Open Source Software in the Defence Industry

Anthony Harrison

Thales

anthony.harrison@uk.thalesgroup.com

Abstract: There are an increasing number of defence programmes incorporating open source software as the defence industry moves from proprietary closed systems towards open systems. It is also perceived as offering 'value for money', which in these challenging times of diminishing budgets is clearly seen as a distinct advantage. Whilst there are currently few open source applications specifically developed for the defence market, there are an increasing number of applications and systems being developed with, or based on, open source components; this philosophy fits in with the customer's objectives to remove the potential of vendor lock-in and the significant cost benefits that this entails. The US Defence market is increasingly taking advantage of OSS, actively promoted through various groups within industry and government, including Mil-OSS and Open Source for America – the next opportunity is for the UK market to be similarly liberated.

Keywords: Open Source, Open Systems, COTS, Defence

INTRODUCTION

Whilst open source software (OSS) is now an established part of mainstream computing with an ever increasing number of applications being developed with, or based on, open source applications and components, there is still some concern over using such software in certain domains. The reason that some domains have been reluctant to take advantage of the undoubted benefits of OSS is often due to misunderstanding of what using OSS actually means. However, in many cases, the use of OSS is no different to selecting a commercial COTS component or package.

One such domain which has limited adoption to date is the defence sector, although this is gradually changing. The use of OSS in this domain, particularly within operational (i.e. field) systems has required education of both the supplier community and the customer, particularly in terms of the impact that using OSS may introduce with regards to national security. Some of the biggest challenges are related to the obligations of a supplier; some of the common misunderstandings include:

- It isn’t possible to mix OSS with proprietary software
- It is necessary to release all of your source code
- If you use OSS, you can’t charge for any of the software as everything is free

Clearly these misunderstandings require that both the supplier and customer communities are well-educated in the OSS market particularly as OSS challenges many traditional theories in economics, software engineering, and project management. There always needs to be careful assessment of each OSS component with regards licencing to ensure national security is not comprised; but it is possible particularly if components with permissive licences are selected. However, there are non-tangible benefits of using OSS as it often results in more reliable and innovative solutions, two essential attributes required of any defence system.

Over the last 10 years, the defence market has undergone a number of significant changes following the increasing adoption of COTS hardware and software systems. This, together the greater reliance on systems built using recognised standards and a need for systems to be increasingly flexible to continually changing mission needs has made OSS a viable proposition within many defence systems. This is part of the move from proprietary closed systems towards open systems in order to meet the customer's objectives to avoid the potential of vendor lock-in and control costs in order to get 'value for money'.

OSS offers a different development model to the traditional system development model with a number of different approaches:

- Existing OSS used unmodified and integrated into a solution. This is very similar to integrating a 3rd party COTS product.

- Existing OSS is evolved, potentially collaboratively and not necessarily by the original developers, to meet a specific need.

- By choice, developers provide solutions as OSS.

Some of the benefits to the customer from the use of Open Source Software include

- Enhanced system reliability. One of the perceived primary benefits of is the apparent increase in quality, demonstrated by a reduced number of defects. The quality of software produced by the Open Source community often exceeds that produced by purely commercial organisations. Through the use of communities, defects may be fixed within hours of being detected, a process which is undoubtedly assisted by the availability of the source code.

- The software is also likely to be more secure as the source code is always available for audit review.

- Solution stability. Many OSS products tend to conform closely to standards efforts. This has a beneficial effect, since standards normally change slower than COTS and interchange formats remain stable. This also results in upwardly-compatible releases of applications which ensure that the investment in the applications (e.g. training, data, etc) can be retained.

- Reduced total acquisition cost. OSS projects are available free of royalties and licence fees, resulting in a reduction in the initial acquisition cost. Better adherence to standards permits competition in the market which also reduces vendor lock-in.

- Enhanced support. Although the use of OSS does not guarantee free support, the fact that an OSS application or component has been used by others increases the choices available for obtaining support. In principle, as anyone can see the source code, anyone can maintain it. Support options may also include different licencing arrangements which may remove certain restrictions with regards use of the OSS in a solution.

All of the benefits to the customer apply equally to a supplier who uses OSS as part of the solution. However there are some additional benefits including:

- Ease of enhancement. OSS components are designed to be evolved which may be required if the base component requires a change in order to form

part of the final solution. Through the use of active communities, the speed of adoption and evolution is far quicker than with developed code.

- Reduced training costs. As OSS software becomes more widespread and popular across development teams, the need to train in proprietary products is reduced. In many cases, the engineers are already familiar with the software as they are using the software at home.

- Reduced development schedule and costs due to reduced amount of developed code. Clearly some cost is still associated with OSS in ensuring that it can be integrated into the total solution but being able to react to changing operational requirements quickly is seen as great advantage.

- Solution derisking. As many defence systems require 'proof of concept' systems to be developed in advance of a major deployment, the use of OSS provides agility in the early solution development and minimises the initial costs often associated with proprietary components.

Use of OSS isn't without pitfalls. One major risk associated with the use of OSS is concerned with the selection of OSS products. The licence agreements associated with each components needs to be well understood before committing to one or more OSS components, particularly with regards the compatibility of the different licences. Another issue that needs to be carefully considered, particularly if the products are to be used in a solution with safety aspects, is an independent assessment of the quality of the product. Whilst this is true for all projects utilising OSS, the impact on national security makes this risk particularly important, particularly if the licences are not permissive.

Whilst there might not be OSS versions of a combat management system or missile guidance system (yet!), there are increasing examples of systems which include a number of OSS components as part of key capabilities within a system. The US DoD has recognised the benefits of open source as part of the cultural change away from proprietary implementations to leverage the benefits of open solutions. The Open Technology Development roadmap published by DoD [1], identifies that OSS supports one of the key advances required '…to rapidly adapt and extend existing software capabilities in response to shifting threats and requirements without, being locked in to a specific vendor or held hostage to proprietary technologies.' A review of the use of OSS in the US for the DoD identified that OSS was appropriate in four key areas [2]:

- Infrastructure Support

- Software Development

- Security

- Research

In the US, OSS adoption is supported by an active and patriotic grassroots movement who believe in adopting open technology innovation philosophies to effectively defend the US. This movement, under the umbrella title of Mil-OSS (***www.mil-oss.org***), has connected and empowered an active community of civilian and military open source software and hardware developers across the United States (and elsewhere). The first military based open source software conference was organised by Mil-OSS in 2009; this has now become an annual event with the 3rd conference being held in August 2011. The idea has also been adopted outside the

US, with a similarly targeted conference being held in Israel in 2010. An opportunity clearly exists to hold a similar conference in the UK of like-minded organisations and individuals.

In 2008, the US established a forge (***www.forge.mil***) to be a collaborative environment in the development of software and services for the DoD. It includes a repository of over 300 defence related OSS applications, although access is currently being restricted to appropriately authenticated organisations by the DOD (a common access card (CAC) obtained from the DoD is required to access the repository). Here lies one of the great challenges facing the military domain and the use of OSS; making the software freely available means there is limited control as regards who is using the software (which could clearly include an opposing nation). By creating a limited forge, funded by government money, there is clearly a reluctance to make the OSS widely available (including to the UK) outside the DoD. There is also a change required in the approach to software procurement owing to the differences in ownership of OSS products and components.

Although access to some of the projects is restricted, some of the projects are widely available. Some examples include:

- OpenCPI (***www.opencpi.org***) which is a realtime embedded computing solution
- FalconView (***www.falconview.org***) which is a PC based Mapping Application
- Opticks (***opticks.org***) which is an expandable remote sensing and imagery analysis software platform.
- OpenStack (***www.openstack.org***) which is a collection of open source technology products delivering a scalable, secure, standards-based cloud computing software solution.
- Nebula (***nebula.nasa.gov***) which offers sets of open-source components that can be integrated into full (and self-service) platforms that range from high-capacity computing, virtualized systems and more, in a highly scalable environment and supports integrated reporting and policy compliance.

Of course there are also many OSS components used which are more commercially focused. Examples include Apache webserver, Nagios for server monitoring, PostgresSQL and Tomcat.

In the UK, there is currently no forum within the defence industry for promoting OSS within defence programmes. However, as the trend towards open systems and COTS components to be used in defence systems has increased, the run-time environment and middleware layers typically consist of components which are not specific to the defence industry. This has been demonstrated in a number of recent middleware implementations including OPUS produced by Thales, which contains a number of OSS components. Additional components in OPUS which are not based on existing OSS components are also released using an Open Source licence. Although OPUS was initially developed to meet some specific programme requirements in the Naval domain, there is nothing in the implementation which restricts its use to this domain, or any other military or non-military domain.

Some components used in OPUS include

Component	Scope
OpenSLP	Implementation of Service Location Protocol
MySQL	Relational database management system
XMLBeans	Java library for accessing XML documents
Boost	Portable and high quality C++ source libraries

Component	Scope
GNUSockets	Implementation of socket library
Tomcat	Java Application server
VSIPL	Signal processing library

The OPUS team is also actively contributing to some OSS communities (e.g. OpenSLP), feeding back solutions to issues relating to the use of the commercial software as applied to a real-time military domain.

Although there are limited number of OSS applications used in operational systems, it is common practice to use in research and data analysis activities. One particular research application is Debrief (***www.debrief.info***), which is a maritime tactical analysis application and is used for analysing maritime vessel tracks in 2 and 3 dimensions. It utilises a number of OSS components including OpenMap and was made open source following a rewrite of the original bespoke application. Releasing Debrief as open source benefited the original customer (the UK's Maritime Warfare Centre (MWC)) resulting in an improved application due to a more rapid discovery of bugs, ease of data interchange between analysis partners (other navies) and encouraging 3rd party enhancements to the application which can be exploited by all users. Whilst releasing a previously closed source application to open source can have significant benefits, there clearly needs to make a careful assessment of the source code to ensure that there are no undue security lapses; this is particularly true of any comments in the source code or careless use of variable names.

The trends observed in the last few years in terms of the adoption of open source in commercial applications, are now being recognised by military systems and there is clearly an increasing willingness by both suppliers and customers to consider open source applications to form part of the business infrastructure necessary for applications within a military domain. As more Military Systems are attempting to become vendor independent, OSS offers a viable route to many suppliers in order to achieve open and flexible systems. An increasing number of applications are using OSS as the basis to the final solution and suppliers can see the benefits of releasing software as open source as a way of extending adoption and promoting standards. As conformance to standards becomes increasingly more important, it is considered that the OSS model is likely to have an increasingly important role to play in the development of future military systems, and offer ‘value for money’ which is essential in these challenging times of diminishing budgets.

REFERENCES

[1] Open Technology Development roadmap Version 3.1 – available from http://www.acq.osd.mil/jctd/articles/OTDRoadmapFinal.pdf

[2] Use of Free and Open-Source Software (FOSS) in the US Department of Defence Version (1.2.04) – available from http://www.isd.mel.nist.gov/projects/rtlinux/dod-mitre-report.pdf

BIO

Anthony Harrison is a Software Architect at Thales with over 25 years experience in the IT/defence industry having held key technical positions in a variety of major projects. He has a BSc in Computer Science and Mathematics from Manchester University, a MSc in Mathematical Modelling from Manchester Metropolitan University and is a Member of the British Computer Society with Chartered Engineer and Chartered IT Professional certifications.