Exploring the potential of OSS in Air Traffic Management

Jean-Luc Hardy and Marc Bourgois
EUROCONTROL Experimental Center
Innovative Research Department
91222 Brétigny-Sur-Orge CEDEX France
{jl.hardy,marc.bourgois}@eurocontrol.int,
WWW home page: http://www.eurocontrol.int/eec/

Abstract. This paper introduces a project that aims at defining an Open Source Software (OSS) policy in the field of Air Traffic Management (ATM). In order to develop such a policy, we chose to investigate first a set of predictive hypotheses. Our four initial hypotheses were presented, refined and discussed in bi-lateral meetings with experts in the ATM field and in several conferences and workshops with OSS experts. At a roundtable, jointly organized by CALIBRE and EUROCONTROL, we confronted early open source experiences and insights in the ATM domain with experiences and knowledge from a panel of OSS experts and practitioners from academia and industry. The revised initial hypotheses are presented using a fixed format that should facilitate further evolution of these hypotheses.

1 Introduction

EUROCONTROL is the European Organisation for the safety of Air Navigation. It has as its primary objective the design and development of a safe and seamless pan-European Air Traffic Management (ATM) system in Europe. Founded in 1960 as a civil/military intergovernmental organisation, it is now a world leader, pioneering advances in ATM technology, operational procedures and system interoperability. The number of Member States has grown from the original 6 to 36.

Many ATM projects are implemented partially or totally through software developments. Proprietary software is the usual practice in the ATM industry. Most software produced by the EUROCONTROL Agency is outsourced. Presently, OSS principles and licenses are not included in the official Intellectual Property Right (IPR) policy of EUROCONTROL.

The next section presents the structure of the study in five parts: a project (OSIFE), a network (CALIBRE), an event (roundtable), a formalism, and a knowledge base.

2 The OSIFE project

By the middle of 2004 we started a study project to get a better understanding of the potential impact of the OSS movement on ATM. The OSIFE acronym was coined: "Open Source Implications For EUROCONTROL". We started by reviewing the

Please use the following format when citing this chapter:

Hardy, J.-L., and Bourgois, M., 2006, in IFIP International Federation for Information Processing, Volume 203, Open Source Systems, eds. Damiani, E., Fitzgerald, B., Scacchi, W., Scotto, M., Succi, G., (Boston: Springer), pp. 173-179

basic literature concerning Open Source and Free Software. The outcome was a definition of the scope, the objective and the method of the project.

In terms of scope, we decided to limit our investigation to the impact of OSS on the core business of EUROCONTROL, i.e. ATM. In terms of objective, we want to understand if, when and how OSS could impact the business in ATM. In terms of method, we chose to describe our insights as a set of predictive hypotheses. To launch the debate, four broad hypotheses about the potential of OSS for ATM were introduced [1]. They can be summarized as follows: the OSS paradigm will

1. facilitate the harmonization of ATM,
2. maintain or improve the quality of ATM software,
3. affect the ATM industry in a positive way,
4. help EUROCONTROL to better meet its public service obligation.

3 The CALIBRE network

Through this first presentation, it became clear that the ATM community was interested about OSS, that further investigations were needed, and that networking was necessary to gather facts and arguments about the 4 hypotheses. During 2005, networking proceeded twofold: within the ATM world and within the OSS world.

To explore the ATM world, we made numerous contacts inside EUROCONTROL. It transpired that many experts involved in the improvement of ATM systems are unaware or unclear about the OSS paradigm. For example, OSS is often wrongly considered as equal to freeware. However, we also had the nice surprise to discover a few projects and experiences where the OSS concepts were used or considered helpful.

To explore the OSS world, the CALIBRE consortium [2] quickly appeared as the appropriate network. It is supported by the European Sixth Framework Programme. As part of its commitments to promote the OSS paradigm in Europe, CALIBRE facilitates an industry forum called CALIBRATION, which provides contacts with representatives of other industries.

The CALIBRE conference at Limerick in September 2005 was a first opportunity to present the 4 initial hypotheses of OSIFE to the OSS community and to collect feedback. The second opportunity was a CALIBRE workshop at Krakow, about quality, safety and security in OSS initiatives. In preparation for the Krakow workshop we were stimulated to deepen our comprehension of these issues: following discussions with EUROCONTROL colleagues at the EUROCONTROL Maastricht ATC centre we introduced two new hypotheses, one about safety and the other about security.

4 The OSS-in-ATM roundtable

Assuming that the stimulating spirit of the CALIBRE network could help to increase the OSS awareness among ATM circles, we dreamed about a meeting between both worlds: the OSS world and the ATM world. Aside the OSS2005 conference in June 2005 at Genova, the idea of such a meeting was proposed to B. Fitzgerald, CALIBRE project leader and immediately endorsed. The format chosen for this meeting was a roundtable on the subject: "Potential of OSS in ATM" [3]. It was co-organised with CALIBRE and took place in December 2005 at the EUROCONTROL Experimental Center (South of Paris). It drew a participation of 28 persons from the CALIBRE expert circle, the EUROCONTROL staff, and the ATM industry. Several outcomes were expected from such a confrontation: (i) increased awareness of the OSS paradigm in the ATM circles; (ii) better appreciation of the relevance of early open source experiences in the ATM domain; and (iii) modification or confirmation of the validity of the hypotheses.

5 The formalism used to describe hypotheses

The discussion about our hypotheses and the difficulty to extract knowledge from the abundant OSS literature calls for the adoption of some kind of formalism to describe pros and cons. The CALIBRE team has used SWOT analysis in previous cases to help clarify the potential of OSS [4].

In this paper, we use the SWOT analysis to articulate a model that should facilitate the identification of the critical semantic elements of each hypothesis and should help to trace the evolution of the hypotheses.

The SWOT analysis of a system classifies facts intrinsic to the system in terms of strengths or weaknesses and facts intrinsic to its environment in terms of opportunities and threats. For the purposes of our research, we try to predict how strengths and weaknesses of a system in the environment – the OSS paradigm – translate to opportunities and threats for the system in focus – the ATM system.

Systematic matching of threats with strengths and opportunities with weaknesses leads to the identification of positive (win-win) and negative (loose-loose) synergies between a system and its environment:

a) (How) could OSS strengths become an opportunity to compensate or correct some of the weaknesses of the ATM systems?
b) (How) could OSS weaknesses become a threat for the ATM systems?

6 The knowledge base of hypotheses

The preliminary hypotheses of the OSIFE project have been revisited using insights that were collected through the networking process, including lessons learned from the roundtable. To respect the 6 pages limitation of the proceedings, only 3 critical hypotheses are presented in this paper, about quality, safety, and security. Quality, and more specifically safety, is the bread and butter of the ATM domain.

6.1 On the quality of ATM software

In our research we take an external perspective on quality. We interpret wide adoption of software and complexity of systems constructed with that software as indications of high quality software.

It is a fact that ATM systems are complex, essentially because of the highly sophisticated user interfaces and the stringent performance requirements put onto the ATM systems. The complexity of ATM systems is continually increasing with their ever-increasing interconnectivity.

6.1a Fact (ATM weakness):

Most ATM software applications are complex.

There is ample evidence of the wide adoption of OSS for tools like operating systems, databases etc. which are undoubtedly complex. Such achievements are only possible if OSS indeed has high intrinsic quality.

6.1b Fact (OSS strength):

OSS can result in complex applications with high quality.

Several authors are sceptical about generalisations of quality statements on OSS, for two reasons: either because in the absence of a hierarchical development team where one person is in charge of the product, "modifications can be made to an individual module that could have a deleterious effect on the maintainability of the open-source software product as a whole" [5], or because "in the absence of firm design and documentation standards, and the ability to enforce those standards, the quality of the code is likely to suffer" [7] .

6.1c Fact (OSS weaknesses):

Quality of OSS cannot be guaranteed in the absence of a hierarchical development team and firm standards for design and documentation.

Taking all these arguments together we logically come to:

6.1d Hypothesis:

OSS can result in complex ATM applications with high quality, provided that a hierarchical development team and firm standards for design and documentation are enforced.

6.2 On safety in ATM

The first objection raised when considering a change to the ways ATM systems are developed or operated is that the change will not be compatible with the stringent safety-critical constraints of the field. Not surprisingly, this objection was prominent in the feedback from attendees at presentations on the potential introduction of OSS, both from an ATM audience [1] and from an OSS audience [8, 9].

During our research we noted the lack of OSS penetration for safety-critical applications. No examples could be found in the literature, neither could any be recalled by the OSS expert panel at the roundtable.

6.2a Fact (OSS weakness):

OSS does not propose specific solutions for safety-critical systems.

6.2b Fact (OSS strength):

By facilitating the peer review process,
an OSS approach can eliminate some safety-critical problems.

Does this mean that the ATM domain cannot benefit from the potential of OSS? No, it merely means that the safety-critical applications in ATM should not be the first to be explored. But then again, there are very many non safety-critical components in the overall ATM system, so plenty of opportunities to build experience with OSS exist. In fact, one ATM expert at the roundtable ably, but provokingly argued that ATM applications are not safety-critical at all, because by definition the traffic is constantly kept conflict free, offering several minutes of reaction time for the humans in the system to deal with outages of automated components. The argument continues to identify the avionics components as the truly safety-critical parts. Nonetheless we can conclude:

6.2c Hypothesis:

The safety of ATM systems will be improved through OSS practices, provided that the peer review process is actively engaged in.

6.3 On security of ATM systems

The second objection that comes to mind when considering the introduction of OSS in ATM is that OSS could create security problems. The security issue has gained prominence because of 9/11. This event has demonstrated that security attacks beyond the worst scenario ever imagined for aviation can happen and that a creative paranoia to guard against such attacks is justified.

6.3a Fact (ATM weakness):

Security flaws in ATM can have catastrophic consequences.

In the OSS literature, the concept of security symmetry is discussed [10]. As summarized by Brian Fitzgerald [private communication]: «'Security Symmetry' is a reference to Ross Andersen's conjecture (discussed in [11]) which proposes that open systems may be more prone to security attacks (because 'evil' crackers can see the code) but this is balanced by more opportunity to identify and fix potential security flaws in the first place (because 'good' hackers can also see the code). »

6.3b Fact (OSS weakness):

'Evil' crackers can exploit security risks.

6.3c Fact (OSS strength):

'Good' hackers can detect and eliminate security risks.

In addition, the OSS paradigm allows software users to check any code incorporated:

6.3d Fact (OSS strength):

Users can perform a security screening of any code incorporated.

Considering ATM, the security of the operational system (i.e. the run-time system) is normally guaranteed by strict physical isolation. For example, operational ATM systems are completely isolated from the internet, and regular audits to ensure this are common practice.

6.3e Fact (ATM strength):

Non-ATM systems (including people) cannot access the ATM operational system.

When taken all together, 6.3e cancels out 6.3b:

6.3f Hypothesis:

The security of the ATM system will be improved through OSS practices, particularly if the software is subject to a security screening.

B. Fitzgerald concluded: «Breaking the security symmetry would be trying to shift the balance more towards realising the benefits, at the expense of incurring the risks.» For ATM, leveraging the security symmetry would require a security screening in the acceptance protocol.

7 Conclusions

This article exploits a formalism for systematically accumulating knowledge about the potential of the OSS in ATM. Starting from a preliminary set of predictive hypotheses, a networking process, engaging both the OSS and the ATM worlds, has been efficient in producing novel insights. The analysis of the outcome from the roundtable is still going on and further refinement of our hypotheses is expected.

8 References

1. J-L. Hardy and M. Bourgois, Open Source Implications for EUROCONTROL (OSIFE), in: Proceedings of the 3rd EUROCONTROL Innovative Research Workshop, edited by Eurocontrol (December 2004).
2. CALIBRE, Limerick (March 6, 2006); http://www.calibre.ie.
3. M. Bourgois, J-L. Hardy, J. O'Flaherty, and J. Seifarth (Eds), Proceedings of the roundtable "Potential of OSS in ATM" (Brétigny, France, December 2005); http://www.oss-in-atm.info.
4. P.J. Ågerfalk, A. Deverell, A. Fitzgerald, and L. Morgan, Assessing the Role of Open Source Software in the European Secondary Software Sector: A Voice from Industry, in: Proceedings of the First International Conference on Open Source Systems (OSS2005), edited by M. Scotto and G. Succi (Genova, Italy, July 2005), pp. 82-87; http://oss2005.case.unibz.it/download.php.
5. S. Schach, B. Jin and D. Wright, Maintainability of the Linux kernel, in: Proceedings of 2nd Workshop on Open Source Software Engineering, ICSE2002, edited by J. Feller, B. Fitzgerald, F. Hecker, S.C. Hissam, K.R. Lakhani, and A. van der Hoek (Orlando, Florida, 2002); http://opensource.ucc.ie/icse2002.

6. J. Feller, B. Fitzgerald, S. Hissam, and K. Lakhani (Eds.), Perspectives on Free and Open Source Software (The MIT Press, Cambridge, USA, June 2005).
7. S. Rusovan, M. Lawford and D. Parnas, Open Source Software Development: Future or Fad? In: [7], pp. 107-121.
8. CALIBRE, 2nd International Conference: The Next Generation of Software Engineering Integrating Open Source, Agile Methods and Global Software Development (Limerick, Ireland, September 9, 2005), http://www.calibre.ie/events/conferences.php.
9. CALIBRE, Quality and Security Workshop (Krakow, Poland, October 18, 2005); www.calibre.ie/events/workshops.php.
10. J. Feller, B. Fitzgerald, S. Hissam, and K. Lakhani, F/OSS Project Leaders and Developers, in: [6], page XXIX.
11. R. Anderson, Open and Closed Systems Are Equivalent, in: [6], pp. 127-142.