

MCAD 数字权限管理

持久和动态地保护重要的设计知识资产 (IP)



目录

外包趋势增加了 IP 风险 3

建模趋势增加了对文件级别 IP 保护的需求 5

当前的 IP 保护方法和外包的要求 5

Pro/ENGINEER 权限管理扩展 7

外包趋势增加了 IP 风险

全球协作对于公司已变得必不可少。AMR 称，如果公司有效地在全球范围内外包业务和开展协作，则可以通过增强创新水平将市场份额提高 30-50%、将产品上市时间缩短 50% 之多，并可以通过减少投入的研发资源将利润和投资回报增加 25%。虽然外包和全球协作带来的这些好处很吸引人，但是，在与外界共享信息时要面对多项挑战，其中包括丢失 IP 的风险有所增加。

有 30% 的组织正将其新产品开发和上市过程的一些环节外包出去，有 40% 的组织计划在未来 12-24 个月内外包业务，另外还有 27% 的组织目前已设立了附属开发中心。

— AMR 2007

全球协作愈演愈烈，从而推动了对更可靠地保护知识产权的需求。许多公司如今都建立了在其 PLM 系统中实施的安全策略和安全流程，以支持全球协作。但是，PLM 系统只能保护处于系统内的信息。在花费了几百万元开发创新的产品之后，大多数公司会与供应商和合作伙伴就 CAD 设计开展协作，具体做法是：邀请他们进入公司的安全 PLM 协作环境，或者通过电子邮件、ftp、实物介质或其他不安全的协作工具向他们提供未经保护的 CAD 模型。一旦数据脱离了 IP 所有者的物理保护圈和/或安全的 PLM 系统，通常就无法阻止数据被有意或无意泄露给第三方、新闻界、竞争对手、黑市制造商和未经授权的其他方。此类泄露可能导致机密性、竞争优势、产品上市时间优势严重受损，最终导致收入大幅下挫。

成功的 IP 安全战略包含许多要素，每个要素在 IP 保护中都扮演着独特和重要的角色。例如，服务器端的 PLM 部署通常应至少提供以下安全功能：

- 基于策略的访问控制和即席访问控制，可以依赖于角色、主体和上下文
- 依赖于过程的访问控制，以仅在完成任务需要用到时才提供提升的访问权
- 安全审核功能，能在可疑的行为模式导致安全性被破坏之前对它们进行监视
- 对常用的企业目录服务器的支持，以确保实施密码安全策略
- 对主要 Web 层基础结构和安全部署体系结构的支持，以最大程度减小受攻击面和出现安全缺陷的可能性

本白皮书着重说明一种创新的文件级别保护方式，以保护一项重要的企业资产——Pro/ENGINEER 数据。有关保护在 Windchill（它是 PTC 的安全、访问受控的内容和过程管理解决方案）中管理的 Pro/ENGINEER 数据的更多信息，请访问 www.ptc.com/go/windchill。

丢失工程 IP 的代价非常沉重

- 通用汽车控告中国的奇瑞汽车公司涉嫌剽窃小型车 Chevy Spark 的设计
- 本田汽车公司赢得有关 Hongda 摩托车的诉讼，并控告双环来宝 S-RV 抄袭它的 CR-V 越野车
- iRobot 控告 Robotic FX Inc.，原因是它的一名前雇员盗取了金额为 2.8 亿美元的美国政府合同的 IP
- 前杜邦雇员盗取 22,000 份机密文档，并偷看了另外 16,000 多份电子文档（IP 价值达到 4 亿美元）
- 著名的半导体公司损失 4 亿美元的收入，原因是，在该公司的新产品上市之前，竞争对手就通过商业出版物获得了新产品的规格

随着外包日益增多，在 MCAD IP 离开安全的 PLM 环境时在文件级别控制、管理和监视这些资产将变得必不可少。

– IDC 2007

来源：

GM—奇瑞，中国日报GongZhengzheng

http://www.chinadaily.com.cn/english/doc/2004-12/18/content_401235.htm

本田汽车公司 台北时报和中国日报

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

http://www.chinadaily.com.cn/english/doc/2004-04/13/content_322850.htm

iRobot Boston Globe 2007

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

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

半导体公司 Adobe 2007

建模趋势增加了对文件级别 IP 保护的需求

从传统的 2D CAD 系统迁移到基于 3D 特征的参数化建模系统的势头方兴未艾，这使得越来越多的公司采用基于模型的产品定义过程。基于模型的产品定义过程的主要目标是，确保单个产品模型中包含了所有相关的设计和制造信息——所谓的“智能模型”概念。三维的数字化产品模型和相关的注释中记录了产品的相关信息，例如设计要求和约束、规格特征、几何定义以及制造和装配过程特征。可以轻松地从此信息抽取到工程交付件中，如检查信息、装配指令和 NC 刀具路径。

通过在模型中填入丰富的信息来“投资于”模型的做法带来了许多好处，包括提高了设计重用率、缩短了产品开发周期，以及加快了产品上市时间。但是，随着公司将越来越多的产品相关信息（设计、行为和制造）加入到数字化模型中，这些 CAD 文件现在包含了数量惊人的重要 IP。此外，随着世界变得更扁平，以及随着产品开发业务越来越多地外包、产品制造越来越多地在海外进行，滥用这些文件的可能性将会急剧提高。

如今，如果某离散型制造商的下一代产品的详细工程模型离开了安全的 PLM 系统，那么，它的安全性通常还比不上价格为 0.99 美元的一首 iTunes 歌曲！虽然离散型制造商在物理安全和 Internet 安全方面投入了大量资金（标记卡、围墙、看守、防火墙、密码、VPN 等），但是，描述其产品的定义和制造过程的数据通常在很大程度上未经保护，因而易被滥用。为了减少被滥用的 IP 的风险和影响（特别是在外包设计和制造业务时），产品开发公司必须改善当前的重要产品开发 IP 保护方法。通过使用数字权限管理 (DRM) 技术在产品开发中实施持久和动态的访问策略，可帮助在文件级别保护重要的 IP，并减少在脱离安全的 PLM 环境散布 IP 时向竞争对手泄密的风险。

当前的 IP 保护方法和外包的要求

取决于所需的安全级别，公司使用以下一种或多种常见方法来保护其 IP：

- 安全的数据传输，使用
 - 加密的数据
 - 受保护的专用网络
- 基于个体或角色的数据存储库访问控制
- 通过密码保护实现的文件级别访问控制
- 有选择地隐藏设计数据

在安全、托管、基于访问的解决方案（如 Windchill）之外保护数据和管理 IP 通常是一个手工过程，而如果未建立正确的流程和基础结构，此过程可能很棘手或难以采用和实施。与外界的协作经常会变得不正规，并延伸到托管的环境之外，这进一步增加了丢失 IP 的风险。

如今，在托管的环境外开展的协作充满风险：在所有信息共享/协作活动中，将近 50% 不正规，而且当今的过程流和安全活动有超过 60% 是手工管理的。

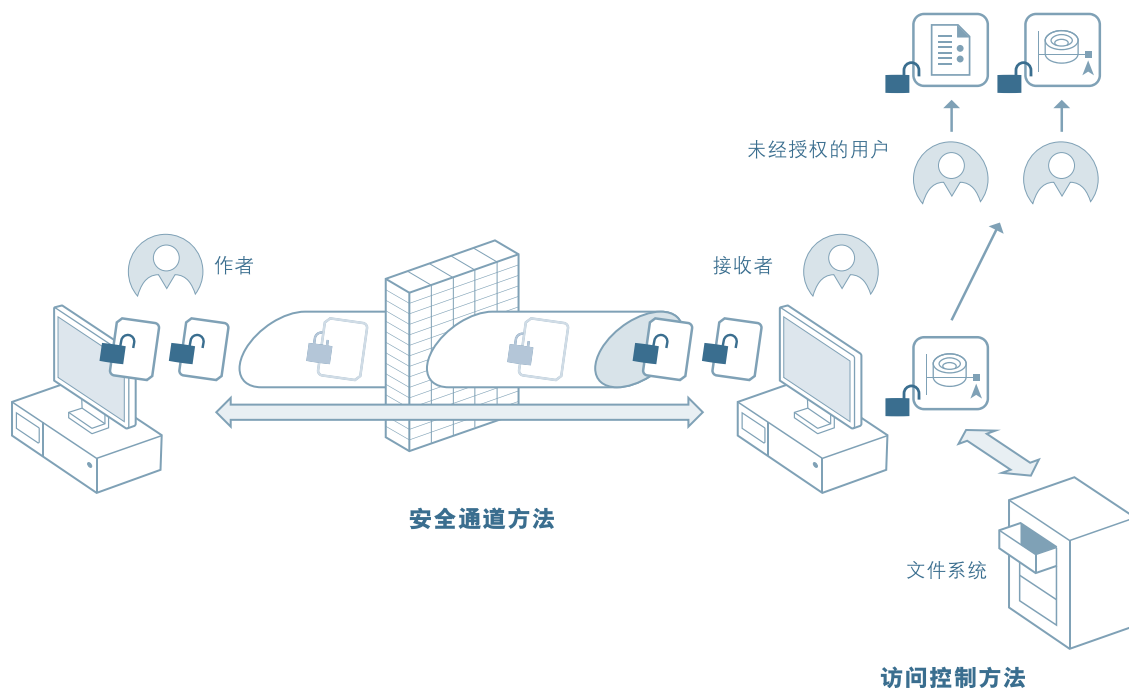
– AMR 2006 年 1 月

虽然当前的 IP 保护方法在数据位于托管的环境中时提供了可靠的保护，但是，它们通常缺少支持越来越多地外包的产品开发过程所需的关键功能：

- 数据的持久保护
- 支持访问需求变化的动态更新

公司需要在任何时候都能控制和管理 IP。如果机密文件被转交给原定查看者以外的其他方，则内容的所有者应能够阻止未经授权的其他方打开或使用数据。

当前的方法利用安全的 IT 基础结构，并控制对数据管理系统的访问，而一旦内容离开物理保护圈，这些方法便无法阻止未经授权的用户查看内容。



在当今不断变化、竞争激烈的环境中，原始设备制造商 (OEM) 和供应商需要能够取消对数据的访问，即使涉及的是那些以前有访问权的人员。如果 OEM 或供应商已经在受保护和托管的环境外分发的数据的访问权，那么，用简单的密码保护的文件和数据管理系统便无法保护数据。一旦从安全的存储库中取出数据，并且访问密码落入用户手中，那么 OEM 或供应商便无法取消访问权。此功能对于支持合约设计者和供应链在现实世界中会发生变化（时常会增加、改变和剔除合作伙伴）的状况至关重要。如果潜在的设计合作伙伴或供应商返回了不合理的报价，或如果现有的关系被终止，那么 OEM 或供应商需要能够更改与已应用于零件或组件的策略相关的权限，以及取消包括访问文件在内的权限。一旦删除了访问权，就应阻止打开文件的能力，即使外界仍可能拥有文件。

相反地，我们可以想像一下，设计合作伙伴或供应商基于对产品的评审提供了一个非常有竞争力的报价，而且 OEM 与它们签订了合约。作为此过程的一部分，OEM 可以将更多的权限延伸到合作伙伴，使它们不仅能够打开模型，还能够打印模型甚至生成下游交付件，例如模具型芯/型腔/模架和 NC 刀具路径，以加工这些交付件。虽然这些交付件在物理上可以位于合作伙伴的地点，但 OEM 需要保留对这些交付件相关权限的控制，以确保它们只能由供应商自身访问和使用。例如，正确的所有者 (OEM) 应将供应商对模架具有的权限与对设计本身具有的权限一起管理。

在外包设计和制造项目时，版本控制和变更管理也是常见的挑战。OEM 和供应商需要确保其合作伙伴仅使用最新的产品信息。通过仅允许访问正确的文件版本，以及不允许访问可能在托管的环境外使用的所有其他版本，可以有效地销毁所有过期的文件，而不管它们散落在地球上的哪个地方。

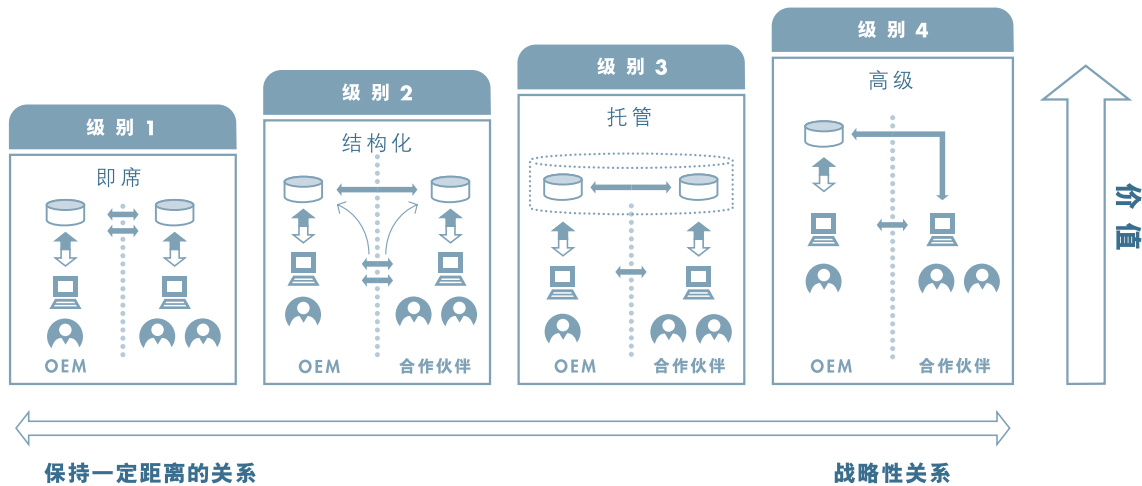
Pro/ENGINEER 权限管理扩展

Pro/ENGINEER 提供业界领先的 MCAD DRM 功能



有了 Pro/ENGINEER Wildfire 野火版 4.0，PTC 客户现在可以利用强有力的加密和一组可变的权限（供特定的用户访问文件）保护其 Pro/ENGINEER 模型和绘图。这些权限对应于双方之间变化的信任等级，而且已被定义为支持在当今的全球产品开发环境中遇到的典型产品开发过程。

在设计和制造外包关系的整个领域中都需要文件级别的 DRM 功能

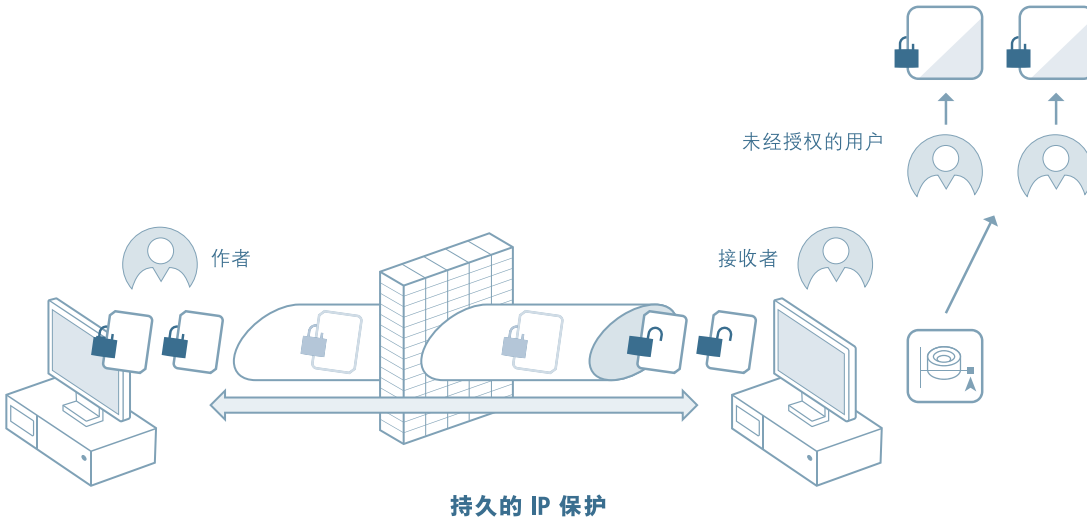


例如，某 OEM 可能需要向某供应商提供数据，以要求其提供供应某零件的报价。但是，该 OEM 希望阻止此供应商无意中将 IP 泄露给其他方（例如，通过发给计划外接收者的电子邮件、病毒或通过不安全的供应商 IT 基础结构），以及阻止此供应商或尚未成为值得信任的合作伙伴的潜在供应商恶意盗取核心 IP。

通过使用新的 Pro/ENGINEER 权限管理扩展 (RMX) 和 Adobe® LiveCycle® Rights Management ES，该 OEM 能够通过策略服务器指定特定的 DRM 策略，以允许该供应商的指定用户在指定的一段时间内对该文件执行特定的操作（例如，只是打开它）。此策略将允许打开和查询（测量、查看剖面等）零件或组件文件，但将阻止所有可能持续或复制数据的操作，例如保存、导出、复制几何、收缩包络、生成制造交付件等。

而且，与使用简单的密码保护的文件不同，受保护的 Pro/ENGINEER 文件受到持久和动态的保护。OEM 可以通过策略服务器快速轻松地授予更多的权限，或禁止这些访问权。OEM 能够随时更改与已应用于该零件或组件的策略相关的权限，甚至能够取消供应商访问文件的权限。一旦 OEM 更改了访问权（即使供应商仍可能拥有文件），在 Pro/ENGINEER 以后检索这些文件时，将会查询策略服务器，验证打开文件的权限，并根据更新的策略来授予或拒绝此权限。Pro/ENGINEER 的功能还包括允许 OEM 保持对下游交付件相关权限的控制，从而确保只能由经授权的供应商访问和使用这些交付件。

Pro/ENGINEER 和 Adobe 解决方案提供的持久 IP 保护能在文件离开安全的内容和过程管理系统后，阻止未经授权的用户访问机密数据。



除了指定策略和实施权限外，Pro/ENGINEER 还提供全面的审核功能，这些功能将报告成功和不成功的打开受保护内容的尝试。这使 IP 所有者能够深入了解模型如何和何时被访问，并通过跟踪每个合作伙伴使用模型的情况明确责任关系。

Pro/ENGINEER 中的 DRM 功能还改善了版本控制和变更管理过程，特别是在外包设计和制造项目时。前一个示例中的 OEM 可以轻松更改对离开防火墙或受保护数据存储库的受保护文件的访问权。通过仅允许访问正确的文件版本和不允许访问所有其他版本，OEM 可以确保其合作伙伴使用正确的信息。

通过实施 DRM 技术以便在数据脱离安全的内容和过程管理环境的保护后在文件级别保护重要的设计 IP，可以帮助您改善设计和制造的外包过程。为了达到最佳效果，公司应

- 评估其整个产品开发过程中的设计 IP 风险
- 为内外各方建立适当的设计数据访问策略和过程
- 实施一个提供全面 IP 安全性的系统，包括在文件级别动态和持久保护 CAD 数据的安全性
- 自动执行应用、管理和监视文件级别 IP 及访问策略的过程

完整的设计 IP 保护系统（过程和技术）可促成安全的协作、减少丢失 IP 的风险、改善版本控制，以及加强变更管理过程。Pro/ENGINEER RMX 和 Adobe Live Cycle Rights Management ES 提供了最先进的技术，可用于保护 Pro/ENGINEER 文件、PDF、Microsoft Word 和 Excel 文档中包含的设计 IP。PTC 全球服务为客户提供融为一体的过程咨询、系统实施服务、创新的培训解决方案以及价值管理，确保客户建立起正确的过程以全面利用和保护他们的重要 Pro/ENGINEER 数据。PTC 还为客户提供适当的培训计划以提高采用率。

Pro/ENGINEER 权限管理扩展改善了设计和制造的外包过程。



PTC 是唯一一家采取了主动、综合的方法在其主要的 CAD 产品中
加入 DRM 功能的软件供应商。其他 CAD/PLM 供应商抱着置身事
外的态度，将此集成工作留给合作伙伴来完成。这样做所产生的
解决方案要么由于泄露 IP 的途径有许多而导致 IP 保护不够充分，
要么由于太过棘手而导致无法在 CAD 系统中富有成效地工作。
我们客户的重要工程 IP 的安全性和保护极为重要，未达到最佳
效果的集成对此无能为力，因此，PTC 选择了直接的方法来提供
DRM 在 Pro/ENGINEER 中的最佳集成。结果，产生了一个平衡的
环境，能同时提供产品开发组织所需的生产效率和安全性。

PTC 通过我们与 Adobe 建立的战略性关系，以及我们对
Pro/ENGINEER 与 Adobe LiveCycle Rights Management ES 所做的集
成，成为保护工程知识产权的开路先锋。

有关更多信息，请访问 www.ptc.com/go/proengineer/drm

版权所有 © 2007，Parametric Technology Corporation (PTC) — 保留美国和其他国家/地区的版权法所赋
予的所有权利。本文所述信息基于一个用户的经验。本文所述信息仅供参考，如有更改，恕不另行通知，
这些信息不应视作 PTC 提供的担保或承诺。