

Standards for Software in Safety-related Applications

Claus Trebbien-Nielsen, DELTA

ctn@delta.dk

Lars Strandén, SP

lars.stranden@sp.se

1. Introduction

There are many standards for safety related applications in use today that specify how development of software and systems should be made in order to adhere to the requirements in specific industrial areas. However, the requirements in these standards are not co-ordinated, and differences apply for different sectors of industry. Further, since products are continuously getting more complex, more than one standard may be applicable and so the requirements of standards can be identical, complement, exclude or even contradict each other.

So a valuable insight would be to be able to evaluate a standard on its own and in relation to other standards. However it is not trivial to define a procedure for this work. In its most generic sense the comparison work is to evaluate and compare two text masses containing partly different information, with different strictness and seen from different views. The written text in itself (i.e. the implementation) contributes with complicating aspects such as:

- The text is written for humans and cannot be formalized into a version leaving no space for interpretations.
- Use of must, shall, should etc makes it difficult to isolate and compare requirements. Further, within a standard both should and shall can exist for the same item.
- Standards have different principle views e.g. if documentation is a separated process or if it is a sub process of several processes.
- Standards have different scope e.g. one can concern the contents of a product and another the way to produce it.

From above we can generally say that we do not have a single way of analyzing and comparing standards. Instead it is necessary to use both a more formal approach i.e. based on some kind of objective measure and also an informal approach i.e. some kind of evaluation and/or judgment. This will be further described below.

Since we have to limit the number of standards in this work we have selected a total of six standards used for different applications namely

- IEC 61508 “Functional safety of electrical / electronic / programmable electronic safety-related systems”
- IEC 61713 “Software dependability through the software lifecycle processes – Application guide”
- RTCA/DO-178B ”Software Considerations in Airborne Systems and Equipment Certification”
- IEC 601-1-4 Medical Electrical Equipment – Part 1: General Requirements for Safety – 4. Collateral Standard: Programmable Electrical Medical Systems.
- EN 50128 Railway Applications: Software for Railway Control and Protection Systems”
- EN 954 safety of machinery: “Safety-related parts of control systems”

Also, for the work described here, SPICE (ISO/IEC TR 15504) is used as reference. Special considerations will be taken to test, verification and validation aspects.

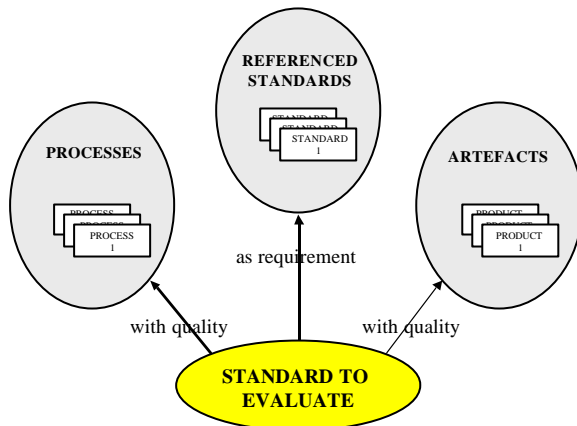
The result of this work is twofold; first, to define a pragmatic procedure that can be used for further standards as well, and second, to make a judgment of the analyzed standards and how they are related.

2. Project description

The project is ongoing and is a joint venture between DELTA Denmark and SP Sweden. The project is sponsored by NORDTEST. The final results of the survey will be published, at the latest, in December 2001. Since DELTA and SP have some different scopes this work will be approached from a process side and from an artifact side. This is of importance when describing the informal aspects of standards. If opinions differ significantly then we can conclude that a standard leaves room for interpretations and vice versa.

3. Top view

The picture below shows the top-down approach for the work within this project.



The evaluated standard may have references to other standards that are considered as requirements. These standards can in their turn be analyzed if necessary thus making a recursive procedure possible. An arrow in this case only describes if such a connection exists or not.

The evaluated standard is also mapped to processes and artifacts. The processes are initially specified by SPICE but extended if necessary. The artifacts are built up successively during analysis. Arrows in these cases include quality description i.e. informal text describing the connection. This includes for example criticality aspects, amount of connection, and contents.

Since some of the standards also define models for criticality classification these will also be discussed. Again, note that the analysis can easily be extended with more standards if necessary.

4. Single standard evaluation

The following steps are made for the analysis:

1. Map the current standard to requirements included in referenced standards.
2. Map the current standard to the set of SPICE processes. Extend it if necessary. For each connection describe the corresponding quality.
3. Map the current standard to the current set of artifacts. Extend it if necessary. For each connection describe the corresponding quality
4. Create an abstract of the standard describing its scope.

5. Standard comparison

When standards have been evaluated separately we could perform comparisons in the following ways:

- Comparing abstracts.
- Making (informal) evaluations of the standards and comparing them.
- Comparing the qualities of the connections for processes and artifacts.
- Comparing amount of referenced standards (when requirements).
- Defining metrics for the included elements within the areas (processes, artifacts and referenced standards). Using metrics for comparisons.
- Focusing the comparison on a specific aspect (here test, verification and validation).

6. Expected results

The results of the work will be recorded in a report. A number of results will be given such as:

- Description of the method for evaluation.
- Similarities between standards and completeness of each standard (i.e. how many other standards are necessary to be complete).
- Visibility of the likes and differences in formal testing requirements.
- Feasibility of SPICE framework for safety related standards.
- Applicability and comparison of models for safety criticality classification.

Or expressed more generally: to create and transfer a judgment on safety related standards to the reader with specific considerations to test, verification and validation.