

Export Controlled Software

LEVERAGING THE CAPABILITY OF PTC INTEGRITY TO ACHIEVE EFFECTIVE EXPORT CONTROL COMPLIANCE IN A GLOBAL WORKING ENVIRONMENT

Companies today are under increasing pressure to bring more products to market faster, products have far greater levels of software 'on board' and in many cases software functionality can outweigh the look and feel of a product in the mind of a buyer when making their decision, so essentially can be the differentiating component. If we take an aircraft engine as an example, when looking at three engines of equal thrust rating, the engine management system which can attain just one percent efficiency over the others is a big deal, and over the life of that engine the resulting savings can be huge.

Executives are increasingly being asked the question: how are you controlling data movement every day? Can you be sure that the system underpinning your global development is enforcing access rights, permissions and visibility to export controlled software?

To cope with the greater emphasis being placed on software as the 'value add' in products and systems, companies are using all facilities available to bring their products to market faster; including global development, outsourcing, better tools and improved process. Aspects such as improved levels of reuse or creation of families of products from an original concept are common place.

While this global development is accelerating, to support ever-increasing demands for software complexity, those who operate in regulated environments are finding that export control regulations have not evolved at the same pace. To avoid falling short, export control regulations are being forced to invest more heavily in controls and infrastructure to maintain compliance and auditability.

In this white paper, we will look at export controlled software, the challenges this software typically presents, how organisations are usually structured to cope and how the introduction of supporting technology can ease the burden, facilitate greater collaboration, and enhance performance and efficiency going forward.

Introduction

Governments worldwide control the export of goods for various reasons depending on the nature and destinations of the proposed export. The export of strategic goods and technology are controlled because of various reasons including:

- National Security
- National Security
- Foreign Policy
- Proliferation
- Short supply
- Anti terrorism
- Weapons of mass destruction
- Crime control
- Regional stability
- UN or EU trade sanctions or arms embargoes

All countries should have an export control policy, an associated legislation, and enforcement mechanisms. The export of strategic goods and technology is enforced by significantly greater controls than everyday goods, such as antiques, medicines or animal products. Failure to comply with export control regulations can result in a stiff penalty, loss of export license, and in extreme cases incarceration. This is why companies take the subject extremely seriously and usually devote extensive infrastructure to stay on the right side of these regulations.

Whether or not an organisation needs an export licence will typically be determined by four factors: the nature of the goods due to be exported, the destination country, the end use, or possible use of the goods and the licensability of trade activities.

The following checklist outlines the broad categories of goods which are likely to be controlled:

- Items that have been designed for or modified for military use
- Dual-use items, e.g., those that can be used for civil or military purposes
- Associated technology and software
- Goods that might be used for torture
- Anything radioactive or which could be associated with weapons of mass destruction or the nuclear industry

Export Controlled Software Challenges

Looking at the technology and software areas, the list of goods that are controlled is vast, and one is advised to look at the relevant documentation in one's country, such as ITAR, or EAR, for the USA and ECO for the UK.

Most organisations will have mature in-house working practices if subject to export control regulations, and often these working practices will be underpinned by some kind of software system to assist in the application, management and tracking of export licenses and associated documentation. If performed manually these tasks alone can be extremely overwhelming.

If a company produces physical goods, the 'hardware' component(s) are arguably easier to control than any software components, for example one can't email someone a 'surface to air' missile. However, software is different, and during development, electronic transfer is normal, and if development is global, or a customer is outside the organisation's home nation, how can the organisation control data movement every day? Can one be sure that the system underpinning global development is enforcing access rights, permissions and visibility to export controlled software?

How Organisations 'Structure' to 'Cope'

With high profile projects such as the 'Joint Strike Fighter' one would think that countries would 'buddy up', and provide exemptions. However this is not so, despite calls for reform being commonplace.

Export controlled software places unique challenges on the company, it is not like a widget, which is ordered, manufactured and shipped never to be seen again. Software has a lifespan, it is normally maintained and supported, it is frequently enhanced or modified and, in effective organisations, it is frequently reused to spawn new products or versions, and/or families of products, consistently lowering the development cost per product or unit shipped. The problem with export controlled software is that if one is exporting it, the destination country it is being exported to will have export control regulations. It may transpire that supporting, maintaining or enhancing that software is near impossible because of the export controls at 'the other end'. Jumping on a plane and going there may not solve the issue, as the software may now contain, for example, 'American eyes only' data and in this case unless you are a US citizen just looking at the software can be classed as an 'export'.

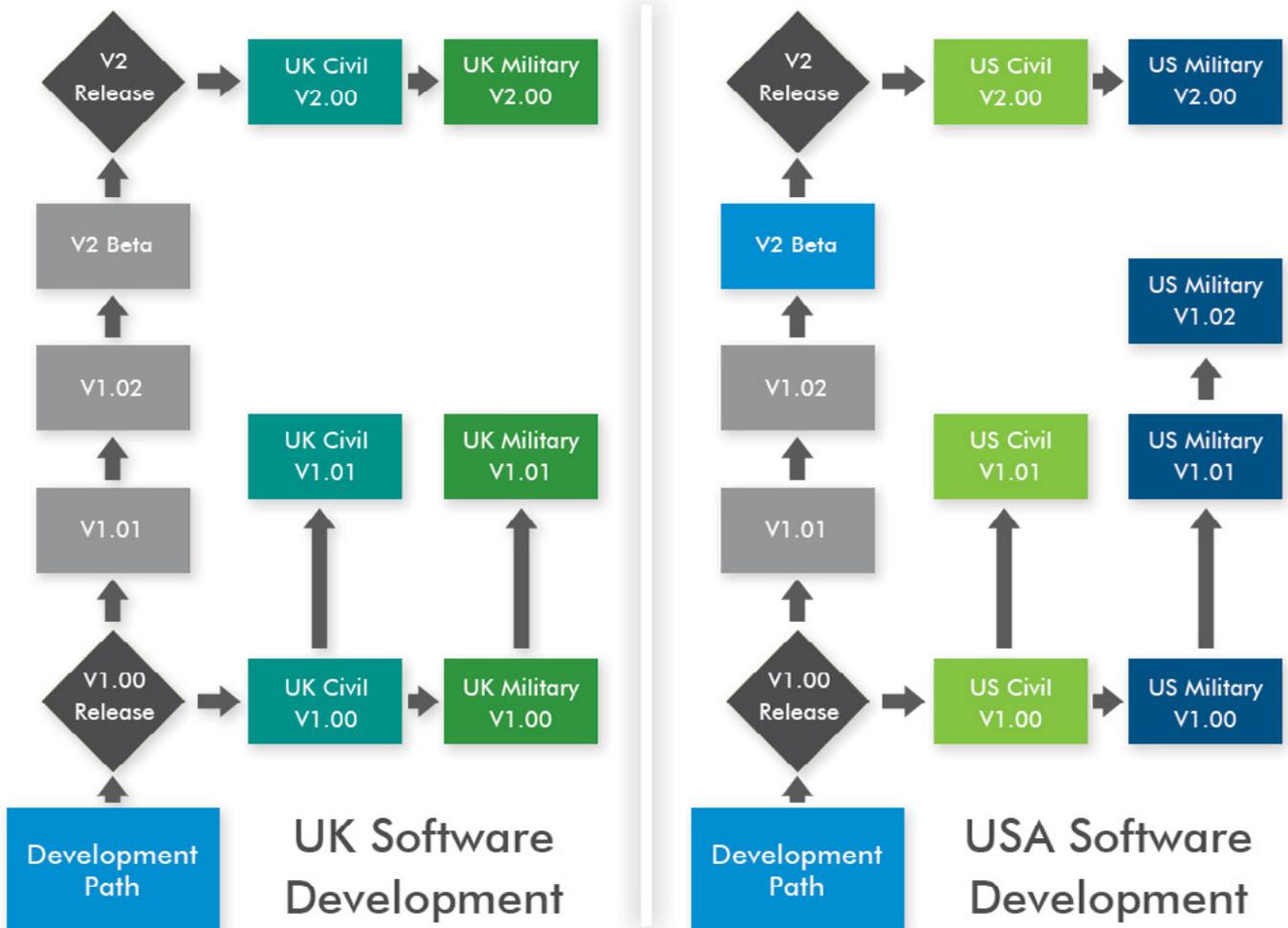
To this end a company will often employ a reseller or distributor in a particular country who is able to supply and provide the necessary support and upgrades for the software.

Larger organisations will often have part of its business based in the destination country, this is fairly common for businesses in the EU to have operations in the USA for example. To ensure maximum compliance these operations are normally fully incorporated businesses.

In Figure A, the company is being ultra cautious, and, essentially, beyond initial requirements gathering are developing their software in isolation. Here they can share advice and expertise, but are avoiding export control in the development

process. In avoiding export control they are having to maintain full development, QA and support capabilities at each site and are duplicating effort.

This kind of model is more common than one may think, to temper the higher cost of this model a company may often produce unique variants of software in each development centre and export the variant of the application to the other.

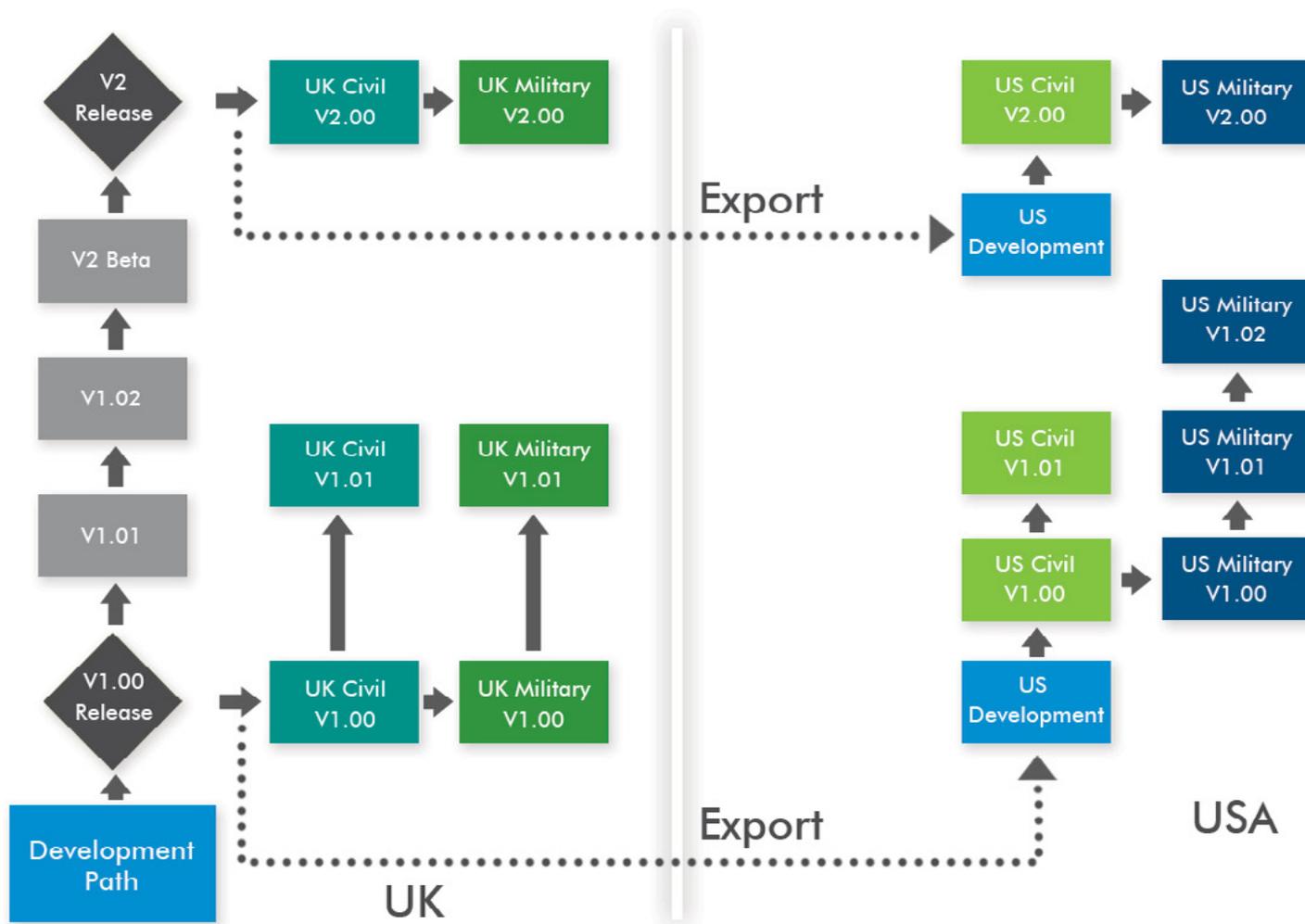


In the example seen in Figure B, a UK based company is developing a software application which is again used in both civil and military applications. The company has a US 'incorporated' operation. The UK exports the V1 application to the 'Inc' in the USA.

The UK continues to develop their next generation software with a team supporting and maintaining the V1 applications currently in use in both Civil and Military guises.

The USA receives the V1 software via export from the UK and carries out further development to make the software suitable for their market and develops a Military variant, provides ongoing support and maintenance for the life of the product.

This is a lower cost model for the company, is robust and is a model which is favoured by many organisations. It falls short of realistically attainable efficiencies because of the burden of export control, there is still a development team, although a lower headcount, in the USA and any innovation created in the USA development path is in isolation.



Supporting Technology

How much more effective would these example scenarios become if export control was no longer applicable? How much more effective would the enterprise be if the teams could work on the projects together? How much would it save the business if they were able to maximise reuse or adopt a product lines method of working?

Export control is not going away, although some reform in the future is expected, but supporting technology is available to enable global development, reuse and software product lines for those who labour under the burden of export control. This kind of technology enables global working without the burden of increased infrastructure, while promoting greater levels of efficiency, improved time to market while maintaining and/or improving quality.

An intelligent application lifecycle management (ALM) solution provides a single point of traceability and auditability for all development artifacts, from initial requirements documents through to test management and release management. It is critical however that the system employed is not an old style 'replication' system which duplicates data across boundaries between development teams. This kind of system compounds export control issues rather than solving them.

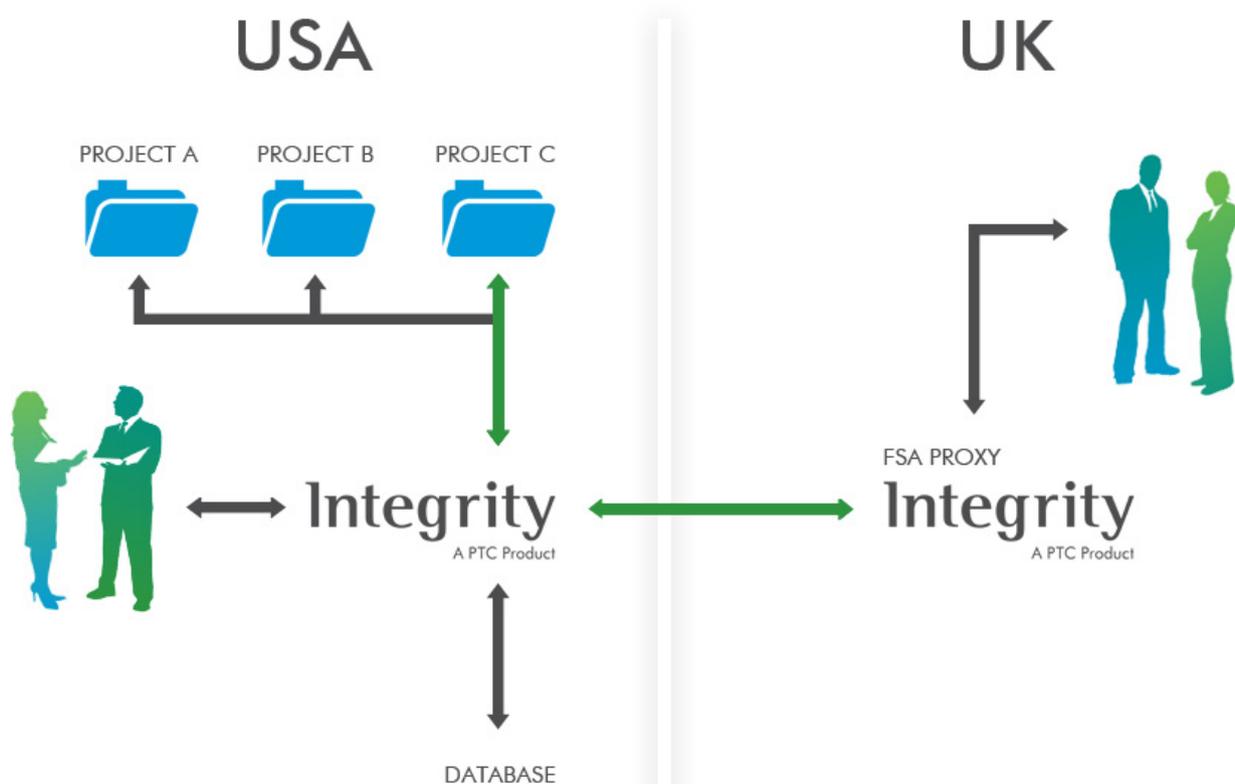
A system is required that allows global working in real time, but that can control permission based access by individual, group, location, by project and critically by project status. It must also be possible to control access permissions for the artifacts from a large to a fine grained level. For instance, common, reusable assets, as exemplified by software product lines (SPL), greatly improve productivity. Fine control of asset permissions maximises cooperative working while securing sensitive assets.

Using the scenario of a team working on a project in three countries, 10 based in Germany, 10 in the UK and 10 in the USA. The application being developed is for a military client in the USA. The team has the task of taking the specification and translating this into a logical set of requirements, developing the software, testing this software against the initial requirements and completing acceptance testing with the client before formal delivery.

At the point where no tangible product exists the team are able to work together up to the point where acceptance testing commences with the client. Any involvement by the German or UK team after this point would normally be regarded as an export. If these teams have been working on the project how can this be avoided?

PTC Integrity applies strict, auditable workflow, and via whatever 'stage' in the workflow a project exists, will determine who has access rights to view, access or modify the assets at each stage. Essentially, when a project is promoted by an authorised person to an 'export control' sensitive state in the project workflow, the team in Germany and the UK simply can no longer see or get any kind of access to the project or any of its component parts, data or information.

Similarly, if a company had PTC Integrity in the USA, the UK and Germany and at each location were working on 3 projects, access to these projects can be controlled easily, local projects (national 'eyes only') can be maintained while allowing selective access to another project.



In the case above, only project C is visible to the remote team in the UK. PTC’s FSA technology allows performant global cooperation while controlling the movement of data to comply with export restrictions.

A third scenario is that a project can be started in one country, and at a point of promotion through its workflow can be transferred to another country ‘eyes only’ state with all visibility removed from the original project team. A further scenario is time limited access. One may have permission to work on assets in the UK for the duration of an export license. It is important to be able to demonstrate that this person has not accessed assets outside of that license. PTC Integrity allows us to model the license in the system so that access to the appropriate artifacts is automatically revoked when the

license expires. This is of course audited by the system too, so the demonstration of compliance is trivial. In addition, since the process is automated there is no chance of accidental breaches of the export control license.

Given that PTC Integrity is a single system that manages requirements, software change and configuration management, test management and release management, there is no break in the chain. Top-down and bottom-up traceability is naturally transparent, and the system by virtue of this keeps users constantly in an ‘audit ready’ position. The system audits all data and system changes allowing demonstration of ‘who’ has accessed ‘what’ and ‘when’. This potential delivers significant value to the business.

Conclusion

Governments worldwide control the export of goods for various reasons depending on the nature and destinations of the proposed export. Export controls exist for a good reason, and are not intended to be a barrier to business or an overbearing compliance burden.

Reform to existing export control regulations is on the horizon, with the USA having recently ordered a full review of the US export control system, one would expect governments to do whatever is possible to bring the regulations up to date. However, this could be a double edged sword, as with the importance of software ever increasing, coupled to consistently improving ability to transfer such at the touch of a button, software could potentially come under even more stringent controls.

If a company is struggling to work effectively due to export control for their software, or fall into one of the traditional examples illustrated in this white paper, then as software continues to increase in complexity and importance going forward, good controls built directly into the organisations development environment will become essential. Manual processes and siloed point solutions will fail at some point.

Export restrictions and local implementations vary greatly so the solution shouldn't assume or impose a set of mechanisms. PTC Integrity has the flexibility to adapt to local requirements but with a robust, enterprise strength security model to control sensitive assets.

The introduction of an intelligent application lifecycle management solution will not only ease the burden of export control compliance, it will help an organisation to bring more products to market faster, with lower development cost while maintaining or improving the quality of the product.

PTC Integrity Business Unit Locations

North America
1 800 613 7535

United Kingdom
+44 (0) 1252 453 400

Germany
+49 (0) 711 3517 75 0

Asia Pacific
+65 6830 8338

Japan
+81 3 5422 9503

integrityinfo@ptc.com

For more information visit: [PTC.com/products/integrity](https://ptc.com/products/integrity)

© 2012, Parametric Technology Corporation (PTC). All rights reserved. Information described herein is furnished for informational use only and is subject to change without notice. The only warranties for PTC products and services are set forth in the express warranty statements accompanying such products and services and nothing herein should be construed as constituting an additional warranty. References to customer successes are based upon a single user experience and such customer's testimonial. Analyst or other forward-looking statements about PTC products and services or the markets in which PTC participates are those of the analysts themselves and PTC makes no representations as to the basis or accuracy thereof. PTC and all PTC product names and logos are trademarks or registered trademarks of PTC and/or its subsidiaries in the United States and in other countries. All other product or company names are property of their respective owners. The timing of any product release, including any features or functionality, is subject to change at PTC's discretion.