Reuse of Existing Software in Space Projects — Proposed Approach and Extensions to Product Assurance and Software Engineering Standards

Manuel Rodríguez[1], João Gabriel Silva[1,*], Patricia Rodríguez-Dapena[2], Han van Loon[3], and Fernando Aldea-Montero[4]

[1] Critical Software S.A., Parque Industrial de Taveiro Lote 48, 3045-504 Coimbra, Portugal
{mrodriguez, jgabriel}@criticalsoftware.com
[2] SoftWcare S.L., C/ Serafín Avendaño 18 Int., 36201 Vigo, Spain
rodriguezdapena@softwcare.com
[3] SynSpace AG, Hardstrasse 11 CH - 4052 Basel, Switzerland
hvl@synspace.com
[4] ESA/ESTEC, Noordwijk, Netherlands
Fernando.Aldea.Montero@esa.int

Abstract. Reuse has the potential to substantially decrease the skyrocketing costs of space missions. The European Space Agency sponsored a study on the product assurance aspects of reuse of previously developed software on space projects, called PA-PDS. Several recommendations emerged from this study, along with change proposals to the main standards of software engineering and software product assurance followed by the European space industry. This paper describes those recommendations, the scope of reuse in the existing standards, and provides a justification for the proposed changes to them. A working group has been formed to develop a standard specifically addressing product assurance aspects of reuse.

1 Introduction

Developing large space software systems with demanding dependability and safety requirements entails significant costs. This is the reason why many organizations have begun to consider implementing such systems using existing software components. The European Space Agency (ESA), like other government and system developers acquiring software-intensive space systems, faces quite often the problem of assessing whether these components proposed for reuse are 'good enough' for the intended usage. This creates a need to specify what can be considered as 'sufficient evidence' of the adequacy of a given software component, from a product assurance viewpoint. This was the main motivation for the PA-PDS study that is at the origin of this paper.

[*] João Gabriel Silva is a professor at the University of Coimbra, Portugal, acting in this study as a senior consultant to Critical Software.

X. Franch and D. Port (Eds.): ICCBSS 2005, LNCS 3412, pp. 258 – 267, 2005.

PA-PDS is an ESA sponsored study aimed at defining the product assurance aspects required to ensure that development with reuse of existing components is a success.

There is a fundamental change required in the approach to system development for component-based systems. In the traditional custom-development approach, requirements (or system context) are first identified, then the software architecture is defined, and finally a (custom) implementation is undertaken. However, this approach needs to be adapted when some existing components are proposed for reuse, since it is unlikely that the marketplace will yield any products that fit the a priori requirements and architecture. Instead, it is necessary to consider the tradeoffs between the system context, architecture and potential candidates for reuse in the marketplace simultaneously. Any of these three parameters may have an impact on the other two, so none can be set without knowledge and accommodation of the others. This substantial change necessitates the adaptation of several industrial processes used to develop systems. The move to reuse-based systems development is not just an engineering or technical change, it is also a business, organizational and cultural change.

The so-called Commercial Off-The-Shelf (COTS) software is a subset of the overall domain of input assets for reuse in the space domain. With this terminology one means the reuse of general-purpose software available on the market usually with no access to the source code. The space industry, due to its small size compared to other software markets, is not known as a primary source of COTS software products. A few exceptions to this exist however, mostly at the ground segment level. Notably in the US, where there is a considerably technology overlap between the space and defense markets, some significant space COTS software products are available (e.g. EPOCH mission control system [1]). In the European space industry, the usage of COTS software products for dependability-critical systems has mostly taken the form of reusing real-time operating system kernels (e.g., Virtuoso [2]).

In the framework of the PA-PDS study, Pre-Developed Software (PDS) is defined as existing software components developed outside the framework of a space project or in previous space projects and used either ‘as is’ or with adaptations. This is a quite general definition not implying any contractual, structure, location or usage restriction. In particular, this definition encompasses not only COTS software but also in-house (or custom) developed software, shareware, freeware, public-domain (or open source) software, and ‘copyleft’ software (e.g., GNU software). As described later, the PA-PDS study has shown that careful reuse of PDS has the potential to significantly reduce development costs and to lead to space systems requiring less time to specify, design, develop, test and maintain, yet satisfying the stringent reliability and quality requirements. To achieve this, new requirements and processes must be defined within the European space standards.

The structure of the paper is as follows. Section 0 provides an overview of the state of the practice on PDS reuse in different domains. The PA-PDS study is described in Section 0, where the motivations, purpose, and main results are presented. Section 0 focuses on the extensions that have been proposed for inclusion into the main European space standards on product assurance and software engineering. It also introduces the main activities carried out by a recently formed ESA working group, whose purpose is to develop a standard specifically addressing product assurance aspects of reuse. Finally, Section 0 concludes the paper.