

# Gestion des droits numériques pour la CFAO

**Pour une protection durable et dynamique de votre propriété intellectuelle**

## Table des matières

Risque accru pour la propriété intellectuelle . . . . .	3
dû à la tendance à l'externalisation	
Nécessité d'une protection de la propriété . . . . .	5
intellectuelle au niveau du fichier due à la	
tendance à la modélisation	
Méthodes actuelles de protection de la propriété . . . . .	5
intellectuelle et spécifications pour l'externalisation	
Pro/ENGINEER Rights Management Extension . . . . .	7

## Risque accru pour la propriété intellectuelle dû à la tendance à l'externalisation

Collaborer au niveau mondial est devenu une nécessité. Selon AMR, les sociétés qui externalisent et collaborent à l'échelle mondiale peuvent voir leur part de marché augmenter de 30 à 50 % grâce à l'innovation, réduire leur délai de commercialisation jusqu'à 50 % et améliorer leur marge bénéficiaire et le retour sur investissement en diminuant de 25 % les ressources de R&D. Malgré l'attrait de ces avantages, l'externalisation et la collaboration posent des problèmes car le partage des informations avec les intervenants externes peut augmenter le risque de perte de propriété intellectuelle.

**30 % des entreprises externalisent une partie des processus de développement et de lancement de produits, 40 % prévoient de recourir à la délocalisation dans les 12 à 24 mois à venir, et 27 % disposent déjà de centres de développement à l'étranger.**

– AMR 2007

La collaboration mondiale est une tendance qui se renforce et oblige à mieux protéger la propriété intellectuelle. Aujourd'hui, de nombreuses sociétés mettent en œuvre des politiques et des procédures de sécurité dans leurs systèmes PLM afin de prendre en charge la collaboration à l'échelle mondiale. Or un système PLM ne peut protéger les informations que si elles restent à l'intérieur de ce système. Après avoir dépensé des millions de dollars dans le développement de produits innovants, la plupart des sociétés collaborent sur les conceptions de CAO avec des fournisseurs et des partenaires soit en les invitant dans leur environnement collaboratif PLM sécurisé, soit en leur transmettant un modèle CAO non protégé par e-mail, via ftp, sur un support physique ou à l'aide d'autres outils collaboratifs non sécurisés. Dès que les données quittent la zone de protection physique du propriétaire et/ou du système PLM sécurisé, rien n'empêche leur communication, intentionnelle ou non, aux tiers : les médias, les concurrents, les contrefacteurs et autres parties non autorisées. Cette divulgation peut constituer une grave menace à plusieurs niveaux : la confidentialité, l'avantage concurrentiel, le délai de mise sur le marché et le chiffre d'affaires.

Une stratégie réussie de protection de la propriété intellectuelle se compose de plusieurs éléments qui jouent chacun un rôle distinct et important. Par exemple, un déploiement PLM côté serveur doit au minimum présenter les caractéristiques suivantes :

- Contrôle d'accès à la fois général et particulier, en fonction du rôle, du contexte ou du principe
- Contrôle d'accès dépendant du processus de manière à n'autoriser un accès étendu que pour effectuer une tâche particulière
- Fonctions de contrôle de sécurité pour surveiller les modes de comportement douteux qui peuvent générer des failles dans la sécurité
- Prise en charge de serveurs d'annuaires d'entreprise communs pour appliquer les règles de sécurité relatives aux mots de passe
- Prise en charge d'une infrastructure Web multiniveau et d'architectures de déploiement sécurisées afin de minimiser les vulnérabilités et les failles de sécurité

Ce livre blanc présente une forme révolutionnaire de protection au niveau du fichier pour des données d'entreprise particulièrement importantes : les données Pro/ENGINEER. Pour plus d'informations sur la protection des données Pro/ENGINEER gérées avec Windchill, la solution PTC de gestion des processus et contenus sécurisée par contrôle d'accès, visitez notre site Web à la page [www.ptc.com/go/windchill](http://www.ptc.com/go/windchill).

### En ingénierie, la perte de propriété intellectuelle a un coût.

- General Motors intente un procès à la société chinoise Chery Automobile Co. pour contrefaçon de la petite citadine Chevy Spark.
- Honda Motor Company gagne son procès contre les motos Hongda et accuse le constructeur Shuanghuan Motors de plagier son CR-V avec le Laibao S-RV.
- iRobot intente un procès contre Robotic FX Inc. pour vol de propriété intellectuelle par un ancien employé pour un contrat d'une valeur de 280 millions de dollars avec le gouvernement américain.
- Un ancien employé de DuPont a volé 22 000 documents sensibles et consulté plus de 16 000 documents électroniques d'une valeur de 400 millions de dollars en termes de propriété intellectuelle.
- Une société réputée dans le secteur des semi-conducteurs a enregistré une perte de 400 millions de dollars de son chiffre d'affaires parce qu'un concurrent a trouvé les spécifications du nouveau produit dans une publicité parue avant la commercialisation du produit.

L'intensification de l'externalisation oblige à contrôler, gérer et surveiller la propriété intellectuelle de CFAO au niveau du fichier.

– IDC 2007

#### Sources :

##### GM-Chery, China Daily, Gong Zhengzheng

[http://www.chinadaily.com.cn/english/doc/2004-12/18/content\\_401235.htm](http://www.chinadaily.com.cn/english/doc/2004-12/18/content_401235.htm)

##### Honda Motor Company, Taipei Times et China Daily

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

[http://www.chinadaily.com.cn/english/doc/2004-04/13/content\\_322850.htm](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/](http://www.boston.com/business/globe/articles/2007/11/03/irobot_wins_injunction_against_competitor/)

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

**Fabricant de semi-conducteurs** Adobe 2007

## Nécessité d'une protection de la propriété intellectuelle au niveau du fichier due à la tendance à la modélisation

Avec la migration continue des systèmes classiques de CAO 2D vers les systèmes paramétriques de modélisation 3D, un nombre croissant de sociétés adoptent un processus de définition de produit basé sur le modèle. L'objectif principal de ce type de processus est d'inclure toutes les données pertinentes de conception et de fabrication dans un seul modèle de produit : le « modèle intelligent ». Toutes les informations relatives au produit (comme les spécifications de conception et de contrainte, la définition géométrique, les caractéristiques des processus de fabrication et d'assemblage) sont capturées dans le modèle de produit numérique en 3D et les annotations associées. Ces informations peuvent être facilement extraites dans les livrables techniques comme les informations d'inspection, les instructions d'assemblage et les trajectoires d'outil CN.

Rempli d'informations complètes et utiles, le modèle apporte une foule d'avantages, notamment une réutilisation accrue des conceptions et l'accélération des cycles de développement de produits et des délais de commercialisation. Mais au fur et à mesure que les entreprises y accumulent les informations de conception, de comportement et de fabrication, ces fichiers CAO renferment une quantité extraordinaire de données propriétaires importantes. De plus, la mondialisation et la délocalisation accrue du développement et de la fabrication multiplient les risques d'abus.

À l'heure actuelle, une chanson à 0,99 \$ sur iTunes est mieux protégée que les modèles techniques détaillés d'un tout nouveau produit dès lors qu'ils sont en dehors du système PLM sécurisé. Alors qu'ils investissent des sommes faramineuses dans la sécurité physique et Internet (badges, clôtures, vigiles, pare-feu, mots de passe, réseaux VPN, etc.), les industriels ne protègent pas suffisamment les données qui représentent pourtant les processus de conception et de fabrication de leurs produits et qui présentent dès lors une grande vulnérabilité face aux abus. Pour limiter le risque et l'impact d'un usage abusif de la propriété intellectuelle, en particulier dans le cas d'une externalisation de la conception et de la fabrication, les industriels doivent améliorer la protection de leurs précieuses données propriétaires de développement de produits. Utilisée pour appliquer des règles d'accès durables et dynamiques dans le développement de produits, la technologie de gestion des droits numériques aide à protéger la propriété intellectuelle au niveau du fichier et à limiter les risques face à la concurrence lorsque les précieuses données sont communiquées en dehors de l'environnement sécurisé du système PLM.

## Méthodes actuelles de protection de la propriété intellectuelle et spécifications pour l'externalisation

Selon le niveau de sécurité requis, les entreprises utilisent une ou plusieurs de ces méthodes courantes pour protéger leur propriété intellectuelle :

- Sécurisation de la transmission des données à l'aide de :
  - Données cryptées
  - Réseaux privés protégés
- Contrôle d'accès au référentiel de données, individuel ou basé sur les rôles
- Contrôle d'accès au niveau du fichier protégé par mot de passe
- Occultation sélective des données de conception

La protection des données et la gestion de la propriété intellectuelle hors d'une solution sécurisée avec contrôle d'accès comme Windchill reposent généralement sur des processus manuels lourds ou difficiles à adopter et implémenter sans l'aide d'une infrastructure ou de processus appropriés. La collaboration avec les partenaires externes tend bien souvent à devenir informelle et à sortir de l'environnement contrôlé, ce qui augmente le risque d'une perte de propriété intellectuelle.

**Aujourd'hui, il est risqué de collaborer en dehors d'un environnement contrôlé : près de 50 % du partage des informations et de la collaboration se déroule de façon informelle et plus de 60 % du flux de processus et des activités de sécurité est géré manuellement.**

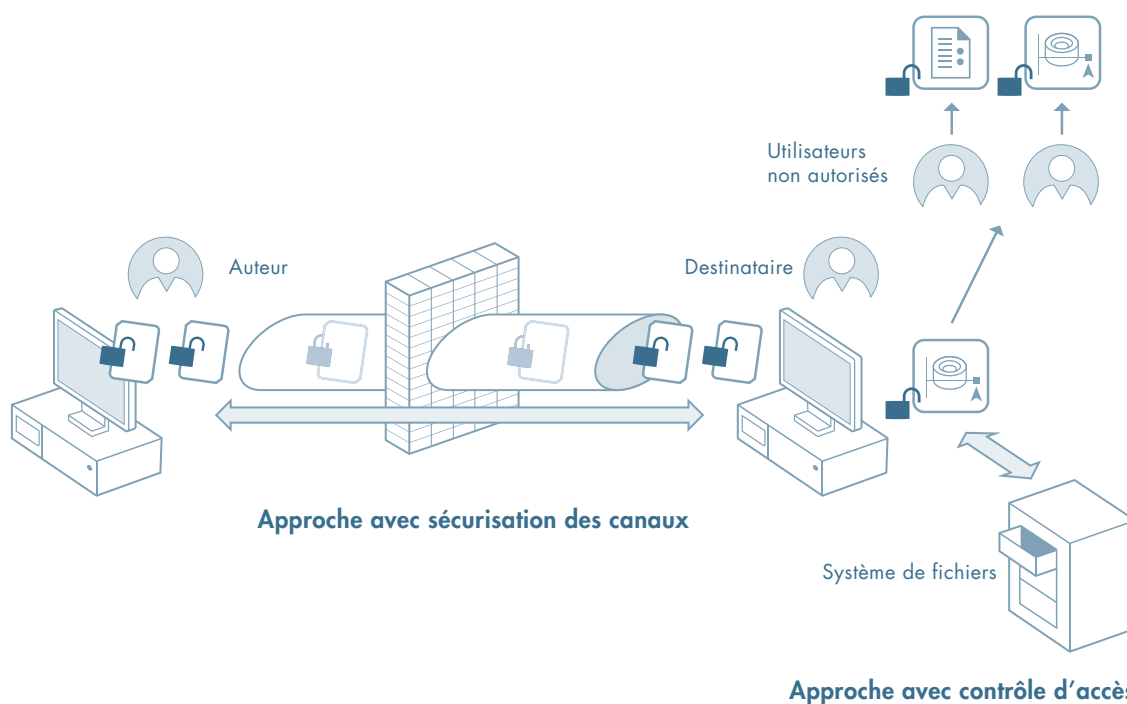
– AMR Janvier 2006

Les méthodes courantes de protection de la propriété intellectuelle garantissent une sécurité fiable dans l'environnement géré mais n'offrent pas les fonctions nécessaires pour prendre en charge un processus de développement de produits de plus en plus externalisé :

- Protection permanente des données
- Mises à jour dynamiques pour prendre en charge les modifications des conditions d'accès

Les entreprises doivent pouvoir contrôler et gérer leur propriété intellectuelle en permanence. Si un fichier confidentiel parvient à d'autres personnes que le destinataire voulu, le propriétaire du contenu doit pouvoir empêcher les parties non autorisées d'ouvrir le fichier ou d'utiliser les données.

**Les approches actuelles qui utilisent une infrastructure informatique sécurisée et contrôlent l'accès au système de gestion des données n'empêchent pas les personnes non autorisées de visualiser le contenu dès que celui-ci quitte la zone de protection physique.**



En raison du dynamisme et de la compétitivité qui caractérisent le marché actuel, les fabricants OEM et les fournisseurs doivent pouvoir interdire l'accès aux données, même aux utilisateurs qui disposaient auparavant de droits d'accès. Les systèmes de gestion de données et les fichiers protégés simplement par un mot de passe ne protègent pas les données si le fabricant OEM ou le fournisseur décide de modifier l'accès aux données transmises hors de l'environnement géré et sécurisé. Dès que les données quittent le référentiel sécurisé et que les mots de passe sont communiqués aux utilisateurs, le fabricant OEM ou le fournisseur ne peut plus révoquer les droits d'accès. Cette fonctionnalité est essentielle pour s'adapter à la réalité mouvante des sous-traitants et des chaînes logistiques, qui nécessite d'ajouter, de modifier ou de supprimer fréquemment des partenaires. Si un candidat (partenaire de conception ou fournisseur) renvoie un devis exorbitant ou si une relation prend fin, le fournisseur ou fabricant OEM doit pouvoir modifier les permissions octroyées dans le cadre d'une politique appliquée pour une pièce ou un assemblage, et révoquer les droits d'accès au fichier. Dès que les droits d'accès sont supprimés, le partenaire externe ne doit plus pouvoir ouvrir le fichier même s'il le détient encore.

Dans le cas inverse, le partenaire de conception ou le fournisseur propose un devis très compétitif, après avoir passé en revue le produit, et décroche un contrat avec l'OEM. Dans ce cas, l'OEM peut étendre les droits du partenaire, lui permettant non seulement d'ouvrir les modèles mais aussi de les imprimer et même de générer des livrables en aval tels que le noyau, la cavité ou la base de moulage, et les trajectoires d'outil CN pour usiner ces livrables. Ces livrables peuvent se trouver physiquement chez le partenaire mais l'OEM doit garder le contrôle sur les droits d'accès aux livrables pour s'assurer que seul le fournisseur puisse les manipuler et les utiliser. Par exemple, les droits d'accès à la base de moulage doivent être gérés avec les droits d'accès à la conception elle-même par le propriétaire légitime : l'OEM.

Le contrôle de version et la gestion des modifications représentent également des difficultés classiques lors de l'externalisation de projets de conception et de fabrication. Les fournisseurs et fabricants OEM doivent pouvoir s'assurer que leurs partenaires utilisent bien les informations produites les plus récentes. En autorisant l'accès à l'unique version correcte des fichiers et en interdisant l'accès à toutes les autres versions qui sont peut-être utilisées en dehors de l'environnement géré, il est possible de « détruire » tous les fichiers obsolètes, où qu'ils se trouvent.

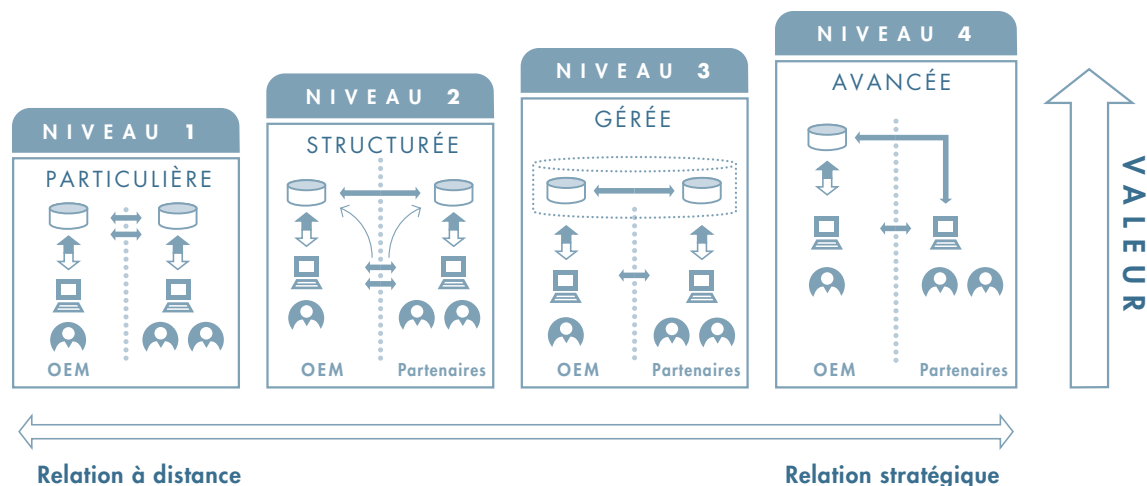
## Pro/ENGINEER Rights Management Extension

### Fonctionnalités Pro/ENGINEER pour la gestion des droits numériques en CFAO



Avec Pro/ENGINEER Wildfire 4.0, les utilisateurs PTC peuvent désormais protéger leurs modèles et dessins Pro/ENGINEER au moyen d'un cryptage fort et d'un ensemble variable de droits d'accès aux fichiers pour des utilisateurs spécifiques. Ces permissions correspondent aux différents niveaux de confiance entre les deux parties et sont définies de façon à prendre en charge les processus courants rencontrés actuellement dans le développement de produits au niveau mondial.

Les fonctionnalités de gestion des droits numériques au niveau du fichier sont nécessaires dans toutes les relations d'externalisation de la conception et de la fabrication.

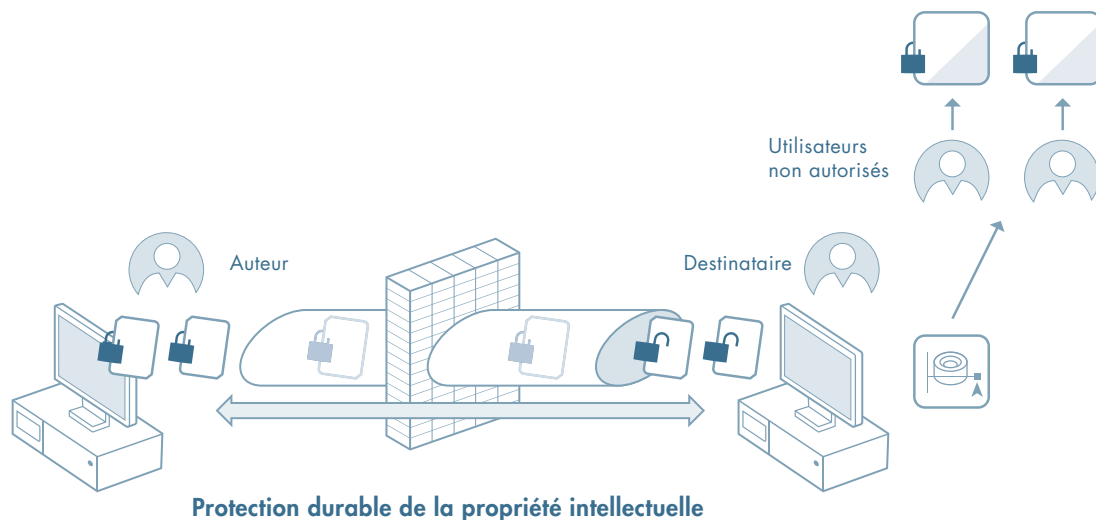


Par exemple, un OEM doit transmettre des données à un fournisseur afin de lui permettre d'établir un devis pour la fourniture d'une pièce. L'OEM veut toutefois éviter que le fournisseur ne communique par inadvertance la propriété intellectuelle à d'autres personnes (par exemple : e-mail à un destinataire incorrect, virus, fuite via l'infrastructure informatique non sécurisée du fournisseur) ou que le fournisseur (ou des fournisseurs potentiels qui ne sont pas encore des partenaires de confiance) ne s'empare volontairement des données essentielles.

Grâce à Pro/ENGINEER Rights Management Extension (RMX) et Adobe® LiveCycle® Rights Management ES, l'OEM peut affecter une politique spécifique de gestion des droits numériques à partir d'un serveur, qui permet aux utilisateurs désignés du fournisseur d'exécuter certaines opérations sur le fichier (par exemple, la simple ouverture) durant une période déterminée. Cette politique d'accès permet d'ouvrir et d'interroger le fichier de pièce ou d'assemblage (cotes, sections, etc.) mais empêche toute action susceptible de conserver ou reproduire les données (enregistrement, exportation, copie de la géométrie, enveloppe simplifiée, génération de livrables de fabrication, etc.).

À la différence des fichiers protégés par un simple mot de passe, les fichiers Pro/ENGINEER protégés bénéficient d'une protection durable et dynamique. L'OEM peut accorder des droits supplémentaires ou interdire l'accès rapidement et facilement à partir du serveur de politiques. Il peut modifier les permissions associées à la politique appliquée à la pièce ou à l'assemblage et révoquer à tout moment le droit d'accès du fournisseur. Quand l'OEM a modifié les droits d'accès aux fichiers (même si ceux-ci sont encore en la possession du fournisseur), le serveur des politiques d'accès est interrogé lors de la récupération ultérieure dans Pro/ENGINEER, et le droit d'ouverture du fichier est contrôlé avant d'être accordé ou refusé en fonction de la politique mise à jour. Pro/ENGINEER permet également à l'OEM de garder le contrôle sur les permissions relatives aux livrables en aval, pour en réserver l'accès et l'utilisation au seul fournisseur autorisé.

**La protection durable de la propriété intellectuelle assurée par Pro/ENGINEER et Adobe empêche les utilisateurs non autorisés d'accéder aux données confidentielles lorsque le fichier se trouve hors du système sécurisé de gestion de contenu et de processus.**



Outre l'affectation de politiques et l'application de permissions, Pro/ENGINEER offre des fonctionnalités d'audit complètes qui consignent les tentatives d'ouverture de contenu protégé, que celles-ci soient réussies ou non. Pour le propriétaire du contenu, ces rapports indiquent quand et comment un modèle a été ouvert, et fournissent des données chiffrées qui permettent de suivre l'utilisation du modèle faite par chaque partenaire.

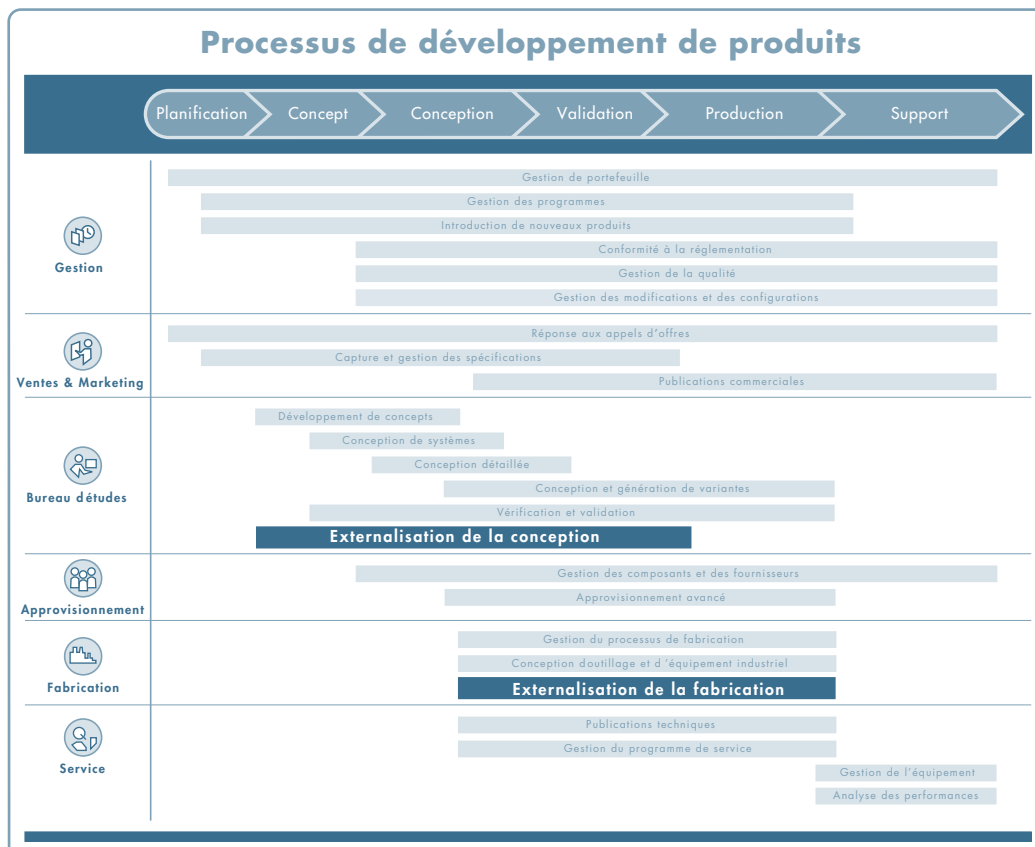
Les fonctionnalités de gestion des données numériques de Pro/ENGINEER améliorent également les processus de contrôle de version et de gestion des modifications, en particulier lors de l'externalisation de projets de conception et de fabrication. Dans l'exemple précédent, l'OEM peut facilement modifier l'accès aux fichiers protégés hors du pare-feu ou des référentiels de données sécurisés. En autorisant l'accès à l'unique version correcte des fichiers et en interdisant l'accès à toutes les autres, l'OEM est certain que ses partenaires utilisent les bonnes informations.

L'implémentation de technologies de gestion des données numériques pour protéger vos précieuses données de conception au niveau du fichier lorsqu'elles se trouvent hors de l'environnement sécurisé du système de gestion de contenu et de processus peut vous aider à améliorer vos processus d'externalisation de la conception et de la fabrication. Pour obtenir des résultats optimaux, les entreprises doivent :

- Évaluer le risque couru par la propriété intellectuelle de conception au cours des processus de développement de produits
- Définir les processus et politiques d'accès aux données de conception pour les intervenants internes et externes
- Implémenter un système garantissant une sécurité complète de la propriété intellectuelle et offrant une protection durable et dynamique des données CAO au niveau du fichier
- Automatiser le processus d'application, de gestion et de surveillance de la propriété intellectuelle au niveau du fichier et des politiques d'accès

Un système complet (intégrant les processus et la technologie) de protection de la propriété intellectuelle de conception sécurise la collaboration, réduit les risques de perte de propriété intellectuelle, renforce le contrôle de version et améliore le processus de gestion des modifications. Pro/ENGINEER RMX et Adobe LiveCycle Rights Management ES fournissent la technologie la plus avancée pour protéger la propriété intellectuelle contenue dans les fichiers Pro/ENGINEER, PDF, Microsoft Word et Excel. L'organisation PTC Global Services offre plusieurs types de services (conseil en processus, mise en œuvre des systèmes, solutions de formation innovantes, gestion des actifs) de façon à mettre à la disposition de nos clients les processus nécessaires à l'exploitation et la protection optimales de leurs données Pro/ENGINEER. PTC propose également des programmes de formation spécialement conçus pour favoriser l'adoption.

Pro/ENGINEER Rights Management Extension améliore les processus d'externalisation de la conception et de la fabrication.



PTC est le seul éditeur de logiciels à adopter une approche proactive et intégrée pour inclure la gestion des droits numériques dans sa principale solution CAO. D'autres fournisseurs de solutions CAO/PLM ne sont pas actifs dans ce domaine et laissent le travail d'intégration aux partenaires. Par conséquent, les solutions qu'ils proposent ne protègent pas convenablement la propriété intellectuelle en raison des innombrables possibilités de fuite ou sont trop lourdes pour permettre de travailler efficacement dans le système CAO. La sécurité et la protection des données de conception de nos clients étant trop importantes pour se satisfaire d'une intégration imparfaite, PTC a choisi une approche directe qui garantit l'intégration optimale de la gestion des droits numériques dans Pro/ENGINEER. Le résultat est un environnement équilibré de productivité et de sécurité, deux éléments indispensables aux entreprises de développement de produits.

PTC est à l'avant-garde de la protection de la propriété intellectuelle dans le domaine de l'ingénierie grâce à sa relation stratégique avec Adobe et à l'intégration de Pro/ENGINEER et d'Adobe LiveCycle Rights Management ES.

Pour plus d'informations, visitez notre site Web à la page [www.ptc.com/go/proengineer/drm](http://www.ptc.com/go/proengineer/drm)

Copyright © 2007, Parametric Technology Corporation (PTC) – Tous droits réservés en vertu des lois sur le copyright des États-Unis d'Amérique et d'autres pays. Les informations décrites dans le présent document s'appuient sur l'expérience d'un utilisateur unique. Ces informations sont fournies à titre informatif uniquement, sont susceptibles d'être modifiées sans préavis et ne sauraient en aucun cas tenir lieu de garantie ou d'engagement de la part de PTC.