Assurance Evaluation for OSS Adoption in a Telco Context

Claudio A. Ardagna[1], Massimo Banzi[2], Ernesto Damiani[1],
Nabil El Ioini[3], and Fulvio Frati[1]
1 Department of Information Technology, University of Milan
{ardagna,damiani,frati}@dti.unimi.it
2 Telecom Italia - Technology & Operations
massimo.banzi@telecomitalia.it
3 Free University of Bozen-Bolzano-nabil.elioini@unibz.it

Software Assurance (SwA) is a complex concept that involves different stages of a software development process and may be defined differently depending on its focus, as for instance software quality, security, or dependability. In Computer Science, the term assurance is referred to all activities necessary to provide enough confidence that a software product will satisfy its users' functional and non-functional requirements.

Here we focus on security and dependability assurance, intended as the activity aimed at increasing the level of confidence that a software product is operating as intended and is free of faults. Recalling that assurance activities are process-oriented, the security activities are mapped on a traditional waterfall-based development process. Of course, cooperative and agile development processes like the ones used for open source do not lend themselves to all assurance tasks, making it difficult in practice to define assurance tasks for open source solutions[1]. Some approaches in the past have been provided in the context of big open source projects, such as Linux, where a patch-based approach has been adopted for the definition of assurance tasks.

Our work is aimed at defining assurance tasks for open source products in mission-critical context, such as telecommunication (Telco) applications. We consider a Telco environment, since it is one of the most challenging in which the adoption of the open source paradigm may be successful and play an important role. Currently a big Telco Player like TelecomItalia is trying to move from an "opportunistic" approach to OSS, to a strategy on how approaching OSS spanning through three main branches: **the evaluation** of the actual (quantified if possible) value that opening an internally developed platform can have, **the definition** of a full governance procedure that allows Project Managers to decide the approach to OSS related to the criticism and the characteristics of the application to implement, and **the creation** of a community of peers that share experience, skills. The drivers for all these initiatives are: the reduction of Total Cost of Ownership (TCO) and the flexibility and dynamicity of solutions implemented using OSS components.

[1] E. Damiani, C.A. Ardagna, and N. El Ioini, Open Source Systems Security Certification, Springer, December, 2008