Introducing ECSS Software-Engineering Standards within ESA

– Practical approaches for space- and ground-segment software

M. Jones & E. Gomez
Ground Segment Engineering Department

A. Mantineo
Quality Office
ESA Directorate of Technical and Operational Support, ESOC, Darmstadt, Germany

U.K. Mortensen
Electrical Engineering Department
ESA Directorate of Technical and Operational Support, ESTEC, Noordwijk, The Netherlands

In June 1994, the ESA Council adopted a resolution that confirmed the Agency's commitment to transferring the existing system of ESA space standards to a new set of standards that were to be prepared by the European Cooperation for Space Standardization (ECSS). For software engineering, this has meant moving from the ESA PSS-05-0 to new software standards: ECSS-E-40 for software engineering and ECSS-Q-80 for software product assurance, both of which are based on a new international standard, ISO/IEC 12207. In addition, to cover the full scope of the old standard, it is also necessary to use the ECSS management standards (the ECSS-M series). Adoption of a new standard is a major change and one that has to be undertaken with care and so this article describes the measures that were taken to ensure a smooth transition, both at ESTEC for space-segment software and at ESOC for ground-segment software.

Why a new software-engineering standard?
ESA has had a highly successful software-engineering standard, ESA PSS-05, since 1984. PSS-05 was prepared by ESA's Board for Software Standardisation and Control (BSSC), which was established in 1977, when the importance of software standards for the proper conduct of complex or critical space-software projects was realised. PSS-05 appeared in Issue 1 in 1984, followed by Issue 2 in 1991. The BSSC also wrote a set of guides to provide more detailed assistance in using PSS-05. Both the standard and the set of guides were published as books.

However, the Council decision in 1994 meant that no further issues of PSS-05 would be published and the new ECSS software-engineering standard would become the one to be used in ESA software projects. Shortly after this decision, ISO published a new international software-engineering standard, ISO/IEC 12207 (Information Technology, Software Lifecycle Processes, 1995), which is now the leading standard in this field. The ECSS software-engineering standard ECSS-E-40, which first appeared in 1999, is based on ISO 12207. In fact, ECSS-E-40 tailors ISO12207 specifically for space projects.

The introduction of this new standard represented a further step in the 'Europeanisation' of the way of working in the Agency. In fact, an objective was to produce a standard to be used throughout the European space business, i.e. by Industry and across the space agencies within Europe, superseding agency-specific standards such as PSS-05. In this way, the problem of a given company or consortium having to follow different standards depending on which agency it is contracted to for any given development is avoided: the ECSS standards thus provide a common backbone.

This European approach also had consequences for ESA's BSSC: whereas formerly the BSSC established and maintained software-engineering standards, now this responsibility is transferred to the ECSS. Of course, the BSSC has in practice been involved in the relevant ECSS Working Group and subgroups – for example, one of the BSSC Co-Chairmen

is also convenor of the ECSS-E-40/ ECSS-Q-80 Working Group. Within ESA, the BSSC still plays an important role, since it has to ensure that the new software-engineering standards are introduced and applied properly and that tailoring methods and ESA implementations of the ECSS standards are available as needed. It also deals with standardisation aspects such as coding standards that will not be covered by ECSS. The rest of the BSSC's responsibilities remain unchanged, ensuring in particular that the standards are applied in ESA contracts, and liasing with the ESA's Legal and Contract Departments on matters affecting software intellectual-property rights.

The structure of the ECSS standards is shown in Figure 1, from which it can be seen that there are three main branches: 'Management', 'Product Assurance' and 'Engineering'. It is a characteristic of software engineering that it involves all three branches of the ECSS standards.

Software in ESA

ESA's core business is the execution of space programmes, including:

– space segments comprised of spacecraft, payloads and launchers
– ground segments comprised of all of the ground facilities needed to operate each mission.

Software is pervasive throughout the whole 'product tree' of any space programme: Figure 2 shows a typical space system schematically, with emphasis on the software elements. The space segment has onboard computers, data-handling systems, attitude and orbit control systems, all of which contain software. The ground segment has mission-control systems, simulators, flight-dynamics systems, mission-analysis tools, communications networks and ground-station data systems such as telemetry and telecommand processors, as well as 'downstream processing' systems for payload data. These all contain software, often of considerable complexity.

Developing and maintaining this software in a disciplined way is a key to the success of any space mission. Failure to do this can result in expensive delays, and in the worst case in catastrophic failure. Following proper software standards is one of the ways of keeping software development under control and ensuring adequate quality.

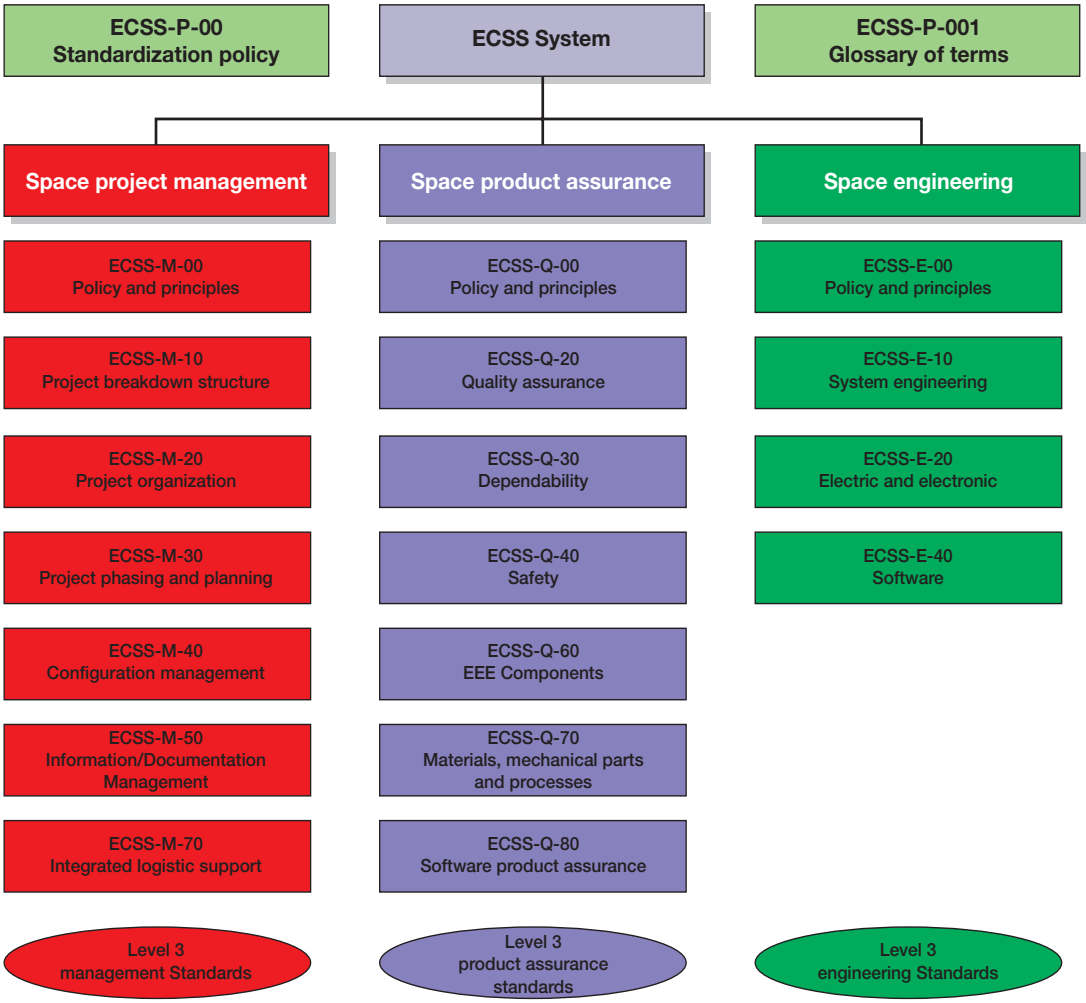


Figure 1. Structure of the ECSS standards

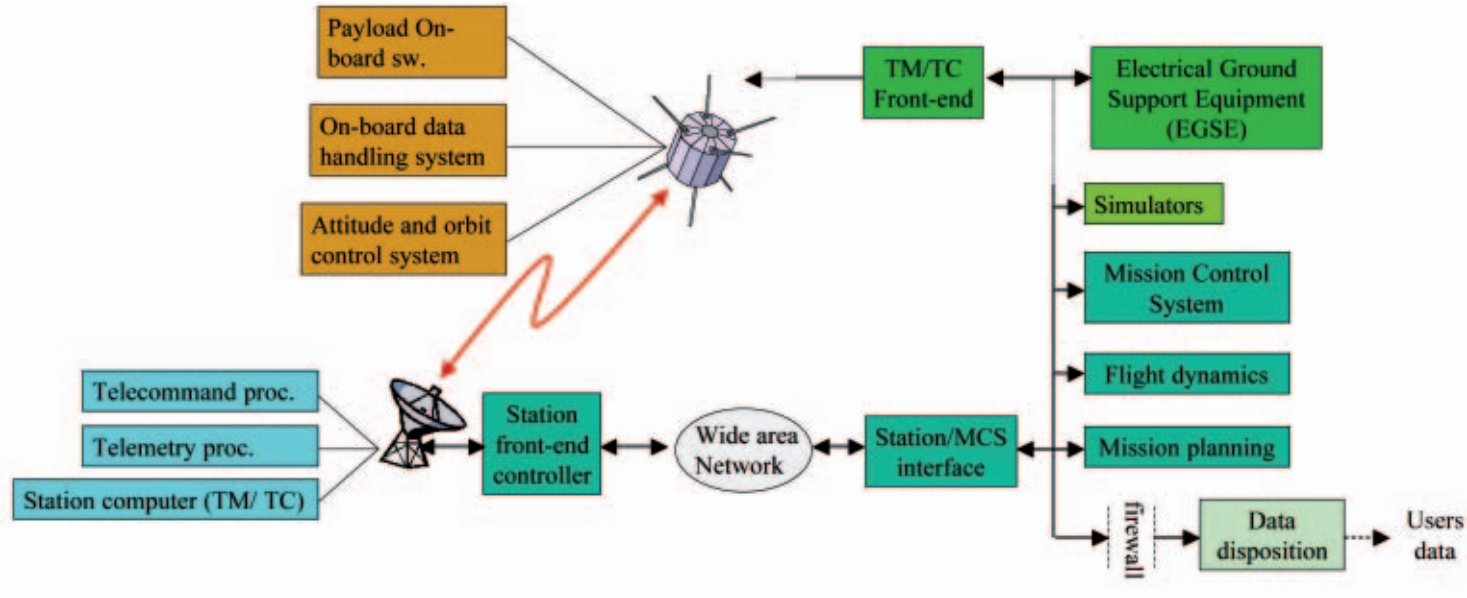


Figure 2. Schematic of a typical space system, with the emphasis on software elements

Overview of ECSS-E-40

ISO 12207 and ECSS-E-40 are based on a defined set of processes. They define:

- requirements on those processes broken down into component activities
- their expected inputs and outputs.

They are in effect 'standards for making standards', the idea being that this permits suppliers to use their own standards, provided that they comply with the requirements of ECSS-E-40 or some tailoring of it defined by the customer. ECSS-E-40 is available at the ECSS Web site: http://www.estec.esa.nl/ecss/, where its partner quality standard ECSS-Q-80 and the ECSS-M standards may also be found.

ECSS-E-40 is based on the customer–supplier concept. As shown in Figure 3, this concept may be applied recursively, as would typically be the case for space projects with ESA as the customer at the top level, and then a chain of customer–supplier relationships extending downwards to the prime contractor and then to the lower levels of subcontractors. Reviews are the main interaction points between the customer and the supplier.

The accompanying coloured panel is a brief review of ECSS-E-40, outlining the required processes, reviews and documentation. It gives the correspondence to PSS-05 where appropriate, for the benefit of readers familiar with that standard. Figure 4 shows the processes of ECSS-E-40 and ECSS-Q-80.

Figure 3. Customer–supplier relationship

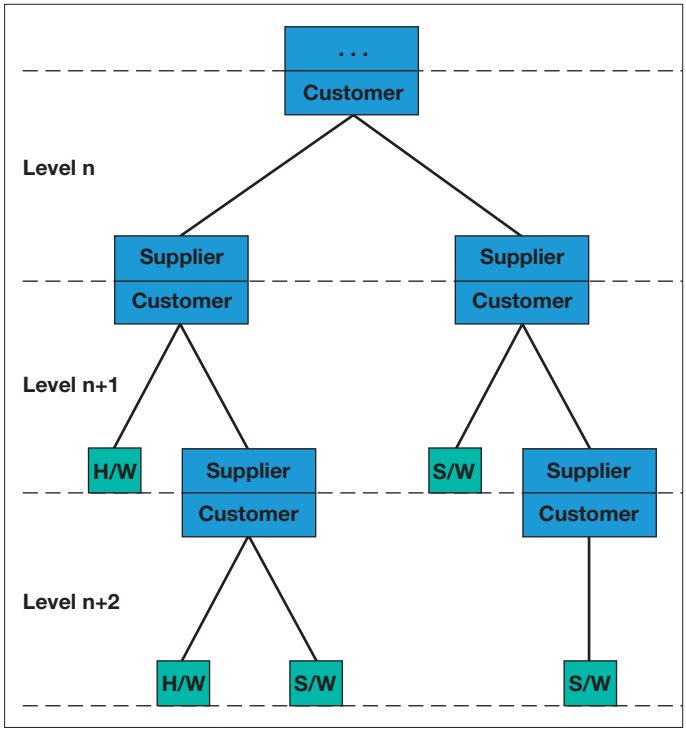
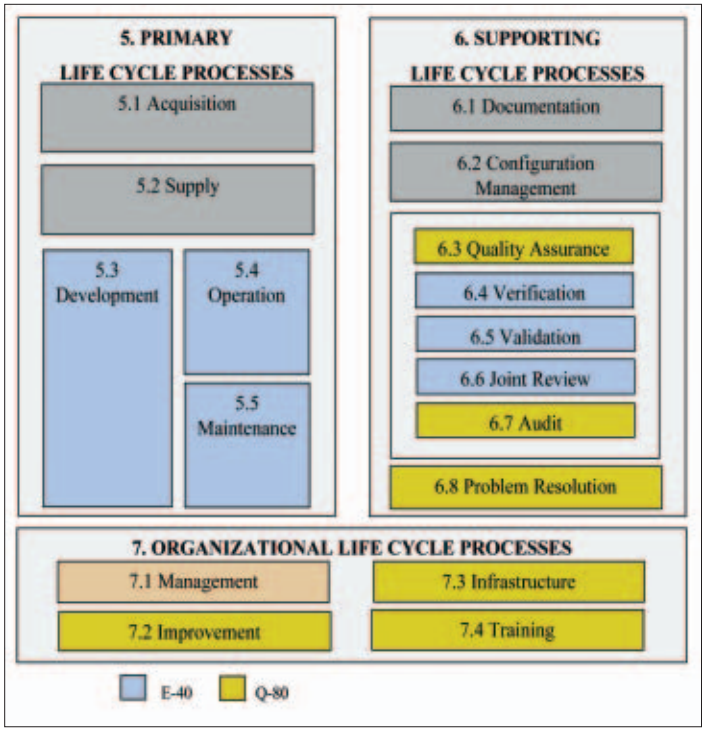


Figure 4. Processes of ECSS E-40 and ECSS Q-80



ECSS-E-40 Processes

System Engineering
This is carried out by the customer and involves such activities as:
– system requirements engineering
– system integration
– system validation.

This is somewhat analogous to the PSS-05 User Requirements (UR) phase, but is more general in that it sees the software as part of a system that put requirements on it – the surrounding system could be onboard hardware and other software systems, and need not necessarily include a human user. In PSS-05, the UR phase was generally understood as a specific activity occurring after the system definition, preparing the software development, but separated from the system activities. In ECSS, this process is the same as the ECSS-E-10 Space System Engineering process, ensuring a better transition of the requirements from system to software.

Software Requirements Engineering
This is carried out by the supplier and in essence involves:
– software-requirements analysis (roughly equivalent to PSS-05 SR phase)
– software top-level architectural design (roughly equivalent to PSS-05 AD phase).

The related review is the Preliminary Design Review (PDR).

Software Design Engineering
This is also carried out by the supplier and involves:
– designing of software items
– coding and unit testing
– integration
– validation with respect to the technical specification (equivalent of PSS-05 System Testing).

The related review is the Critical Design Review (CDR).

Software Validation and Acceptance
This comprises:
(i) Validation with respect to the requirements baseline: the milestone is the Qualification Review (QR), which is carried out in the supplier's environment and is often referred to as the 'Factory Acceptance Test'
(ii) Software delivery and installation
(iii) Software acceptance: the milestone is the Acceptance Review (AR) and is carried out in the operational environment (like PSS-05 Acceptance Test, AT). This is also referred to as the Site Acceptance Test (SAT), and may be preceded by a Preliminary SAT (PSAT). Acceptance is carried out by the customer.

Activities (ii) and (iii) are analogous to the PSS-05 Transfer Phase.

Software Operations Engineering
This comprises:
– preparation of software operations procedures
– preparation of plans for operational testing (i.e. of new releases coming from the maintenance process)
– software operations proper
– user support, including what is usually called 'first-line support', e.g. help desk.

Software Maintenance
This comprises:
– software problem analysis
– software problem correction (software modification)
– re-acceptance (i.e. validation of corrections)
– software migration (cf. PSS-05 'adaptive' maintenance)
– software retirement.

ECSS software maintenance is similar to PSS-05 Operations and Maintenance (OM Phase), but ECSS-E-40 places more emphasis on migration and retirement, and separates first-line maintenance from software operations.

Reviews
The following table summarises the reviews required by ECSS-E-40:

Name	Acronym	Associated process
System Requirements Review	SRR	System engineering
Preliminary Design Review	PDR	Requirements engineering
Critical Design Review	CDR	Design engineering
Qualification Review	QR	Validation and acceptance
Acceptance Review	AR	Validation and acceptance
Operational Readiness Review	ORR	Software operations engineering

Software documentation
Figure 5 shows the main categories of ECSS-E-40 documentation. It is arranged in 'folders', into which the various output documents are aggregated. The main folders are:
– Requirements Baseline (RB)
– Technical Specification (TS)
– Design Definition File (DDF)
– Design Justification File (DJF).

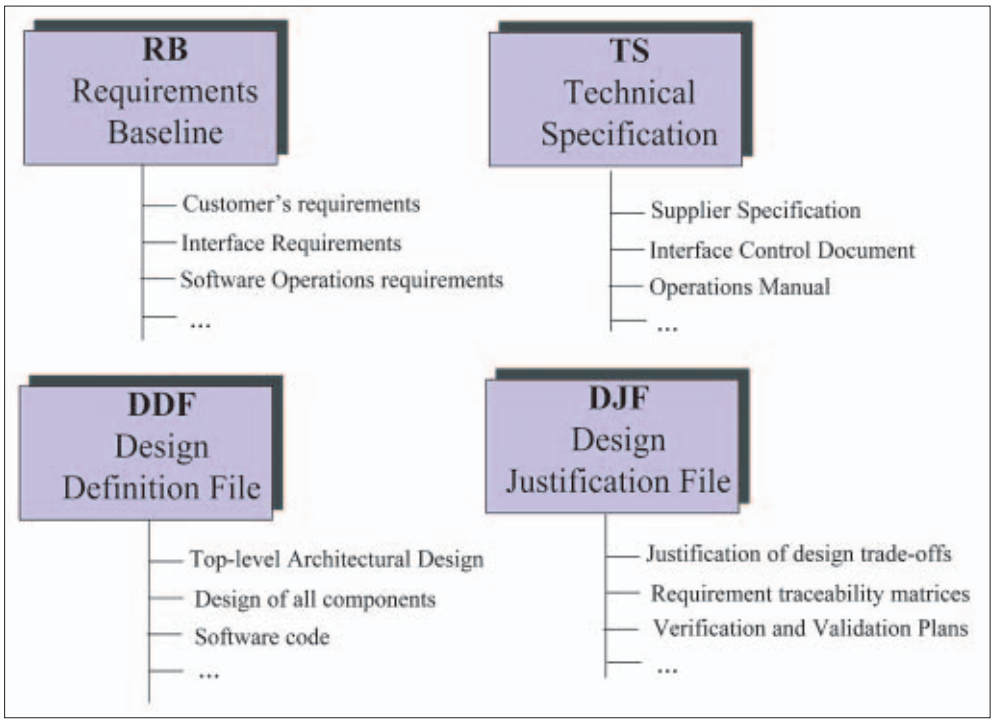
The contents of these folders are built up in the course of the project, as shown in Figure 5. The folders may, of course, be logical, i.e. they may in effect be directories pointing to the documents they 'contain' rather than being physical folders.

Software life cycles
The software life cycle defines the sequencing and dependencies of the processes. As with PSS-05, no particular life-cycle model is imposed, but its selection is an essential management activity. The supplier must document this choice in the Software Development Management Plan.

Comparison of ECSS-E-40 and PSS-05
The BSSC carried out a detailed analysis of ECSS-E-40 and PSS-05, comparing in particular the ECSS-E-40 processes with the PSS-05 phases, including process/phase inputs and outputs, and reviews. The main conclusions were that PSS-05 mandatory practices cover about 70% of the ECSS-E-40 requirements. The analysis also identified ECSS-E-40 requirements not covered by PSS-05-0 practices.

Figure 6 shows a mapping of PSS-05-0 phases to the ECSS-E-40 processes, including related reviews, reflecting the fact that a process model can always be projected into a set of phased activities. Figure 7 illustrates the contrasting features of the two standards, the main ones being:
– process-based (ECSS-E-40) versus practice-based (PSS-05)
– ECSS-E-40 is based on the notion of customer and supplier, while PSS-05 has no such concept
– ECSS-E-40 and ECSS-Q-80 apply to 'product software', i.e. software that is part of a space-system product tree and developed as part of a space project. They are applicable to all the elements of a space system: the space segment, the launch-service segment and the ground segment. By contrast, PSS-05 is general (it could apply to any software) and applies to a software project
– ECSS-E-40 allows the customer to 'tailor' the standard, i.e. the deletion of non-applicable processes, activities or tasks. Tailoring is specified in the customer's request for proposal, and may involve additional unique or special processes, activities or tasks.

Figure 5. Main categories of ECSS E-40 documentation



Transition from PSS-05 to the ECSS set of software standards
In 1996, the BSSC issued an information note to all ESA staff providing information about the planned transition. It also laid down one general principle: it was not required to apply ECSS-E-40 retroactively to projects already using ESA PSS-05, and this still holds true.

Applying ECSS software standards to space-segment projects
Spacecraft onboard software has several features unique for the

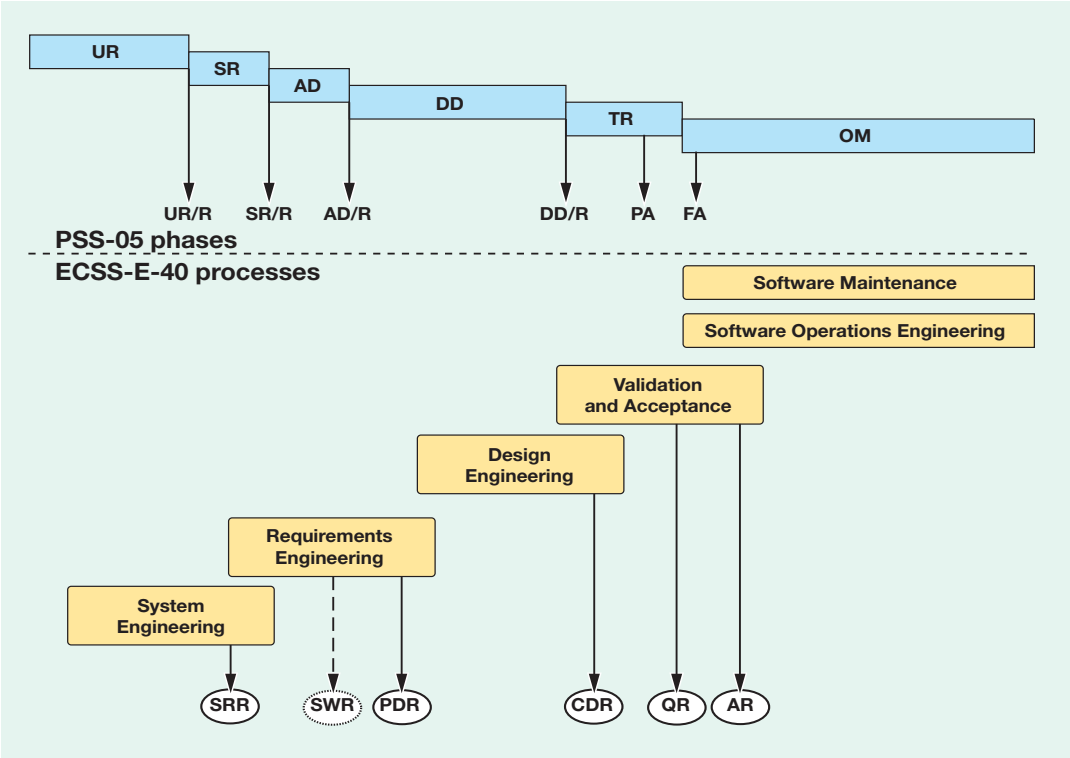


Figure 6. Mapping of the PSS-05 phases to the ECSS E-40 processes

domain. Not least, it has a high level of criticality for the spacecraft, since failures can cause loss of the entire mission. Unlike aircraft systems, for example, no prototype flights can be made and the software has to work correctly as soon as the satellite arrives in orbit. Therefore, testing and qualifying the software to ensure it will work correctly 'first time' is a major challenge. Because of avionics, power and mass constraints, onboard software is designed with severe limitations on processing power and memory. However, it controls and handles most of the electrical systems and the interfaces to the onboard avionics, and therefore it belongs to the technically difficult class of 'hard real-time software', with many processes running in parallel and response requirements in the microsecond range. Moreover, since a large and ever-increasing proportion of mission and spacecraft functional requirements are implemented by onboard software, its specification and design is strongly coupled with the overall system-engineering activities of the mission.

This major expansion in spacecraft onboard software functionalities occurred after the 1980s, when PSS-05 was written. Hence, in producing the ECSS Software Standards, it was a priority to introduce and modernise the standards to take into account this evolution. Introduction of system-engineering processes and interfacing software-engineering activities to the overall system-engineering process are good examples of this. Another example is the adoption of life-cycle milestones such that software developments follow the same conventions as any other space-system development (SRR, PDR, CDR, etc.).

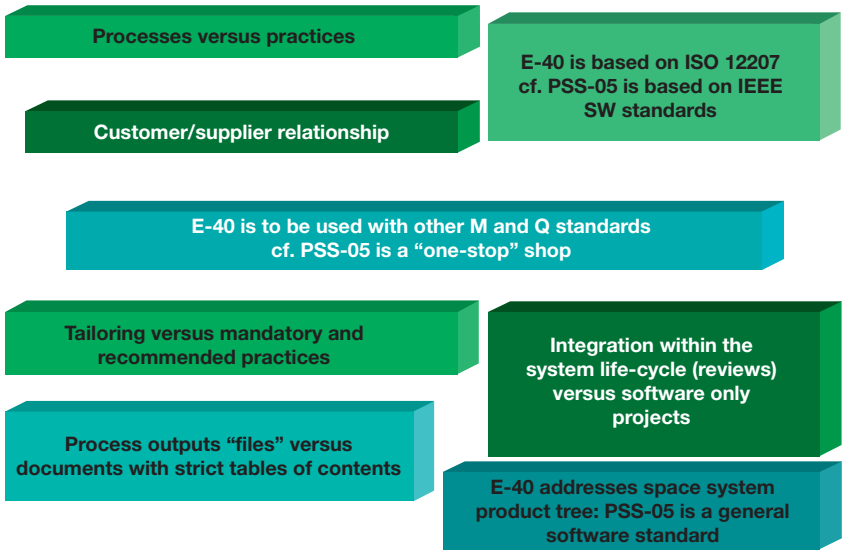


Figure 7. Comparison of the main features of PSS-05 and ECSS E-40

The first use of the ECSS Software Engineering standards was made as early as 1996. Since then, the combination of ECSS-E-40 and ECSS-Q-80 has been successfully applied to several tens of space projects, ranging from full-size satellite projects (in Space Science, Earth Observation, and Navigation) to smaller R&D activities in the areas of onboard software, Electrical Ground Support Equipment (EGSE), analysis tools and algorithm development. The transition to the new set of software-engineering standards has been successful, with no major problems vis-a-vis the ongoing space-segment developments.

Key factors in the successful introduction and application were:
– A strong commitment from the participating ECSS partners in producing very high quality standards and with internal commitments for the integration into their respective business processes.
– Training material and introduction courses both for those with previous experience with other standards and for those entering the space market for the first time.
– The ECSS tailoring possibility, allowing adaptation of the requirements to individual projects or domains.

Applying ECSS software standards to ground-segment projects at ESOC

The ESA Ground-Segment Software Engineering and Management Guide (ESA GS SEMG)
At ESOC, the bulk of ESA's ground-segment software is procured via frame contracts. Typically, there are several frame contractors in each discipline area (e.g. mission control systems, simulators, flight dynamics) and they compete for work as it arises. PSS-05 has been applied for all such software procurement and was made applicable in the relevant frame contracts. This led to a uniform approach to reviews and documentation across the various contracts in any given area. The desire was to continue this practice and avoid a situation in which different suppliers use different implementations of ECSS-E-40. This is particularly important for long-lived and complex infrastructures or generic software, where several different contractors may be involved.

Transition to the ECSS standards involves:
– using a process-based standard instead of a practice-based standard
– coping with the distribution of the ECSS standard over many documents (E40, Q-80, ECSS-M-) instead of one (PSS-05).

It was to ease these steps and provide a common implementation basis for the various frame contracts that the ESA Ground Segment Software Engineering and Management Guide (ESA GS SEMG) was written. This provides ECSS compliance in the form of a set of practices. It is written in a style similar to PSS-05, with a clear correspondence to the ECSS processes and requirements, and it covers all relevant ECSS standards in a single (multi-volume) document.

The SEMG is an *implementation guide*, applying the relevant ECSS standards to software development for ground segments. Implementation aspects include, for example, document templates and advice on how to perform the necessary work, in addition to the ECSS requirements. It is also an initial tailoring of the ECSS requirements for ground-segment software developments. The SEMG has removed some requirements that were not applicable to ground-segment development and has also introduced some missing ones, particularly in the areas of configuration management and software project management. Another example of the tailoring is the addition of the Software Requirements Review (SWRR) between SRR and PDR to provide a separate review of the software requirements and facilitate continuity with established practice.

An important feature of the ECSS software standards is that they may be tailored in accordance with customer needs and project or system characteristics. The GS SEMG can, therefore, be further tailored (corresponding in effect to a tailoring of the ECSS source standards). The Tailoring Template, also published by the BSSC, is a companion guide to the GS SEMG that provides guidance when introducing further tailoring. Specifically, it gives advice on the processes to be considered applicable within a given software-development project. It clarifies the principles upon which the tailoring process is based, allowing for the selection or waiving of some of the practices described in the Guide. It does not constitute a specific tailoring of the GS SEMG as such, and therefore should not be considered or referred to as contractually binding. However, a tailoring resulting from it could be made contractually binding.

The GS SEMG could be applied to any development of ground-segment software for a space mission. However, it is primarily intended for use in ground-segment software development at ESOC, where the GS SEMG will be referenced (i.e. made applicable) in procurement contracts.

The SEMG has three volumes:
– Part A: Software Engineering, covering ECSS-E-40
– Part B: Software Management, covering the ECSS-Q-80 and ECSS-M- series
– Part C: Document Templates.

Part A was the first one to be written and was the result of work carried out by a Working Group comprised of software engineers drawn from the ground-segment disciplines that develop and maintain software (simulations, mission-control systems, flight dynamics, ground-station information systems and spacecraft checkout).

The GS SEMG is based on new versions of ECSS-E-40 and ECSS-Q0-80, the so-called 'B' versions, which are currently under formal review within the ECSS. These do not differ in any principle respects from the ones currently on the ECSS Web site, but there are a large number of corrections and improvements.

The ESOC Quality Management System (QMS)
In November 1999, ESOC was the first ESA entity to be certified according to the ISO/IEC 9001 Quality Standard, following an 18-month preparatory phase. The rationale for this was that ESOC was providing services both to ESA projects and to external 'third party' projects, the latter following an ESA Council decision in 1998. ISO 9001 certification therefore increases ESOC's effectiveness and attractiveness as a supplier of services.

To support ISO 9001 certification, ESOC prepared a Quality Management System (QMS), which is a set of internal procedures and instructions defining implementation of work processes at ESOC and the associated responsibilities. It consists of:

– a Quality Manual describing top-level requirements on the management system

– a set of procedures and work instructions describing all of ESOC's business processes,

The procedures and work instructions are split up into different areas such as Ground Segment Management, Infrastructure, Configuration Management, and Procurement via Contracts. The QMS does not repeat the various technical and procedural standards that are used in ESOC's work, but rather refers to them as necessary.

At the time that the QMS was first written, all ESOC software projects were based on the PSS-05 standards, and so this was referenced in the QMS.

The transition process at ESOC
The transition process at ESOC involved reviewing the Quality Management System, identifying the changes needed to adapt to the new standard, making those changes, and formally re-issuing the QMS. A QMS revision team was defined, made up where possible of the original authors of the various QMS documents. A Workshop was held in April 2001 to introduce the team to the new standards, agree on the subset of documents that would require change, and make a plan for the phase-in of the new standard. The resulting plan foresaw a set of activities extending over one year, with an approved updated set of QMS documents by the second quarter of 2002, with a view to using the standard for new projects from that time onwards. Management approved this plan in May 2001.

The April 2001 Workshop determined that some 20 documents needed updating. In some cases the updates required were substantial, as with for example the procedure on 'Control of Software Procurement via Contract', where there were numerous references to PSS-05 had to be replaced. There were about half a dozen documents in this category. Other documents, such as all of the procedures relating to configuration control, needed only minor changes. A QMS Consistency Workshop was held in January 2002 to review the whole body of updated QMS documents and ensure that they were coherent.

In fact, the schedule was successfully maintained, with the formal issue of QMS documents taking place in early May 2002.

Training courses are planned, including a technical one for data system managers and technical officers in charge of defining and procuring software systems.

Conclusions
This article has outlined the new ECSS software-engineering standards and an intense set of activities within ESA to ensure their smooth introduction into the Agency's procurement of software for both the space and ground segments. The ECSS standards have been applied for some time to space-segment projects. The transition to ECSS standards for ground-segment projects at ESOC took place later, with the first projects beginning to use them via an implementation guide (the GS SEMG) this year. Indications are that the careful preparation and support has helped make the transition a smooth one.