

MCAD Digital Rights Management

Protect Your Critical Design Intellectual Property (IP) Persistently and Dynamically

Contents

Trends in Outsourcing Increase IP Risk	3
Modeling Trends Increase the Need for Persistent File-Level IP Protection	4
Current IP Protection Methods and Requirements for Outsourcing	4
Pro/ENGINEER® Rights Management Extension	6

Trends in Outsourcing Increase IP Risk

Global collaboration has become a necessity for companies. According to AMR, companies that effectively outsource and collaborate globally can grow market share through increased innovation 30-50%, reduce time-to-market by up to 50%, and increase their margins and return on investment by reducing R&D resources by 25%. While these benefits of outsourcing and global collaboration are compelling, there are several challenges when sharing information with external parties including an increased risk of IP loss.

30% of organizations are outsourcing some aspect of their new product development and launch processes, 40% plan to outsource over the next 12-24 months, and another 27% currently have captive development centers in place.

– AMR 2007

The increasing trend in global collaboration is driving the need for more robust protection of intellectual property. Many companies today have security policies and processes implemented in their PLM systems to support global collaboration. However, a PLM system can only protect information while it's inside the system. After spending millions of dollars developing new, innovative products, most companies collaborate on CAD designs with suppliers and partners either by inviting them into their secure PLM collaboration environments, or by providing an unprotected CAD model via email, ftp, physical media, or other non-secure collaboration tools. Once that data is out of the physical protection ring of the IP owner and/or secure PLM system, there is usually nothing to prevent its intended or unintended disclosure to third parties, the press, competitors, black-market manufacturers, and the other non-authorized parties. Such disclosure can result in a significant loss of confidentiality, competitive advantage, time-to-market advantages, and ultimately revenue.

Engineering IP Loss is Costly:

- **“Honda, General Motors Corp. and Toyota Motor Corp. have all sued . . . arguing look-alike designs or logos are costing them business in the world's third-largest auto market”**
- **iRobot sues Robotic FX Inc. for IP stolen by a former employee for a \$280M US government contract**
- **Former DuPont employee steals 22,000 sensitive documents and views more than 16,000 other electronics documents worth \$400M of IP**
- **Well-known semiconductor company lost \$400M in revenues because competitor saw new product specifications in a trade publication before launch**

A successful IP security strategy is composed of many elements, each serving a distinct and important role in IP protection. For example, a server-side PLM deployment should typically provide at least the following security features:

- Both policy- and ad-hoc-based access control that can be role, principal, and context-dependent
- Process-dependent access control to provide elevated access only when required to complete a task
- Security auditing capabilities to permit monitoring of potentially suspicious behavior patterns before they lead to security breaches
- Support for common corporate directory servers to ensure password security policies
- Support of leading web tier infrastructure and support of secure deployment architectures to minimize attack surface area and the potential for security bugs

This whitepaper focuses on a revolutionary form of file level protection for one critical corporate asset, Pro/ENGINEER data. For more information on protecting Pro/ENGINEER data managed in Windchill, PTC's secure, access-controlled, content and process management solutions, please visit www.ptc.com/go/windchill.

*Sources:

<http://www.taipetimes.com/News/biz/archives/2004/12/25/2003216700>

http://www.boston.com/business/globe/articles/2007/11/03/irobot_wins_injunction_against_competitor/

<http://www.informationweek.com/news/showArticle.jhtml?articleID=197006474> Feb 2007

<http://www.adobe.com>

Modeling Trends Increase the Need for Persistent File-Level IP Protection

With the on-going migration from traditional 2D CAD systems to 3D feature-based, parametric modeling systems, an increasing number of companies are adopting a model-based product definition process. The primary objective of a model-based product definition process is to ensure that all pertinent design and manufacturing information is contained in a single product model – the so-called “smart model” concept. Information about the product such as design requirement and constraint specification characteristics, geometric definition, and manufacturing and assembly process characteristics, is captured in the three-dimensional digital product model and related annotations. This information can be easily extracted into engineering deliverables such as inspection information, assembly instructions, and NC tool paths.

Investing in the model by packing it with rich information, results in a whole host of benefits including increased design reuse, shorter product development cycles, and faster time to market. However, as companies incorporate more and more information about the design, behavior and manufacture of their products into the digital model, these CAD files now contain an incredible amount of valuable IP. Furthermore, as the world becomes flatter, as more product development is outsourced and more manufacturing is off-shored, there will be a sharp increase in the likelihood that these files can be misused.

Today, there is typically more security around a \$0.99 iTunes song than the detailed engineering models of a discrete manufacturer’s next generation product when they are outside a secure PLM system! While discrete manufacturers invest a lot of money on physical and internet security (badges, fences, guards, firewalls, passwords, VPNs, etc.), the data that represents the definition and manufacturing processes for their products often remains largely unprotected and thus vulnerable to misuse. In order to reduce the risk and impact of misused IP, especially when outsourcing design and manufacturing, product development companies must improve their current methods of protecting their valuable product development IP. Using digital rights management (DRM) technology to implement persistent and dynamic access policies in product development can help protect valuable IP at the file level and reduce the risk of competitive exposure when IP is distributed outside the safety of a secure PLM environment.

Current IP Protection Methods And Requirements for Outsourcing

Depending on the level of security required, companies use one or more of these common methods to protect their IP:

- Secure data transmission using
 - Encrypted data
 - Protected, private networks
- Individual or role-based access control to a data repository
- File-level access control via password protection
- Selective concealment of design data

Protecting data and managing IP outside a secure, managed, access-based solution such as Windchill is typically a manual process that can be cumbersome or difficult to adopt and enforce without the right processes and infrastructure. Often times, collaboration with external parties becomes informal and extends outside the managed environment, which further increases the risk of IP loss.

Collaboration outside the managed environment is risky today: almost 50% of all information sharing/collaboration is informal and over 60% of today’s process flow and security activities are managed manually.

– AMR Jan 2006

While the current methods of protecting IP provide robust security when the data resides in the managed environment, they often lack key capabilities needed to support an increasingly outsourced product development process:

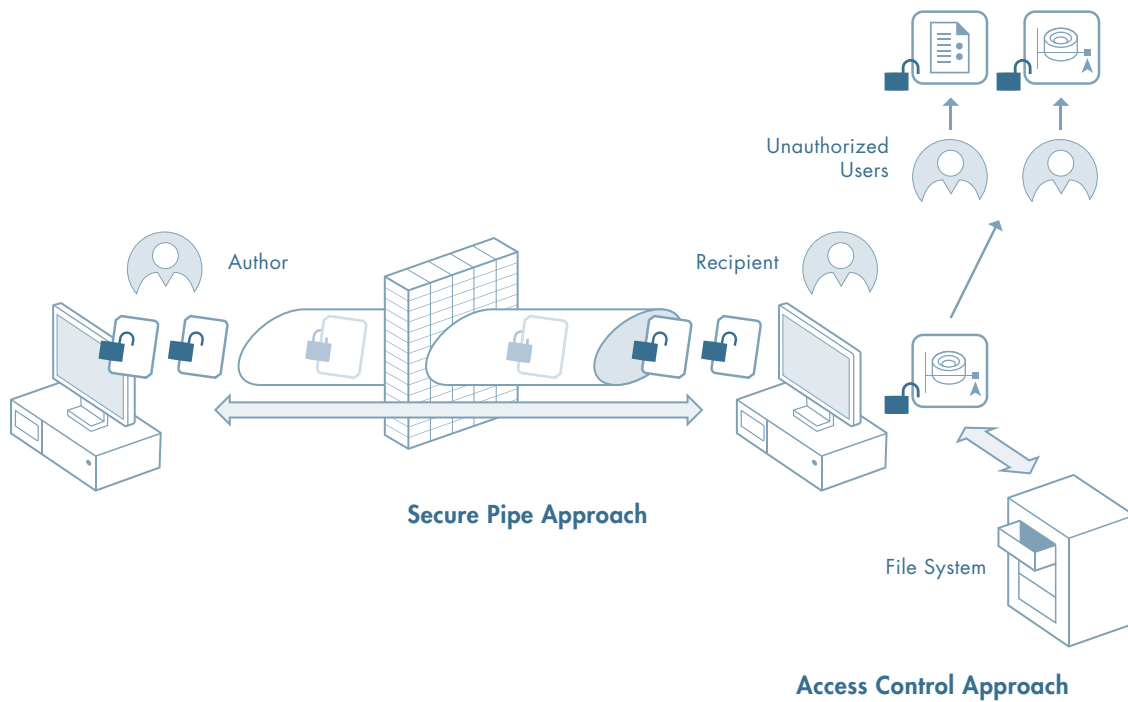
- Persistent protection of data
- Dynamic updates to support changes in the access requirements

Companies need the ability to control and manage IP at all times. If a confidential file is forwarded to other parties beyond the intended viewer, the owner of the content should be able to prevent unauthorized parties from opening or using the data.

Controlling, managing and monitoring MCAD IP at the file level once it leaves a secure PLM environment will become a necessity as outsourcing increases.

– IDC 2007

Current approaches which leverage secure IT infrastructure and access control to a data management system do not prevent unauthorized users from viewing content once it is outside the physical protection ring.



In today's dynamic, competitive environment, original equipment manufacturers (OEMs) and suppliers need to be able to revoke access to data, even to those that previously had access rights. Simple password protected files and data management systems do not protect data if the OEM or supplier changes its mind about access to data that has been distributed outside a protected, managed environment. Once the data is removed from the secure repository and access passwords are in the users' hands, the OEM or supplier cannot rescind access rights. This capability is critical to support the real-world dynamics of contract designers and supply chains where partners are added, modified, and removed on a frequent basis. If a prospective design partner or supplier returns an unreasonable quote or if an existing relationship is terminated, the OEM or supplier needs to be able to change the permissions associated with the policy that has been applied to a part or assembly and revoke rights to even access the file. Once access rights have been removed, the ability to open the file should be prevented even though the external party may still possess the file.

Conversely, we can imagine that the design partner or supplier has provided a very competitive quote, based on their review of the product, and the OEM engages them in a contract. As part of this process, the OEM may extend further rights to the partner, allowing them to not only open the models, but possibly print them and even generate downstream deliverables such as a mold core/ cavity/ mold base and NC tool-paths to machine those deliverables. While those deliverables may physically reside at the partner's site, the OEM needs to retain control over the rights to those deliverables, ensuring that they can only be accessed and used by the vendor himself. The vendor's rights to the mold base, for example, should be managed along with the rights to the design itself by the rightful owner – the OEM.

Version control and change management are also common challenges when outsourcing design and manufacturing projects. OEMs and suppliers need to ensure that their partners are using only the most up-to-date product information. By enabling access to only the correct version of files and disabling access to all other versions that may be in use outside the managed environment, all out-of-date files can effectively be "shredded," no matter where they are on the planet.

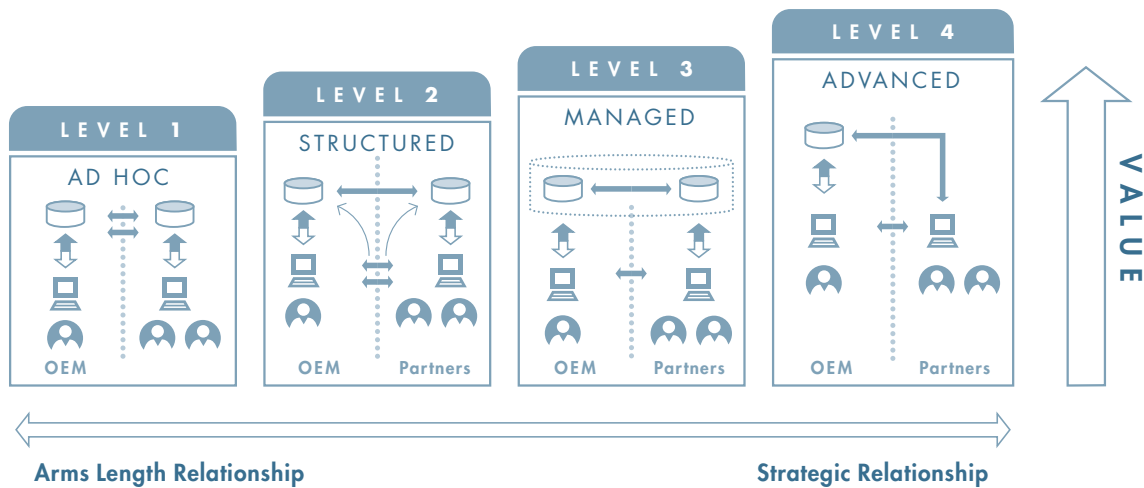
Pro/ENGINEER Rights Management Extension

With Pro/ENGINEER Wildfire 4.0, PTC customers can now protect their Pro/ENGINEER models and drawings with strong encryption and a variable set of "rights" for specific users to access the files. These rights correspond to varying levels of trust between the two parties and have been defined to support typical product development processes encountered in today's environment of global product development.

Pro/ENGINEER provides industry leading MCAD DRM capabilities



The graphic below illustrates the spectrum of process maturity levels and resulting OEM-partner relationships for design and manufacturing outsourcing processes. Persistent file – level DRM capabilities are necessary for all design and manufacturing outsourcing process maturity levels.

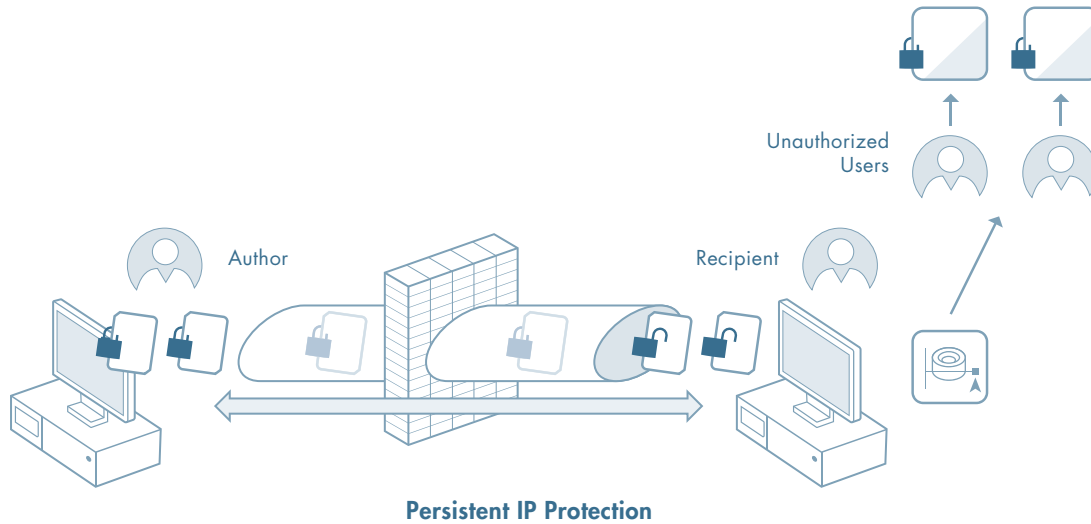


For example, an OEM may need to provide data to a supplier to request a quote to supply a part. However, the OEM wants to prevent inadvertent disclosure of IP by the supplier to others (e.g. via email to an unintended recipient, virus, leak through unsecured supplier IT infrastructure) as well as prevent malicious theft of core IP by the supplier or potential suppliers who are not yet trusted partners.

Using the new Pro/ENGINEER Rights Management Extension (RMX) and Adobe® LiveCycle® Rights Management ES, the OEM is able to assign a specific DRM policy from a policy sever, which would allow that supplier's named users to perform specific actions on that file -for example, only open it- for a specified period of time. This policy will allow for the part or assembly file to be opened, and interrogated (measured, cross sections viewed, etc.), but will prevent all actions that could persist or replicate the data such as Save, Export, Copy Geometry, Shrinkwrap, generate manufacturing deliverables, etc.

Also, unlike simple password protected files, protected Pro/ENGINEER files have persistent and dynamic protection. The OEM can grant more rights or have their access disabled quickly and easily from the policy server. The OEM can change the permissions associated with the policy that has been applied to that part or assembly, and even revoke the vendor's right to access the file at any time. Once the access rights have been changed by the OEM, even though the vendor may still possess the file, when they are subsequently retrieved by Pro/ENGINEER, the policy server will be queried, and the right to open the file will be verified and granted or denied based on the updated policy. Pro/ENGINEER also has capabilities that will allow the OEM to retain control over the rights to downstream deliverables, ensuring that they can only be accessed and used by the authorized vendor.

Persistent IP protection provided by the Pro/ENGINEER and Adobe solution prevents unauthorized users from accessing confidential data when the file is outside a secure content and process management system.



In addition to assigning policies and enforcing permissions, the policy server delivers comprehensive auditing capabilities, which report both successful and unsuccessful attempts to open protected content. This provides the IP owner with insight into how and when a model is accessed and provides accountability through the tracking of each partner's use of a model.

The DRM capabilities in Pro/ENGINEER also improve version control and change management processes, especially when outsourcing design and manufacturing projects. The OEM in the previous example can easily change access to protected files outside the firewall or protected data repositories. By enabling access to only the correct version of files and disabling access to all other versions, the OEM can ensure that their partners are using the right information.

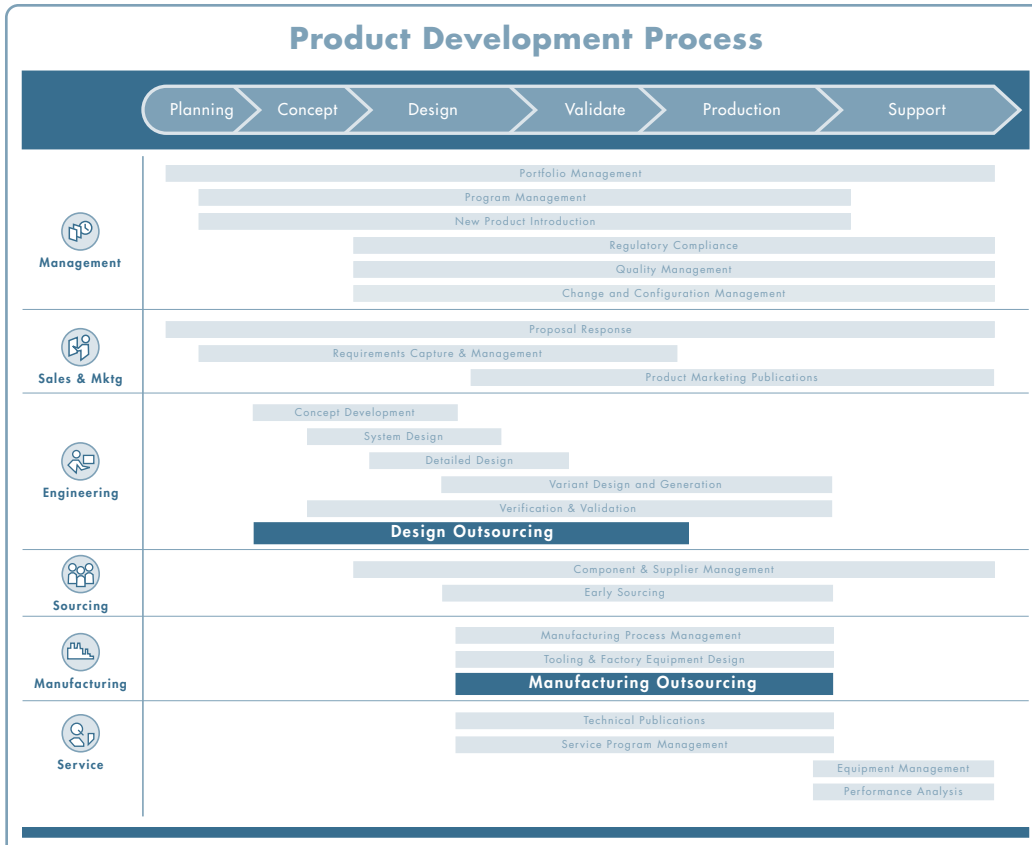
Implementing DRM technologies to protect your valuable design IP at the file level when the data is beyond the protection of a secure, content and process management environment, can help you improve your design and manufacturing outsourcing processes. For optimal results, companies should

- Assess design IP risk throughout their product development processes
- Establish appropriate design data access policies and processes for both internal and external parties
- Implement a system that provides comprehensive IP security, including dynamic and persistent protection of CAD data at the file level
- Automate the process of applying, managing and monitoring file level IP and access policies

A complete design IP protection system- processes and technology- facilitates secure collaboration, reduces the risk of losing IP, improves version control, and fortifies change management processes. Pro/ENGINEER RMX and Adobe LiveCycle Rights Management ES provide the most advanced technology for protecting design IP contained in Pro/ENGINEER files, PDF, Microsoft Word and Excel documents.

PTC Global Services provides customers with a blend of process consulting, system implementation services, innovative education solutions, and value management that ensures customers have the right processes in place to fully leverage and protect their valuable Pro/ENGINEER data. PTC also provides customers with the right education programs to drive adoption.

Pro/ENGINEER Rights Management Extension improves design and manufacturing outsourcing processes.



PTC is the only software vendor that has taken a proactive, integrated approach to including DRM in its primary CAD product. Other CAD/PLM vendors are taking a hands-off approach, leaving this integration work to partners. The result is a solution that either provides inadequate IP protection due to many paths of IP leakage or is so cumbersome that productive work within the CAD system is not possible. Because the security and protection of our customers' valuable engineering IP is too critical to leave to a sub-optimal integration, PTC has chosen a direct approach to deliver an optimized integration of DRM within Pro/ENGINEER. The result is a balanced environment that provides the productivity and security that product development organizations need.

PTC is leading the way on the protection of engineering intellectual property through our strategic relationship with Adobe and our integration of Pro/ENGINEER with Adobe LiveCycle Rights Management ES.

For more information, please visit www.ptc.com/go/proengineer/drm

© 2008, Parametric Technology Corporation (PTC)—All rights reserved under copyright laws of the United States and other countries. PTC, the PTC Logo, Pro/ENGINEER, Wildfire, Windchill, Windchill PDMLink, Pro/INTRALINK, 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. Windows is a registered trademark of Microsoft Corporation. Adobe and LiveCycle are registered trademarks of Adobe Systems Incorporated.