Creating Competitive Advantage: The role for ALM in the PLM world

Michael Azoff
Principal Analyst, Ovum
michael.azoff@ovum.com
Version 9 Oct, 2014
**Agenda**

This presentation in one slide:

1. Engineered product complexity is increasing.
2. ALM experience and tools exist.
3. The trend is for ALM and PLM systems to combine.
4. Engineered products with huge software content are shipping now.
5. The safety-critical standards are catching up.
6. Industry is beginning to exploit 2) and 3) and there is a lag between 4) and 5).
7. Internet of Things security issues want to spoil the party.
8. It is time to re-think how we approach the challenges to reap benefits.
Embedded software in engineered products

- Engineers now have choice to design same functionality mechanically, electronically or in software.
- Today software is the value add in engineered products.
Complexity growth of embedded systems

Source: Christof Ebert & Capers Jones, IEEE Computer
Size of codebases are increasing

Source: informationisbeautiful.net
Systems of systems

Source: Inchron
ALM and PLM
Product Lifecycle Management

PLM activities

- Requirements, project management, test management, change management, knowledge sharing
- Bill of materials:
  - As designed, as released to manufacturing, as manufactured, as delivered, as supported, as decommissioned
- 3D design / CAD, modeling:
  - Mechanical, electronic, electro-mechanical
  - Service lifecycle and MRO
- ALM for embedded software

Product lifecycle

Inception → Design-test-develop → Manufacturing → Service in production → Retire
Product change requests across the lifecycle
Embedded software risk

Embedded Software Risk

Dangerous

Reliable

Mature

Ad hoc, unconnected docs and tools

ALM

ALM-PLM integrated

Software development management maturity
ALM maturity in a PLM world

Software development management maturity
Software lifecycle management

- A mature practice in enterprise IT, relatively new concept in PLM world.
Engineered product verification testing

Product

Lifecycle management / QA

Model in the loop
Software in the loop
Hardware in the loop

Tester

Finished product interface testing:
- Is it safe?
- Is it secure?
- Does what it's meant to?

Testing in design development:
- Take testing upstream
- Improve quality
- Improve testing and QA process
Agile testing and QA: automation: continuous testing

1. Commit code changes

2. Triggers continuous integration and testing server

3. Testing feedback report

Source codebase server

Build server

Software engineering team
Business benefits of ALM-PLM integration

- Visibility across all assets:
  - Improve search and locate information.

- Accurately link firmware with hardware:
  - Avoid errors, avoid damage costs, avoid reputation risk.

- Traceability of assets for engineers in all lifecycle phases:
  - Reduce time wasted.
  - Enable effective collaboration across globally distributed units.

- Support maintenance, repair, & operations (MRO):
  - Quickly locate parts and manage defect fixes.
  - Reduce inoperative time of broken products.
Future for ALM and PLM

- ALM name will appear differently across vendor solutions – will add to confusion for users.

- We see ALM as an essential toolset to adopt in increasingly embedded software led PLM world:
  - Industry has no choice! Manage the complexity or be drowned by it.
  - Software development complexity is a new experience for many in engineered product world.

- ALM system adoption is a decision for management.

- PLM vendors are moving towards ALM in different ways, this is one of the most active areas in the PLM solution space right now.

- ALM-PLM integration is necessary – integration standards can reduce costs for end users.
Different stakeholders in ALM adoption

- It matters who has the budget and final say on ALM product choice
Safety, standards, and security
Many standards for safety-critical compliance: Avionics

<table>
<thead>
<tr>
<th>Aircraft certification</th>
<th>Standard</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aircraft Systems</td>
<td>SAE ARP4754A</td>
<td>01 Dec 2010</td>
</tr>
<tr>
<td>Airborne Software</td>
<td>RTCA DO-178C</td>
<td>13 Dec 2011</td>
</tr>
<tr>
<td>Airborne Electronic Hardware</td>
<td>RTCA DO-254</td>
<td>19 Apr 2000</td>
</tr>
<tr>
<td>CNS/ATM Software</td>
<td>RTCA DO-278A</td>
<td>13 Dec 2011</td>
</tr>
<tr>
<td>Software Tool Qualification</td>
<td>RTCA DO-330</td>
<td>13 Dec 2011</td>
</tr>
<tr>
<td>Model-Based Development and Verification Supplement</td>
<td>RTCA DO-331</td>
<td>13 Dec 2011</td>
</tr>
<tr>
<td>Object-Oriented Technology Supplement</td>
<td>RTCA DO-332</td>
<td>13 Dec 2011</td>
</tr>
<tr>
<td>Formal Methods Supplement</td>
<td>RTCA DO-333</td>
<td>13 Dec 2011</td>
</tr>
<tr>
<td>Guidelines for Development of Civil Aircraft and Systems</td>
<td>SAE ARP4754A</td>
<td>21 Dec 2010</td>
</tr>
</tbody>
</table>
## Many standards for safety-critical compliance: medical

<table>
<thead>
<tr>
<th>Medical devices certification</th>
<th>Standard</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDA: Quality system regulation</td>
<td>21CFR 820</td>
<td>1 April 2008</td>
</tr>
<tr>
<td>FDA: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices</td>
<td>337</td>
<td>11 May 2005</td>
</tr>
<tr>
<td>FDA: General Principles of Software Validation, Final Guidance for Industry and FDA Staff</td>
<td></td>
<td>11 Jan 2002</td>
</tr>
<tr>
<td>Quality management systems – Requirements for regulatory purposes</td>
<td>ISO 13485</td>
<td>2003</td>
</tr>
<tr>
<td>Medical device software life cycle processes</td>
<td>EN 62304</td>
<td>2006</td>
</tr>
<tr>
<td>Application of Risk Management to Medical Devices</td>
<td>ISO 14971</td>
<td>2007</td>
</tr>
</tbody>
</table>
Safety-critical standards, continued

- Automotive
  - ISO 26262
  - Motor Industry Software Reliability Association (MISRA)
- Industrial control
  - IEC 61508
- Railways
  - EN 50128
- Nuclear power
  - IEC 60880
ALM plays crucial role to enable traceability

For example, Airborne Software DO-178C on software development traceability:

- Trace Data, showing the bi-directional association between **system requirements allocated to software and high-level requirements** is developed.

- Trace Data, showing the bi-directional association between the **high-level requirements and low-level requirements** is developed.

- Trace Data, showing the bi-directional association between the **low-level requirements and the source code** is developed.
Software in standards

- Each industry is addressing same issues of lifecycle management and governing software quality.

- The relevant standards are distributed across many documents and difficult to get a single view.

- There is a lag between what the standards bodies are issuing and the practice in the field:
  - Compliance standards are not forward looking they are backward looking.
Assessing risks by looking backwards
Cybercriminals Use Text Messages to Empty ATM Cash

By Anthony Cuthbertson
March 25, 2014 10:16 BST

SMS texts are being used by cyber criminals to withdraw cash from ATMs infected with malware. Cybercriminals are able to withdraw cash from ATMs across the world by simply texting an SMS message to a compromised cash machine, according to a new report.
What can be done about software security in products

- Code in machine language.

- Move security into hardware:
  - Move algorithms onto chips.
  - Intel is building hooks at chip level for security purposes (acquired McAfee)

- Create separation layer and one way traffic between safety critical and rest of system, eg infotainment system.

- Security thinking:
  - A lot of knowledge exists but is implemented because of cost.
Software Security Development Lifecycle (SSDL)

Comprehensive security development initiative

- A strategic approach to improve quality and security understanding from the beginning to the end of a project.

- Goal is to keep improving security through applying a security process (not by chance), the SSDL.

- Focus on building-in security functions, as well as security hygiene:
  - Functions: authentication, authorization, encryption, input validation.
  - Hygiene: prevent top 10 OWASP defects.
Secure connected products

- Build software using SSDL.
- Secure by default.
- Input validation.
- Multi-factor authentication.
- Reduced attack surface.
- Prevent known exploits.
Software safety standards

- Creating high quality software is difficult.
- Ensuring safety-critical standards are met will get more and more difficult as codebases keep increasing.

- Internet of Things will create opportunities but also security risks:
  - Connecting products that can cause harm makes malware life threatening.
Industry safety-critical standards are siloed

DO 178C

ISO 26262

IEC 62304

...
But software is software

Propose for industries to adopt joint common software standard and guidelines

DO 178C  ISO 26262  IEC 62304
Benefits of a unified approach to embedded software safety-critical standards

- Tackle the most serious issue:
  - No existing embedded software security standards.
- Shared experiences and rapid distribution of good practices.
- Unified practices can promote better tool support – the ALM vendors will move faster to support the standards.
- Promote software and hardware re-use as standards in ECUs are also promoted.
- Can benefit from software security activity in enterprise IT:
Inhibitors

- Core competencies are commercial confidential.
- Tool vendors give way to open standards slowly.
- Engineering companies are protective of their markets.
Software standards exist that can form a starting point for embedded software

- Aspects of software lifecycle management such as ALM tool traceability are being required for safety-critical certifications.

- There is more that can be adopted, e.g. automation of traceability and visibility across all aspects of development, and across ALM and PLM.

- Ensuring high quality software, guidelines and rules for common software defects exist:
  - Open Web Application Security Project (OWASP) is an online community dedicated to web application security.
  - Object Management Group (OMG) has issued first version of Consortium for IT Software Quality (CISQ) standards: http://it-cisq.org/standards-page/
  - There exists an ISO standard aimed at software industry:
What can we do next

- Industries will gain the benefits of software in engineered products if they co-operate in building safe and secure software.

- Software security is the biggest threat to the software innovation we seek and the Internet of Things we want to build – therefore addressing this issue must be the driver.

- The large engineering companies (from manufacturing to tools vendors) have leadership role opportunities to make a common cause possible.
Thank you

michael.azoff@ovum.com
Disclaimer

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Ovum (an Informa business).

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.