Rocket

EBOOK

5 étapes pour sécuriser vos échanges de données de produit dans Teamcenter

Comment créer un processus d'échange de données de produit sécurisé

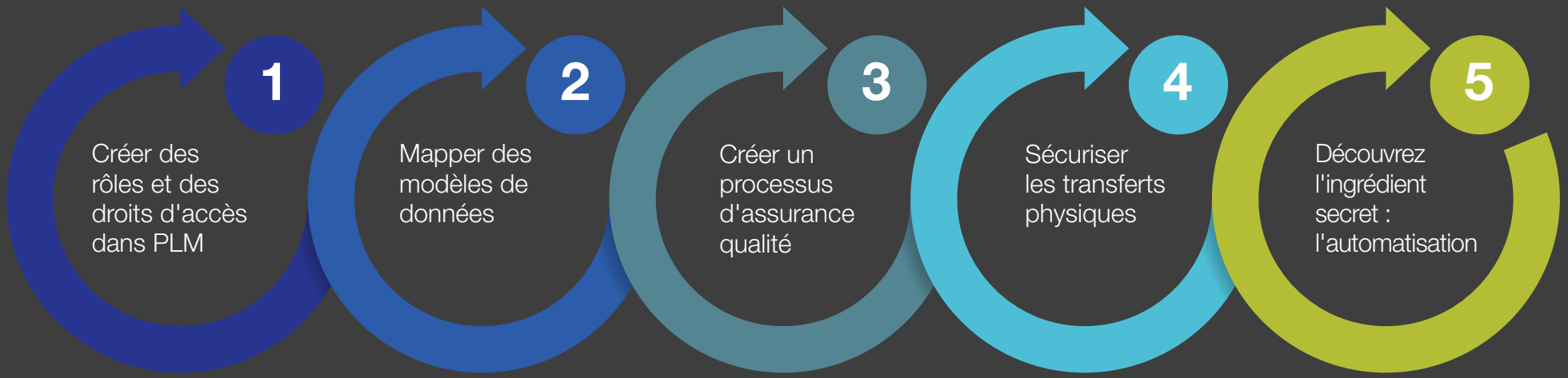
Les fabricants du monde entier se préoccupent de la sécurité de leur propriété intellectuelle, en particulier de la sécurité des données de conception de produit. Ils s'appuient sur des écosystèmes de chaînes d'approvisionnement complexes pouvant inclure des dizaines de fournisseurs et de partenaires qui échangent des données souvent au quotidien. Que ce soit avec un fournisseur de niveau 1 ou 2, un partenaire de coentreprise ou un fabricant d'équipement d'origine (OEM), des interactions fréquentes introduisent des risques dans le processus d'échange de données. Il serait imprudent de prendre en compte la sécurité du processus d'échange de données uniquement à l'extrémité finale.

L'industrie automobile est particulièrement vulnérable, car sa chaîne d'approvisionnement est complexe et distribuée à l'échelle mondiale. Il est difficile de garder une longueur d'avance et tout avantage dont dispose une entreprise du fait de sa propriété intellectuelle est temporaire. Le seul moyen de tirer profit de cet avantage consiste à mettre un produit sur le marché le plus rapidement possible. Cependant, sans la bonne approche en matière de sécurité, de processus et de standardisation, cet avantage peut rapidement disparaître.

Les fournisseurs de niveau 1 et 2 doivent gérer des échanges de données sécurisés entre plusieurs parties tout en tenant compte de leurs propres procédures internes de gestion de données. Les employés qui travaillent avec des outils de CAO et de PLM imposés par des partenaires OEM gaspillent souvent leurs talents pour effectuer des tâches manuelles fastidieuses d'échange de données de produit (PDX). Cela est particulièrement vrai pour les entreprises qui utilisent le logiciel Siemens Teamcenter®. La sécurisation du PDX nécessite plusieurs étapes ; la procédure appropriée, de la configuration de l'environnement Teamcenter à l'envoi et à la réception des données, contribue grandement à la sécurité de votre propriété intellectuelle et des données de vos clients.

La première section de cet ebook explique la stratégie en 5 étapes pour sécuriser l'échange de données de produit. La deuxième section explique comment déployer la stratégie dans Teamcenter.

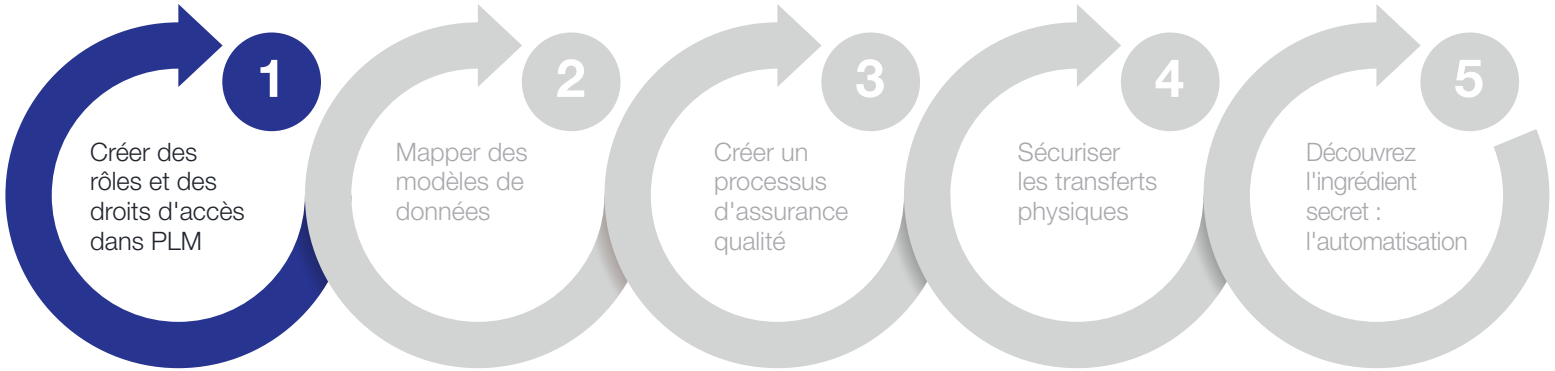
Cinq étapes pour créer un processus PDX sécurisé



1 Créer des rôles et des droits d'accès dans PLM

Créez des rôles et des droits d'accès dans votre système PLM afin de limiter l'accès à certains fichiers aux bonnes personnes et de créer des flux d'information qui définissent (et contrôlent) l'état de vos données. Limiter la sélection des données en fonction du modèle de sécurité que vous avez appliqué permet d'empêcher les utilisateurs d'envoyer des états de cycle de vie incorrects aux partenaires. Sans stratégie, les utilisateurs peuvent potentiellement exporter toutes les données de votre environnement PLM, quel que soit leur état et leur caractère sensible.

Par exemple, un fabricant travaillant avec Nissan® et Ford® sur de nouveaux systèmes de tableau de bord peut décréter dès le début que les ingénieurs travaillant sur le produit Nissan ne pourront pas accéder aux fichiers de produits Ford, et inversement.

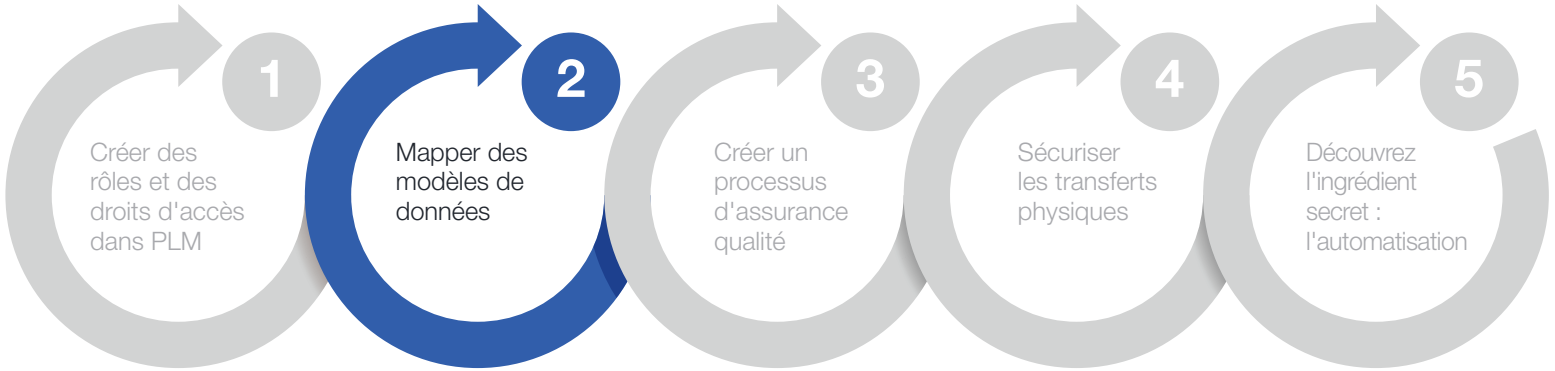


2 Mapper des modèles de données

Configurez votre solution PLM à l'aide d'un modèle de données répondant aux besoins de votre entreprise et aux exigences requises pour la gestion des données client (types d'éléments, attributs, etc.). Établissez une correspondance entre votre modèle de données PLM et le modèle de données du partenaire pour l'envoi comme pour la réception de données, afin de pouvoir traiter efficacement des ensembles de données de conception. Cela vous permettra de traiter en toute sécurité des fichiers de données à partir de votre propre modèle de données et de vos conventions de dénomination, puis de les transférer dans le modèle de données et les conventions de dénomination d'un partenaire. Cela inclut le mappage d'attributs, le changement de nom de structure, la comparaison des ensembles lors de l'importation et la vérification de la qualité.

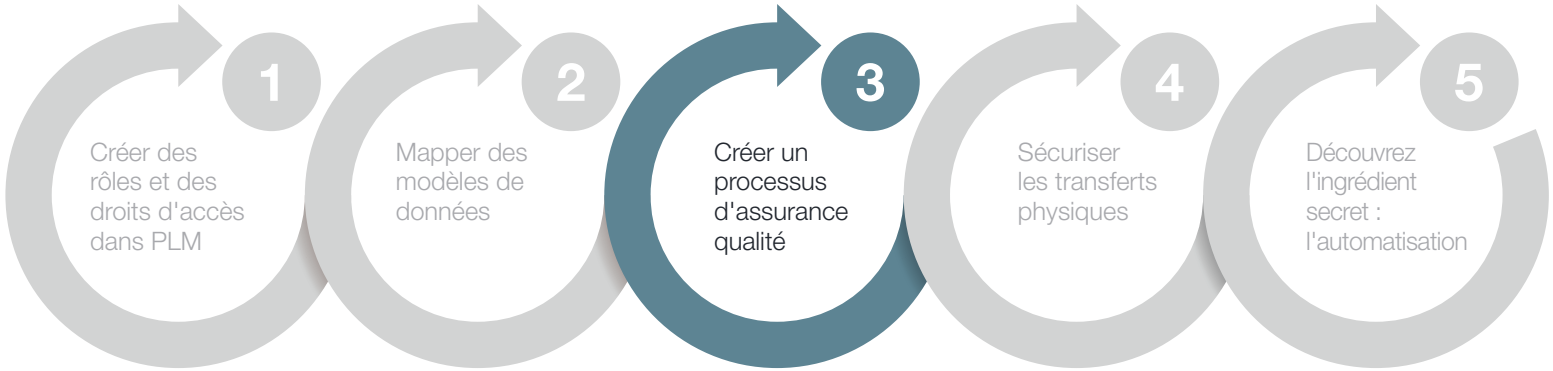
Les fabricants ont généralement leurs propres conventions de dénomination, tout comme leurs partenaires. Pour poursuivre avec l'exemple ci-dessus, imaginez une situation où Nissan utilise le système de CAO A avec la convention de dénomination « Product_Assembly_Version_Date », Ford utilise le système de CAO B avec « Date_Product_Assembly_Version » et votre société utilise « Date_Version_Product_Assembly ». Si vous commencez un projet en configurant votre flux d'information de façon à gérer automatiquement la personnalisation des noms de fichiers et des conversions, vous pouvez réduire le risque d'erreurs humaines pouvant entraîner des violations de sécurité accidentelles et des perturbations ailleurs dans la chaîne d'approvisionnement.

Bonus supplémentaire, l'automatisation de ce processus libère les ingénieurs des tâches courantes associées au partage externe des données, comme par exemple le changement de nom des fichiers de pièces. Cela permet aux OEM, aux fournisseurs et à toute autre personne impliquée dans la chaîne d'approvisionnement de gagner du temps et de l'argent.



3 Créer un processus d'assurance qualité

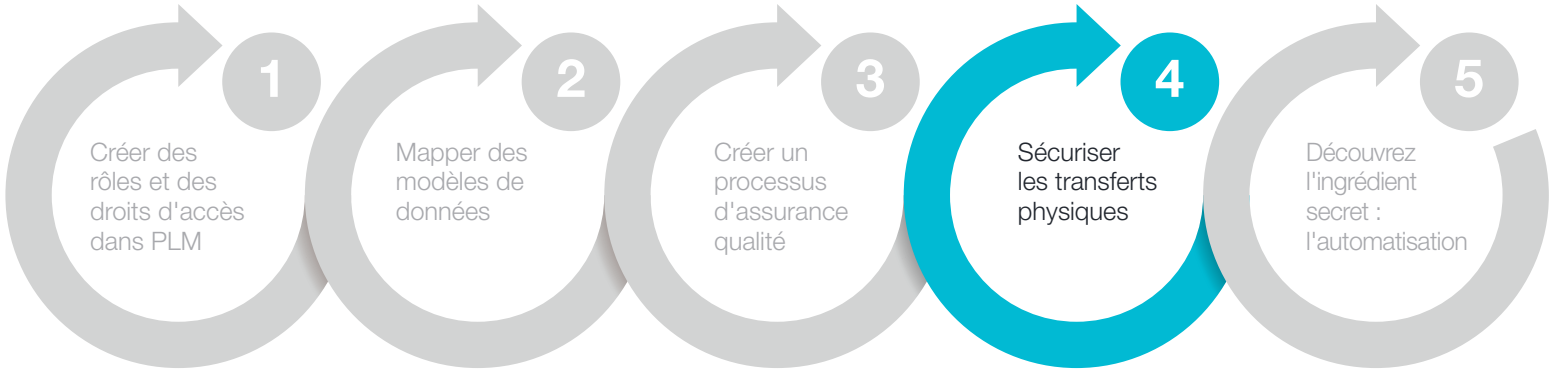
Même si vous essayez d'éviter les failles de sécurité et d'assurance qualité (AQ) par le biais de l'automatisation et de la configuration, il y a encore un risque que quelque chose passe à travers les mailles du filet. Créez un processus d'assurance qualité « passe-partout » pour vous assurer que les erreurs et les failles de sécurité soient détectées avant l'échange de données. Il existe un certain nombre de solutions tierces exceptionnelles, telles que TECHNIA Q-checker pour Dassault Systèmes CATIA® et Heidelberg® CAx Quality Manager (HQM) pour Siemens NX®, qui permettent de s'assurer que les données de CAO sont conformes aux exigences de qualité d'un client donné. Certaines de ces solutions se connectent directement à votre processus PLM et/ou PDX et s'exécutent automatiquement.



4 Sécuriser les transferts physiques

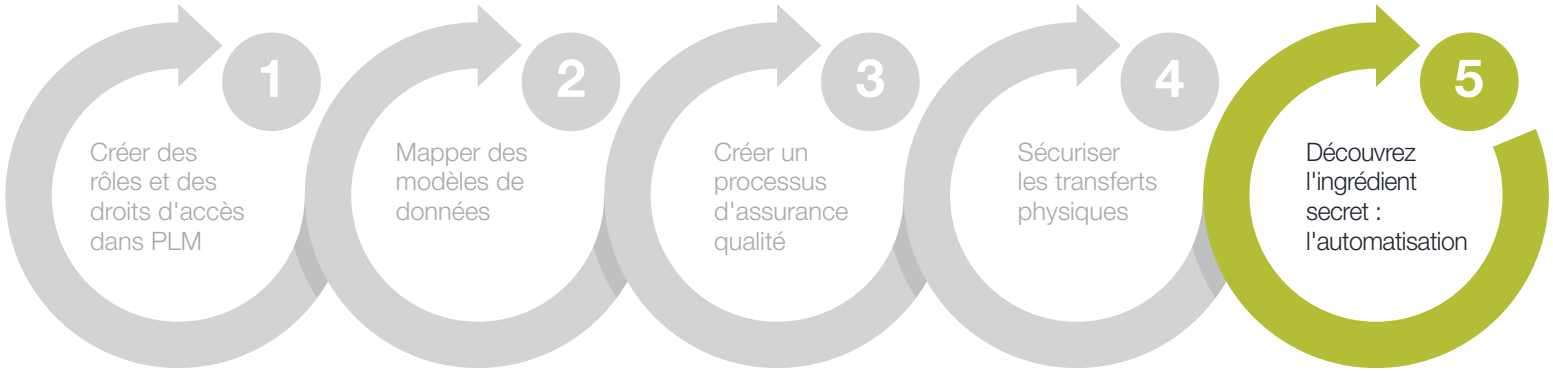
Le transfert physique des fichiers IP est la partie la plus visible de la stratégie de sécurité, et l'une des étapes les plus critiques pour bien faire les choses. Normalisez la manière dont votre entreprise traite et échange les données de conception de produits avec les partenaires dans tous les projets en configurant votre système de façon à ce qu'il prenne automatiquement des décisions pour l'utilisateur. Éliminez également les processus de diffusion à haut risque tels que les services de partage de fichiers par messagerie électronique, FTP et un cloud B2C. Assurez-vous que votre processus standard inclut un niveau approprié de chiffrement des données, par exemple des clés de chiffrement publiques/privées pour les besoins de personne à personne.

N'oubliez pas d'envisager un processus sécurisé pour la réception et le stockage des fichiers de données, ainsi que pour leur envoi. Le partage sécurisé des données ne constitue que la moitié de l'équation ; vous devez également pouvoir importer et héberger des données de conception de produits en toute sécurité. C'est l'un des aspects les plus difficiles pour la mise en place d'un processus sécurisé d'échange de données.



5 Découvrez l'ingrédient secret : l'automatisation

Vous avez déjà probablement remarqué que l'automatisation est un thème commun à la plupart de ces étapes, et ce, pour une bonne raison. La mesure la plus efficace pour minimiser les risques de sécurité dans votre processus PDX consiste à automatiser le plus possible. L'erreur humaine constitue la première menace pour la sécurité de la propriété intellectuelle de toute entreprise ; la réduction des interactions humaines avec le processus PDX la rendra plus sûre. L'automatisation est une option intrinsèquement sécurisée, car cela limite les risques d'erreur humaine.



Comment créer un processus d'échange de données de produit sécurisé ***avec Siemens Teamcenter et Rocket Software***

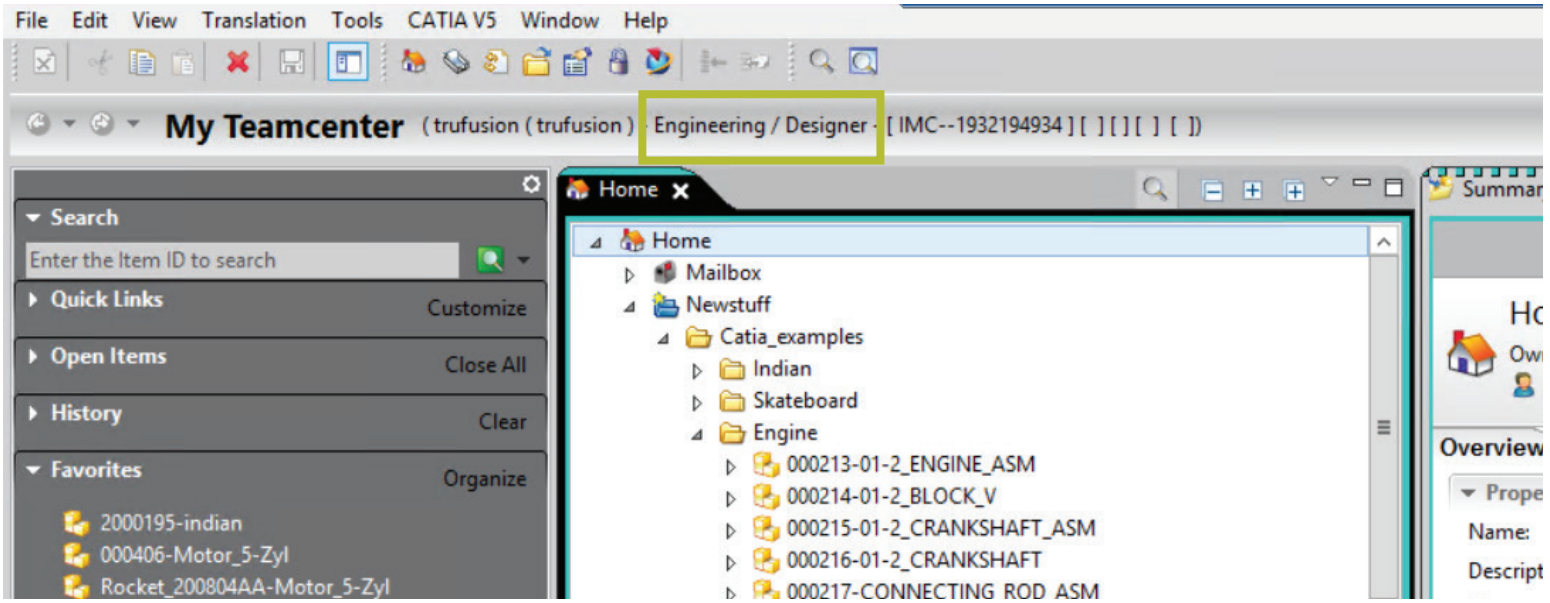
Rocket® TRUfusion™ Enterprise est une solution complète et sécurisée d'échange de données de produit qui aide les clients Teamcenter du monde entier à échanger des données de conception de produits et d'autres propriétés intellectuelles avec des partenaires de la chaîne d'approvisionnement et des sites de fabrication internes distants. Les clients de TRUfusion Enterprise minimisent les risques inhérents au partage de données de conception en remplaçant les tâches d'échange de données manuelles et déconnectées par des processus automatisés conçus pour s'exécuter directement dans Teamcenter. L'automatisation avec TRUfusion permet aux ingénieurs d'économiser potentiellement des milliers d'heures par an, le temps gagné dans les tâches administratives pouvant être utilisé pour des tâches plus importantes qui soutiennent les objectifs de l'entreprise.

Les pages suivantes montrent comment la combinaison de Rocket TRUfusion Enterprise et Teamcenter peut vous aider à répondre à chacune des cinq recommandations présentées ci-dessus.

1 Créer des rôles et des droits d'accès dans PLM

Vous pouvez configurer votre intégration TRUfusion Enterprise avec Teamcenter pour prendre en compte les modèles de sécurité dans Teamcenter et autoriser les utilisateurs à sélectionner uniquement les fichiers appropriés lors de leur communication avec les partenaires de la chaîne logistique.

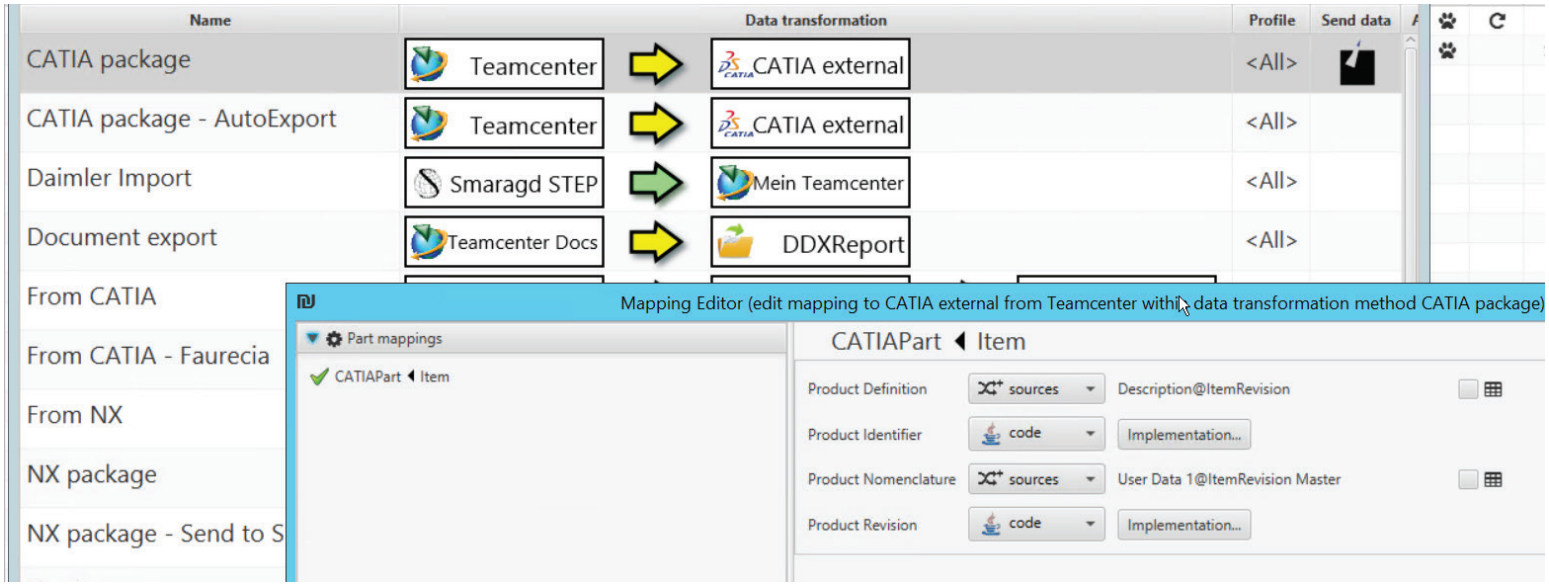
Nous vous recommandons d'inclure des filtres et des créations de rôle lors du déploiement initial de Teamcenter ou de l'ajout de nouveaux projets à votre implémentation Teamcenter. Votre administrateur ou consultant en implémentation peut facilement ajouter les rôles à votre instance Teamcenter. Des groupes, rôles et utilisateurs peuvent être créés dans la section Organisation de Teamcenter, l'un étant un sous-ensemble de l'autre. Par exemple, si Utilisateur1 a le rôle de « Responsable Produit A » et que le rôle « Responsable Produit A » fait partie du groupe « Client A », alors Utilisateur1 doit hériter de toutes les fonctionnalités d'accès au sein du rôle Client A Responsable de produit, et ainsi de suite.



Lorsque des rôles sont configurés dans Teamcenter, ils sont clairement visibles dans le programme

2 Mappage des modèles de données dans Teamcenter

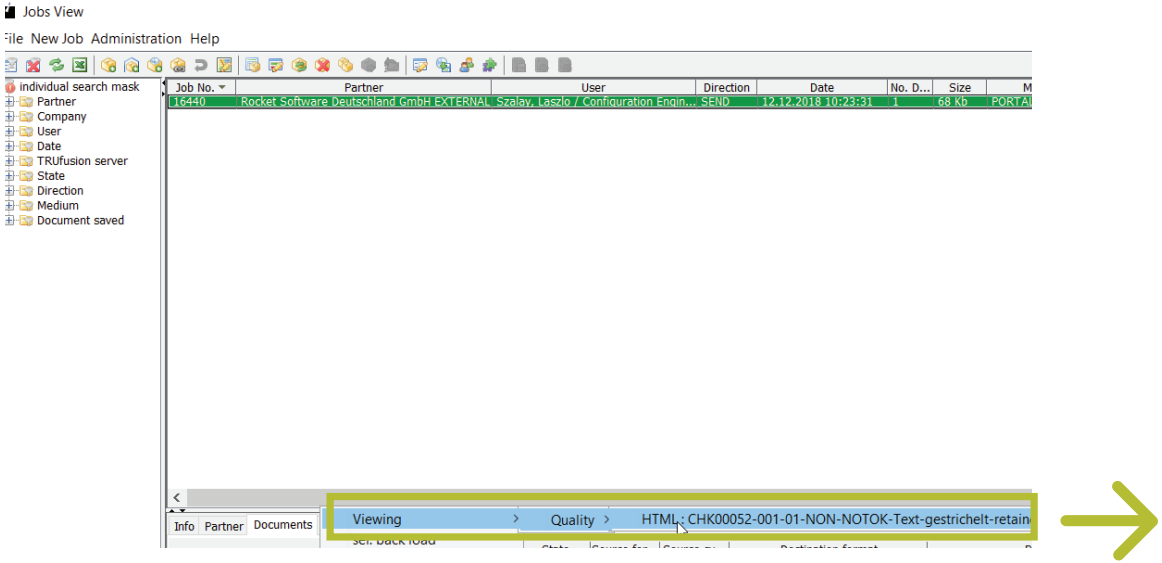
Vous pouvez configurer l'intégration Teamcenter pour mapper les attributs et les ensembles de données entre votre modèle de données Teamcenter et le modèle de données de l'OEM ou du partenaire pour l'envoi et la réception de données. Il s'agit d'une étape plus technique qui nécessite l'écriture de scripts pour mapper des attributs et d'autres données de produit d'un programme à un autre.



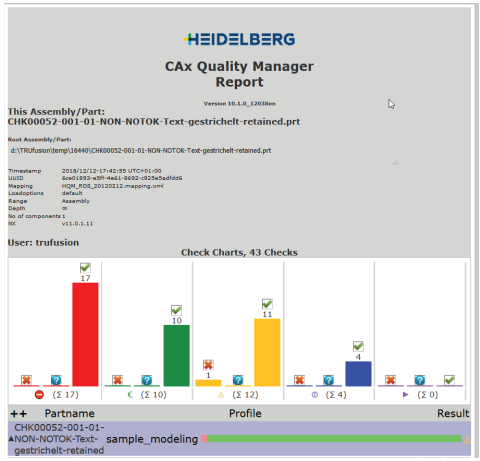
Mappage entre les modèles internes et les modèles de l'OEM ou du partenaire pour faciliter l'échange de données

3 Créer un processus d'assurance qualité

Envisagez d'utiliser des outils d'assurance qualité CAO supplémentaires pour éviter les failles de sécurité et vous conformer aux normes de qualité CAO/FAO ainsi qu'aux exigences de dénomination de votre partenaire. TRUfusion Enterprise fournit des intégrations avec Q-Checker (pour CATIA V5) et HQM (pour NX) permettant d'exécuter des vérifications dans le cadre du flux d'échange de données habituel. Pour chaque travail, l'intégration définit l'environnement correct (version CAO, version Q-Checker-/HQM, profil de vérification) afin d'exécuter Q-Checker/HQM en mode par lot et fournir des résultats via l'interface TRUfusion Enterprise s'il doit être examiné. Si tout semble correct, le travail est traité et terminé ; si une erreur ou une alerte se produit, le travail est interrompu pour que les données de CAO puissent être corrigées et soumises à nouveau.



Accès direct aux outils AQ CAO dans TRUfusion Enterprise

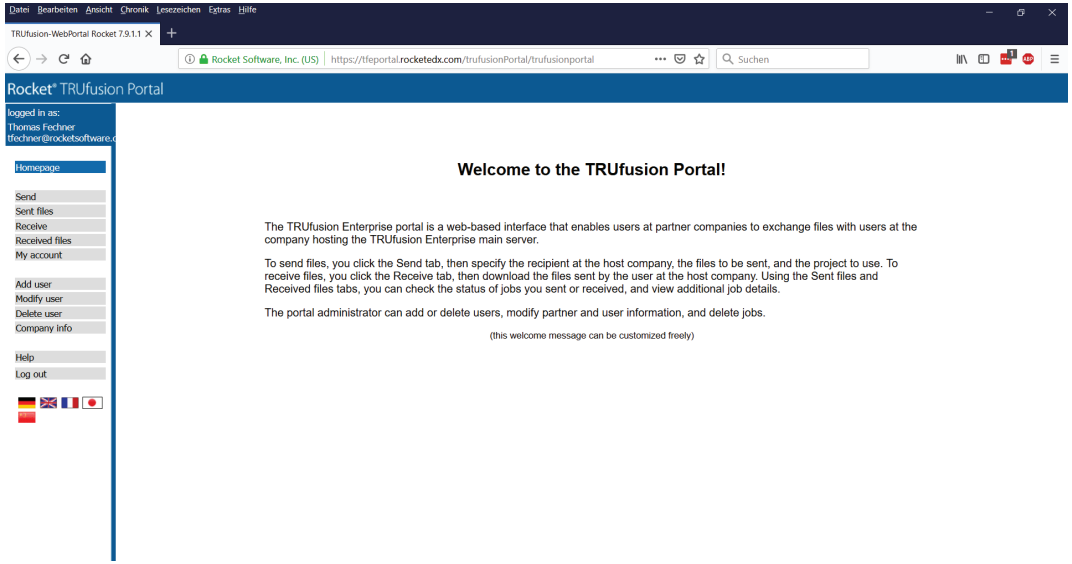


Exemple de rapport de l'outil d'assurance qualité CAO

4 Sécuriser les transferts physiques

TRUfusion Enterprise est configuré pour gérer les types de données que vous avez sélectionnés, les étapes de traitement des données correspondant, ainsi que le conditionnement et la diffusion nécessaires. Une fois reçues, vous et le partenaire pouvez utiliser les données selon vos besoins. Nous proposons plusieurs solutions qui fonctionnent en tandem avec TRUfusion pour un transfert de fichiers physiques sécurisé :

- Protocole de transfert de fichiers Odette (OFTP2) sur Internet via Rocket Eurex-c
- Un portail Web, via le portail Rocket TRUfusion Enterprise
- Une solution d'échange de fichiers SaaS, Rocket TRUexchange



Le portail TRUfusion est un moyen sécurisé de recevoir et d'envoyer des données de CAO et d'autres données à des partenaires et à des employés de sites distants.

5 Découvrez l'ingrédient secret : l'automatisation

L'automatisation est au cœur de TRUfusion Enterprise et cela vous permet d'automatiser l'ensemble du processus d'échange de données entre Teamcenter et le partenaire, notamment :

- Importer/exporter dans Teamcenter
- Mappage des attributs et des conventions de dénomination entre les systèmes CAO et PLM pour convertir différents modèles de données
- Vérifications qualité CAO
- Conversion vers/à partir de formats neutres (par exemple STEP, IGES, 3DPDF, JT)
- Conversion entre les formats de fichiers de CAO natifs des principaux fournisseurs (par exemple, CATIA V5 vers NX), à l'aide de convertisseurs tiers intégrés
- Conditionnement spécifique au format
- Transfert de fichiers sécurisé
- Notifications par e-mail
- Documentation de la piste de vérification complète
- Archivage

Échange sécurisé de données de produit avec Rocket

Le respect de ces étapes vous aidera à rester compétitif sur le marché, en vous permettant de répondre rapidement aux appels d'offres et de réaliser rapidement des projets critiques. Et, bien sûr, vos ingénieurs économiseront des heures de travail sur chaque projet.

Avec TRUfusion Enterprise, vous pouvez être sûr que votre équipe sera en mesure d'échanger rapidement et facilement des données avec des partenaires, de suivre des processus cohérents, de limiter les erreurs et d'assurer la sécurité des données de conception de produit.

Demander une démonstration TRUfusion

Rocket

rocketsoftware.com
info@rocketsoftware.com
États-Unis : 1 855 577 4323
EMEA : 0800 520 0439
APAC : 612 9412 5400
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com