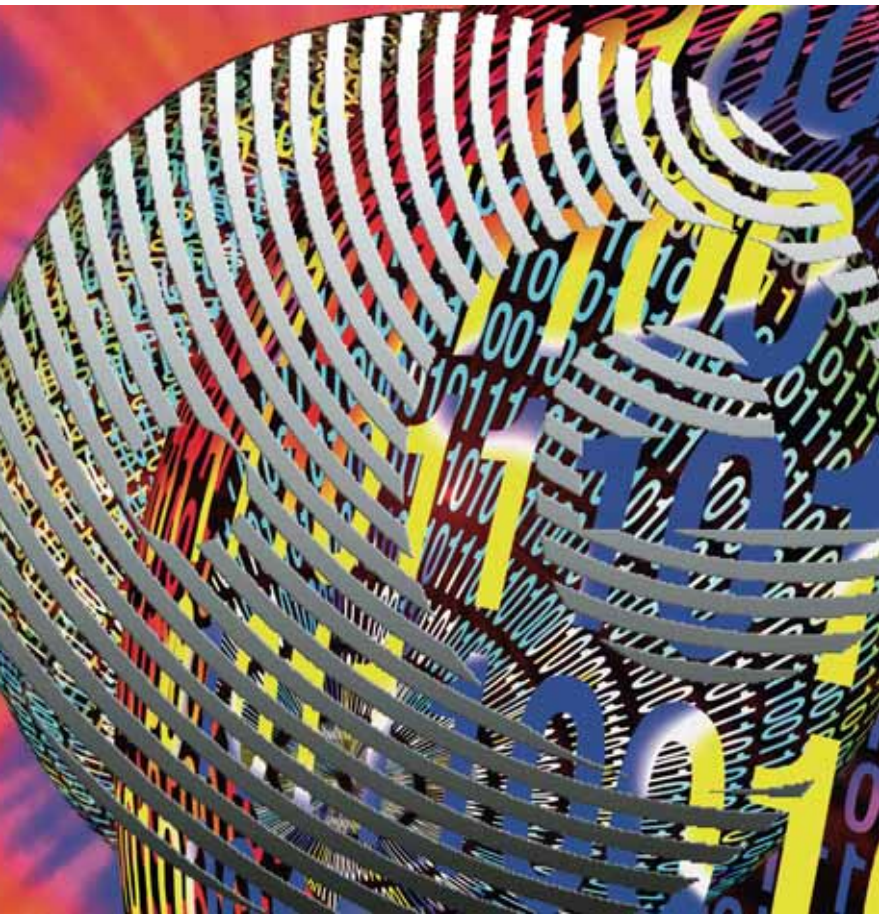


Checking Whether SCOS is up to SPEC

Fernando Aldea
ESA Directorate of Technical and Operational Support,
ESTEC, Noordwijk, The Netherlands

Michael Jones, Eduardo Gomez
ESA Directorate of Technical and Operational Support,
ESOC, Darmstadt, Germany

Hendrik Schäbe
TÜV InterTraffic, Germany

Originally developed as operational software to support ESA's space missions, SCOS-2000 is now being promoted as an ESA product available to the worldwide space community and more than 40 customer licences have already been granted. To support its promotion, a certification activity is now in progress which involves benchmarking the product against a set of agreed quality criteria (the quality model) by an independent organization (TÜV InterTraffic). The evaluation and certification process is based on a method called 'SPEC' (Software Product Evaluation and Certification).

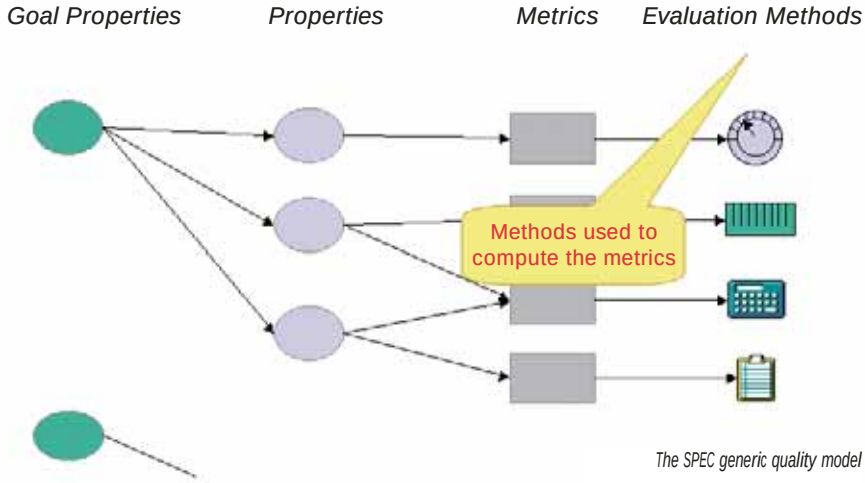
What exactly is SPEC?

SPEC is a software product evaluation and certification method that has been developed under ESA contract. Based on several international standards, it has already been used to evaluate a number of software packages, but SCOS-2000 is the largest one to date.

The quality model that underpins the SPEC method is composed of so-called 'goal properties' (e.g. functionality), which can be split into a set of second-level 'properties'. Each property can be quantified by a set of metrics, which are measured using one of several methods. The goal property of 'functionality', for example, can be broken down into the properties of completeness, correctness and efficiency. Efficiency can in turn be measured

by looking at such numerical indicators, or 'metrics', as timing margins, memory margins, throughput and resource utilisation.

Software product quality depends on numerous factors. Some of them are inherent in the product, whereas others are derived from its development process and from the operational context in which the software must run. Consequently, indicators of the software development process and the developer organisation's capabilities are also needed in the context of software product evaluation and certification, as they provide valuable indications of product quality. For this reason, the SPEC method incorporates not only product-related, but also development-process-related goal properties, and also covers practices specific to the space sector (such as those defined in the ECSS-E-40 and ECSS-Q-80 European Standards).



The SPEC generic quality model

SPEC Goal Properties

Product Related
- Functionality
- Reliability
- Maintainability
- Re-usability
- Operability
- Documentation Quality

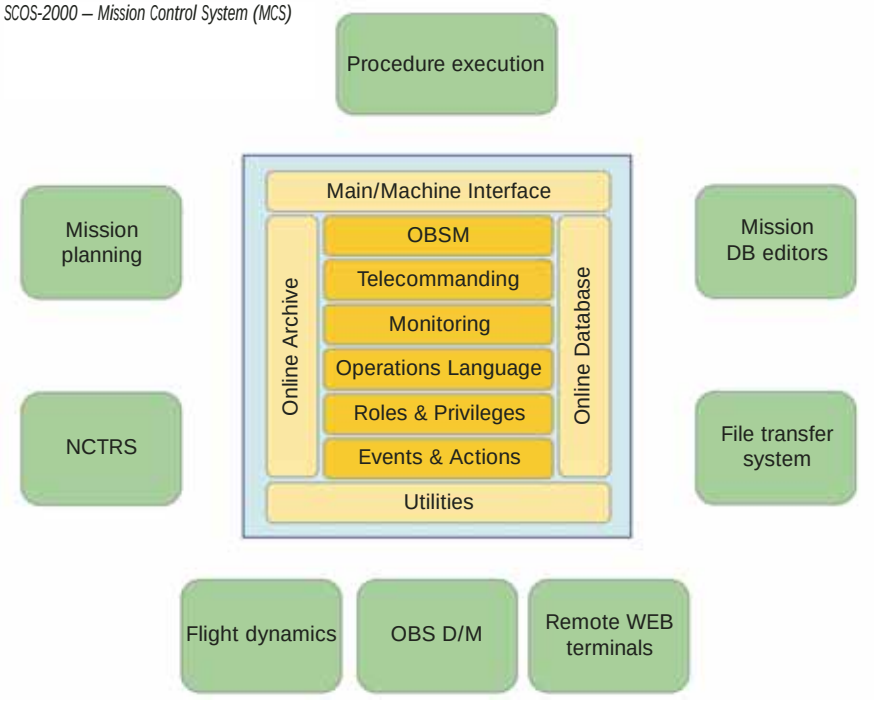
Process Related
- Suitability for Safety
- Software Development Effectiveness
- System Engineering Effectiveness

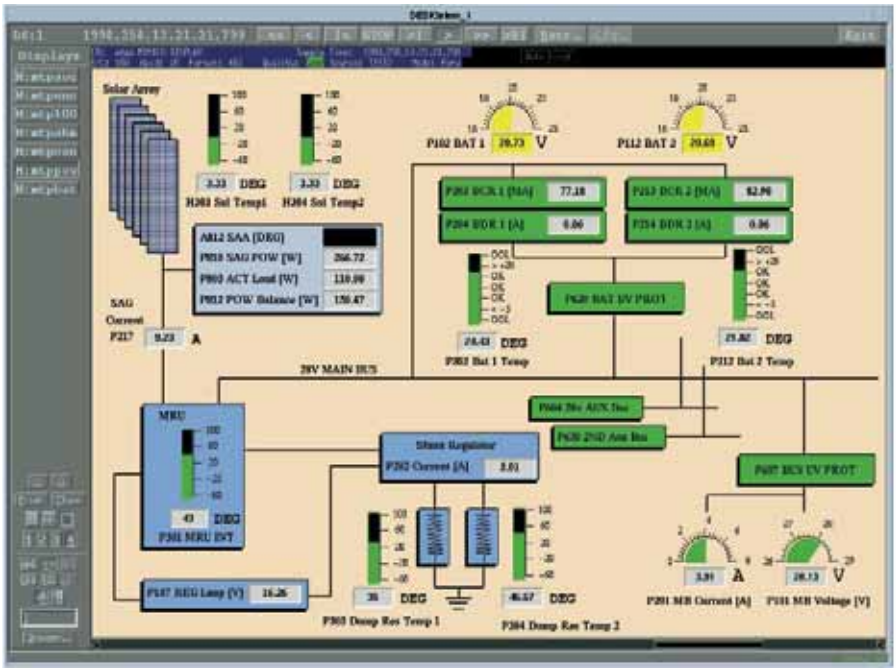
What exactly is SCOS-2000?

SCOS-2000 is a generic reusable software system that facilitates the implementation of Mission Control Systems (MCS) for both small- and large-scale space missions. The typical SCOS-2000 configuration is a distributed system, running across a network of workstations, although it may be scaled down to a 'SCOS-2000 in-a-box' (i.e. single workstation) configuration for simpler missions. The functions covered are:

– Telemetry Processing (TM)
– Telecommanding (TC)
– Online Database (DB)
– Online Archive (ARCH)
– General Services and Utilities
– Operation Language (OL)
– Roles & Privileges (USER)
– Events & Actions (EVAC)
– On-board Software Maintenance (OBSM).

The inherent flexibility of SCOS-2000 allows client missions to configure the system to their own requirements using the database (containing spacecraft telemetry, telecommand and display characteristics) and the various system-configuration files.





Example of displayed SCOS-2000 information

Evaluating SCOS-2000 with SPEC

The evaluation and certification process was split into two phases:
– Phase I. Baseline Evaluation
– Phase II. Delta Evaluation and Certification.

During the first phase, a baseline version of the SCOS-2000 (version 2.1e) was evaluated and a set of recommendations for product improvement has been issued. In the second phase, the updated version of SCOS-2000 will undergo a 'delta evaluation' and will eventually be certified in a process agreed between ESTEC, ESOC and TÜV. The first phase was in fact preceded by a Software Criticality Analysis (SCA), based on the results of a Software Failure Modes, Effects and Criticality Analysis (FMECA software), which provided necessary input, but was not part of the SPEC method itself.

The results of the Baseline Evaluation (Phase-I) can be summarised as follows:
– Of the 85 metrics defined by SPEC, 10 were considered inapplicable.
– 3 metrics were not measured due to lack of an appropriate tool or evaluation method, but they were replaced with other similar metrics.
– 5 out of 72 metrics failed to reach the target value.

Thus, although SCOS-2000 met the target values in most cases, it still needs improvement before it can be correctly certified as Class-B (mission-critical) software. Possibly more important than the formal certification, is the critical review of the software itself and its production process and methods. In this context, a set of recommendations have been identified that will lead to further enhancement of the product, including:
– provision of a homogeneous quality level throughout the product documentation, including the older elements
– improvement of traceability documentation (e.g. from requirements to design, design to code, requirements to test cases)
– analysis of the current architecture to identify possible changes that can help reduce the complexity of some modules
– use of better/improved software coding standards.

In addition, a process-improvement programme has been initiated at one of the SCOS-2000 subcontractors, which should help increase the overall quality of the development and maintenance process.

The Next Steps

Most of the recommendations emanating from the SPEC Phase-I evaluation are currently being addressed by several activities designed to improve SCOS-2000 as a software product. The results will be incorporated into future versions of SCOS-2000, one of which will be subjected to the delta-evaluation exercise.

These improvements will be complemented with new coding standards that will take into account state-of-the-art software development methodologies such as Model Driven Architecture. The new standards will contain language-independent practices and conventions, but will also cover the specificities of the languages used to develop SCOS-2000, primarily C++ and Java.

In addition, a new SPEC-based evaluation activity has been initiated on RTEMS, a real-time operating system that is being proposed as onboard COTS software in some spacecraft systems. RTEMS is developed and maintained as Open Source Software (OSS), which makes it a real challenge in terms of application of the SPEC method, which was originally conceived for software products developed in a more traditional way. SPEC therefore needs really to be adapted to this particular type of software, but the RTEMS evaluation is expected to provide useful experience in how to apply the SPEC approach to COTS and OSS products.

Acknowledgement

The key players in the SCOS-2000 evaluation and certification process are:
– TÜV InterTraffic (Germany), acting as evaluator and certifier.
– Critical Software (Portugal), as the sub-contractor performing the Software Criticality Analysis (SCA).
– ESOC Ground Segment Engineering Department, responsible for SCOS-2000 development and the requester of the certification.
– The SCOS-2000 suppliers, providing information on SCOS-200 development.
– ESTEC Software Product Assurance Section, providing the Technical Officer for the activities and supervising the application of the SPEC method, developed under a previous contract run by them.