TITLE: Standards - Myths, Delusions and Opportunities

TITLE: Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS" [l'Utilisation des produits vendus sur etageres dans les applications militaires de defense "l'Exploitation sans merci des produits commerciaux"]

Standards – Myths, Delusions and Opportunities

(February 2000)

Nic Peeling
(DERA Fellow)
Richard Taylor
(DERA Senior Analyst)

Defence and Evaluation Research Agency,
Woodward Building, DERA Malvern
St Andrews Road, Malvern
Worcs., WR14 3PS, UK
N.Peeling@eris.dera.gov.uk
R.Taylor@eris.dera.gov.uk

Introduction

This paper describes how a new approach to defence standardisation could deliver, for the first time, the benefits that defence standards and Open Systems have for so long promised.

The paper traces the history of defence computing standards. It examines the original benefits that standardisation promised in the defence arena. It examines why so many defence standardisation efforts have failed to deliver on those promises. It then goes on to examine why the original efforts to create a standards-based computing market (the Open Systems movement) also failed. The limitations of a standards-based approach will be described from both a technical and commercial viewpoint. The paper concludes with an optimistic message, that the Internet Standards and the Open Source movement have the potential to deliver on the original promise of the Open Systems movement.

Original benefits promised by standardisation

In the UK, computing standard efforts started in the mid 1960s with the standardisation of Coral 66 as the standard high level language for real-time software, and the Ferranti Argus M700 as a standard computer architecture. The prime benefit intended for such standardisation was the reduction in through-life maintenance costs for software and hardware by reducing the diversity of programming languages and computers utilised in UK MOD systems.

A subsidiary benefit of these early standardisation efforts was the increased portability and reusability of software written in Coral 66 and Argus M700 assembler.

Coral 66 was invented because no existing commercial language (such as Algol 60) had the necessary list of mandatory features:

- Deterministic behaviour needed for real-time, embedded applications;
- Highly efficient run-time code;
- Support for structured programming.

Reduced diversity and *application portability* have remained two of the enduring benefits sought by defence standards.

In the 70s and 80s additional benefits were pursued by defence standardisation efforts:

- Promotion of best practice to industry (e.g. PCTE);
- Interoperability (e.g. ISO OSI);
- Promotion of a market in competing, but compatible, implementations (e.g. Ada and PCTE).

Why did the original promise so often fail?

Although Coral 66 is remembered with some affection, most defence standardisation efforts have either failed totally (e.g. PCTE+), or have been abandoned after the mainstream market passed them by (Ada), or have locked the defence community into niche products (ISO OSI's X.400). The principal reasons for this limited success are:

- You cannot buck the market (e.g. Ada and ISO OSI); eventually COTS products make defence-specific niche products look too expensive, with too little product support;
- You can never truly create a homogeneous defence world (e.g. a country still has to interoperate with its allies, and its suppliers);
- Standards created by committee are often either "lowest common denominator" or very difficult to implement. This leads to industry de-facto standards shooting ahead (e.g. TCP/IP).

Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.

The Open Systems market

By the early 80s the lack of success of defence standardisation efforts was widely understood, if not openly acknowledged. It was at this time that the UNIX supply industry coined the term Open Systems and standards organisation such as IEEE (with POSIX), the OSF and X/Open rose rapidly to positions of great prominence. The defence community saw the Open Systems movement as a chance to reduce operating system diversity, enabling application portability, allowing competitive hardware procurement, all within a framework that commanded mainstream COTS support. Not surprisingly the defence world were early, enthusiastic supporters of the Open Systems movement, with many countries adopting Open Systems standards within their defence computing policies.

Yet again the defence world had backed a loser. The principal reasons that the Open Systems movement fizzled out were:

- The UNIX vendors could not resist differentiating their UNIX offerings in order to lock customers into their particular flavours of UNIX. Consequently the promise of application portability was undermined, and software vendors usually only supported a few of the largest vendors, and many abandoned UNIX altogether for the more homogeneous Microsoft world;
- The operating system that has the most applications wins. Microsoft tied Windows very closely to the PC, whereas the leading UNIX suppliers tied their operating systems to their own proprietary hardware. As PC sales took off, Windows came to be the favoured desktop operating system for software vendors to support. UNIX and Open Systems retreated into the server operating system market, and in the 90s Microsoft started to take that away from them with their NT operating system.

Common Operating Environments

In the late 90s the UK's MOD accepted that the Open Systems movement was not going to deliver an answer to its needs for computing standards and started the development of Common Operating Environments (COEs) and the UK Defence Interoperability Environment (DIE). The COEs and DIE were comprised of a pragmatic mixture of de-jure and de-facto standards, and proprietary products. Unlike the US's DII COE, the UK approach was standards-based and was not a software build and system integration infrastructure. Consequently the DIE and COEs were intended to promote, rather than guarantee, interoperability and application portability.

The COE and DIE initiatives have promoted a major shift in the procurement patterns of MOD projects, with greater adoption of Windows on the desktop, and a move towards a domain-based approach to security.
The COEs and DIE approach creates a number of challenges:

- Can the definition of the COEs and UK DIE evolve at a rate that matches the furious pace of change in the marketplace;
- Given that the COEs and UK DIE evolve at a similar rate to the IT marketplace, there is a significant issue in either keeping defence systems up to date with the latest COEs and DIE, or of managing multiple legacy systems;
- The situation of whether a pragmatic approach that includes de-facto and proprietary standards is consistent with guidelines for open competition, is not totally clear.

Given that the benefits of the COEs and UK DIE are less clear cut than an approach that seeks to guarantee interoperability and application portability; and that the costs of maintaining and applying a rapidly evolving set of standards will be non-trivial; only time will tell if the COEs and DIE approach is cost effective.

The Way Ahead? - Internet Standards and Open Source

The last two years has seen a phenomenal growth in the usage and profile of both Internet standards (such as HTML and XML) and Open Source implementations (such as Linux). Both these movements have been fuelled by the dramatic growth of the Internet. These movements are driven by forces that make them of particular interest to the defence community:

- The Internet by its nature is not tied to any particular proprietary hardware or software platforms;
- The Internet's focus is on interoperability. This coincides with the emergence of extranets, which have convinced many organisations that interoperability with the outside world (customers, suppliers and partners) is a more important business driver than intra-organisational interoperability. As a consequence the roie of proprietary standards, such as Microsoft Office formats, as a mechanism for interoperability between organisations is in decline;
- The Internet and Open Source communities are led by engineers. This has two very important effects: firstly, that it is relatively free from commercial politics and "dumbing down"; and secondly, that this world takes implementation issues very seriously;
- The Open Source method of licensing software means that it is virtually impossible for manufacturers to produce differentiated products that undermine application portability. For this reason it is possible that Linux may soon become the software vendors non-Windows platform-of-choice;

- The Internet and Open Source communities are able to attract massive development resources, much larger than even a company of Microsoft's size can deploy;
- Open review of source code leads to two very important properties: firstly, open source software over time becomes extremely robust; and secondly, open review is coming to be seen as the key to controlling software vulnerabilities, and the Open Source model makes patches to vulnerabilities available very fast indeed.

The defence world should consider whether the Internet and Open Source communities are now delivering on the promise of the Open Systems movement. In addition there are benefits offered that go beyond anything that current standards can provide:

- Open Source may be the only way of getting the twin benefits of COTS support and visibility of vulnerabilities;
- Open Source may offer an alternative to GOTS and niche-COTS solutions to defence-specific requirements;
- It may be possible to develop defence-specific variants of Open Source programs;
- Given the technology focus of the Internet and Open Source communities, it is possible that the defence world can influence the direction of these communities.

Conclusions

Defence standardisation efforts have traditionally been frustrated by the rapid rise of de-facto COTS standards.

The latest UK defence standardisation efforts based on COEs and the UK DIE are based on a pragmantic choice of de-facto, de-jure and proprietary standards. Only time will tell if these latest efforts provide the benefits of standardisation in a cost-effective way which can keep pace with the rapid developments in the IT marketplace.

This paper argues that the defence community should consider whether the latest developments in Internet Standards and Open Source, offer an opportunity to capture the benefits of Open Systems which the UNIX industry squandered in the 1980s.