.

This examination is based on :

- an evaluation of the general quality assurance organization
- the quality requirements of the Helicopter Division of Aérospatiale
- an analysis of the technical proposals made in response to the above requirements
- the approval of the quality plans (general plan for supplies and specific plan for software) proposed by the supplier for development.

4.2.1 – Software quality evaluation

The evaluation of a supplier's general organization as applicable to software is described in an Aérospatiale document taking the general requirements of NATO's AQAP 13 into account.

The general evaluation principle is based on the examination of organization and resources ; this allows the supplier to effectively master software quality without prejudging the customer's specific contractual requirements.

This general quality evaluation is therefore the initial quality action undertaken by Aérospatiale vis a vis suppliers developing software integrated to avionics systems.

4.2.2 – Aérospatiale's Helicopter Devision quality requirements

The sub-system functional and operational requirements are processed by Engineering Department specialists during the system definition phases.

Quality requirements are considered from then on and included in specification documents.

These quality requirements drawn from the Quality standards of the Helicopter Division of Aérospatiale are specifically drafted for each sub-system described in the specifications ; these requirements mainly impose :

- A Software Development Guide explaining Engineering, Quality Assurance and Configuration Management me-

thods ; suppliers will have to follow the principles laid out in this Guide.

- Aérospatiale's Helicopter Division's participation in software development Quality Assurance reviews (see paragraph 4.1 Presentation of Quality Assurance Procedure).
- Supplying Quality Assurance documentation :
  - Sub-system and software quality plans
  - Sub-system and software configuration management plan

to be defined from the early stages of the development.

- Supplying or setting to disposal engineering and test preparation documents (plans and programmes) as well as test, review and audit reports.

The above requirements form the technical reference used to evaluate supplier's proposals.

4.2.3 – Analyzing technical proposals

Quality assurance in the suppliers' technical proposals is examined as follows :

Those points not covered in the proposals are first identified for official clarification (rejection or acceptable deviation).
A formal analysis report is then transmitted to the supplier for action and new proposal.

A Quality Plans draft is usually appended to the technical proposal ; this draft forms the basis for Quality discussions.

The functional and operational aspects of suppliers' technical proposals are covered by a similar procedure :

The various Aérospatiale departments concerned (Engineering, Product Support, Tests, Quality) hold an official meeting to decide whether the suppliers' proposals meet Aérospatiale's requirements.

Whenever the technical proposal is accepted by Aérospatiale, the technical resources effectively available at the supplier's can be examined under Aérospatiale's Quality Assurance Department's responsibility.

4.2.4 – Quality plans / resources available

Quality plans are reference documents dealing with the resources available to the suppliers to develop the contractual systems/software.

The Quality plans draft was discussed beforehand as the technical proposal was examined and a review is initiated by the Quality Assurance Department as development starts.

The supplier's final quality assurance and management configuration plans are formally examined during this review. The suppliers' internal procedures referenced in these drawings are also presented.

The Aérospatiale representatives occupy different functions previously defined :

- The engineer in charge of the sub-system technical definition.
- The representative of the Methodology Department attached to the systems Engineering Department specifically tasked with the examination of development tools and their effective modes of utilization at the suppliers'.
- The Quality Assurance Department's representative monitoring the application of procedures and specific Quality Control and Assurance regulations.

Deviations with respect to responses made as proposals were analyzed are underlined and a corrective plan is set up.

Upon completion of this review and once they have been approved by the Aérospatiale representatives, these plans will form the baseline of the quality actions to be undertaken as digital equipment is developed.

5 – CONCLUSION

The experience acquired by the Helicopter Division of Aérospatiale as concerns quality assurance of software integrated to avionics systems has shown that «software quality» is primarily determined by :

- Mastery of technical objectives and quality assurance at the level of system and sub-systems composed of digital equipment.
- The development of official verification and validation actions at the various design stages to avoid modifying technical decisions at a later stage.

This represents a significant amount of methodological work which should not be considered as a limitation ; it should rather be considered as an «industrial environment» that helps mastering software quality which is, by definition, neither visible nor palpable.