EBOOK

5 Steps for Securing Your Product Data Exchange Within Teamcenter

How to create a secure product data exchange process

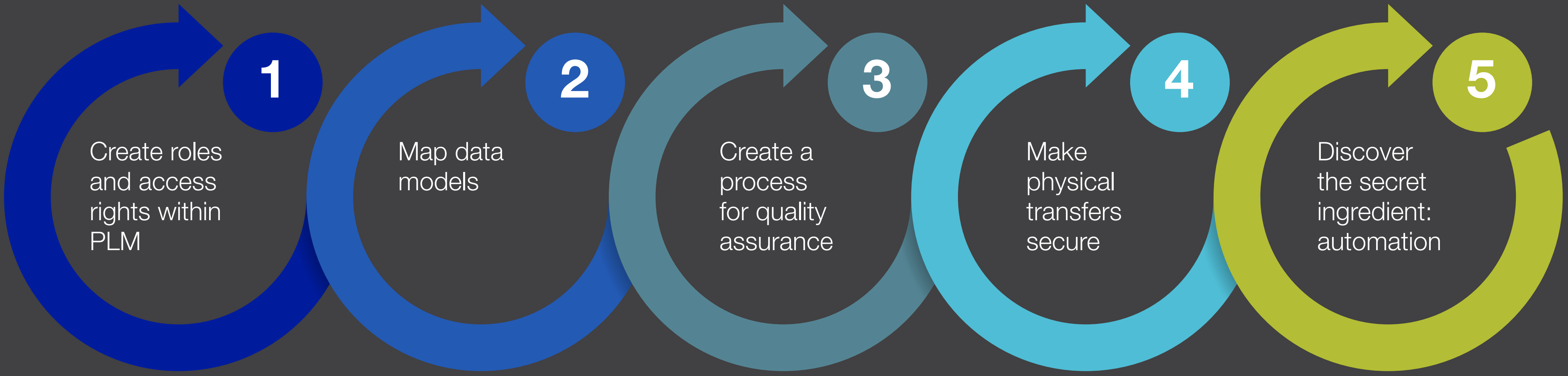
Manufacturers worldwide are concerned about the security of their intellectual property (IP)—especially the security of valuable product design data. They rely on complicated supply chain ecosystems that can include dozens of suppliers and partners, often exchanging data on a daily basis. Whether it's with a Tier 1 or 2 supplier, a JV partner or an original equipment manufacturer (OEM), frequent interactions introduce the opportunity for risk in the data exchange process. It would be reckless to consider the security of the data exchange process solely at the end.

The automotive industry is particularly vulnerable, as its supply chain is complex and globally distributed. It's difficult to stay ahead, and any advantage a company has with respect to their IP is temporary. Getting a product to market as quickly as possible is the only way to realize that advantage, but without the right approach to security, process and standardization, that advantage can quickly disappear.

Tier 1 and 2 suppliers have to manage secure data exchanges across a range of parties while staying aligned to their own internal data management procedures. Employees who work with CAD and PLM tools mandated by OEM partners often waste their talents dealing with time-consuming, manual product data exchange (PDX) tasks. This is especially true for companies using Siemens Teamcenter® software. Securing PDX requires several steps; the proper procedure—from configuring the Teamcenter environment to the sending and receiving of data—contributes greatly to the security of your IP, and of your customer's data.

The first section of this eBook explains the 5 step strategy to securing product data exchange. The second section provides how to deploy the strategy within Teamcenter.

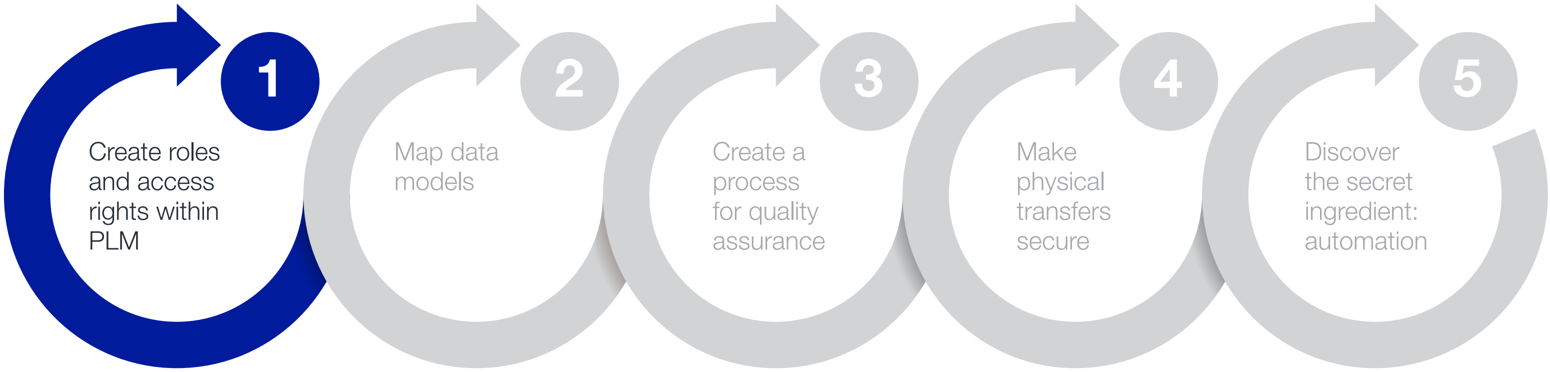
Five steps for building a secure PDX process


1
Create roles and access rights within PLM
2
Map data models
3
Create a process for quality assurance
4
Make physical transfers secure
5
Discover the secret ingredient: automation

1 Create roles and access rights within PLM

Build out roles and access rights within your PLM system so you can filter access of certain files to the right people, and create workflows that set (and control) the status of your data. Limiting the selection of data based on the security model you've applied helps prevent users from sending incorrect lifecycle statuses to partners. Without a strategy, users can potentially export any data within your PLM environment, regardless of its status and sensitivity.

For example, a manufacturer working with both Nissan® and Ford® on new dashboard systems can establish at the beginning that engineers working on the Nissan product can't access Ford product files, and vice versa.

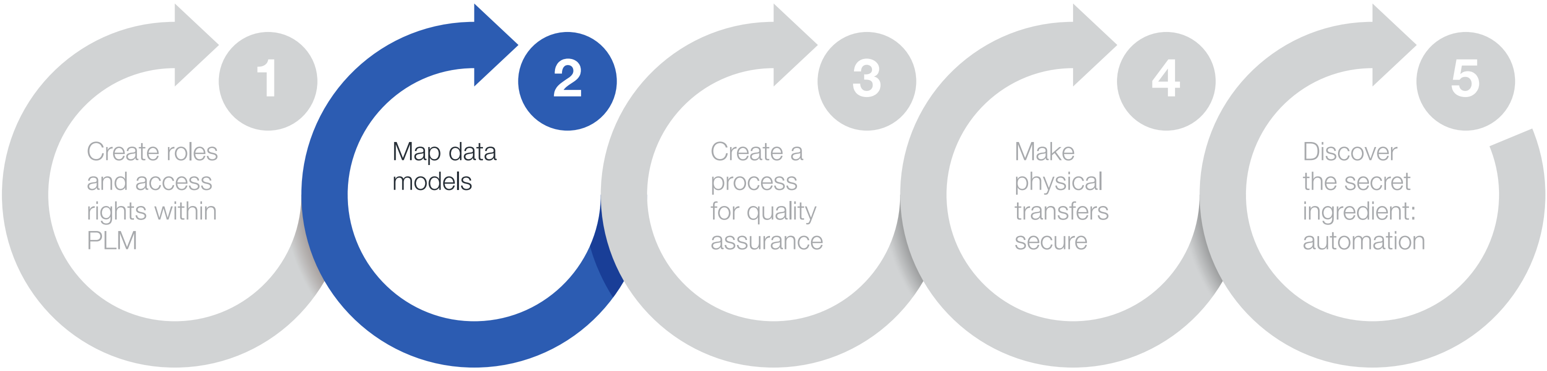

1
Create roles and access rights within PLM
2
Map data models
3
Create a process for quality assurance
4
Make physical transfers secure
5
Discover the secret ingredient: automation

2 Map data models

Configure your PLM solution with a data model that satisfies the needs of your company, as well as the necessary requirements of handling customer data (item types, attributes, etc.). Map between your PLM data model and the partner's data model for both sending and receiving data so that packages of design data can be processed efficiently. This will allow you to securely process and transfer data files from your own data model and naming conventions into a partner's data model and naming conventions. This includes attribute mapping, structure renaming, package comparison on import, and quality checking.

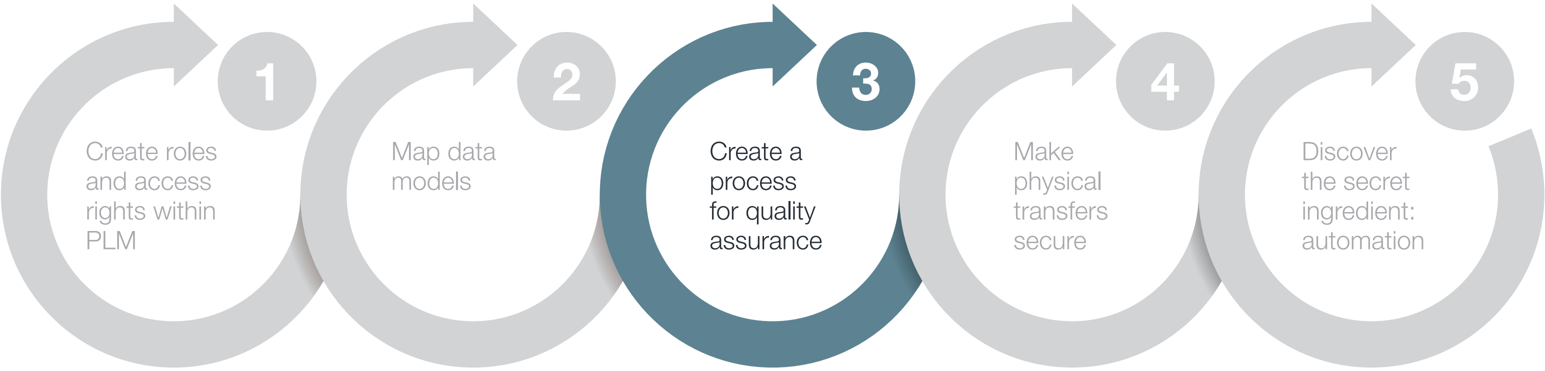
Manufacturers typically have their own naming conventions, as do their partners. To continue with the above example, imagine a situation where Nissan uses CAD system A with the naming convention "Product_Assembly_Version_Date," Ford uses CAD system B with "Date_Product_Assembly_Version," and your company uses "Date_Version_Product_Assembly." If you begin a project by configuring your workflow to handle customization of the file names and conversions automatically, you can minimize the chance of human errors that can cause accidental security breaches and disruptions elsewhere along the supply chain.

As an added bonus, automating this process frees engineers from mundane tasks associated with sharing data externally, such as renaming parts files. This saves time (and money) for OEMs, suppliers, and anyone else involved in the supply chain.


1
Create roles and access rights within PLM
2
Map data models
3
Create a process for quality assurance
4
Make physical transfers secure
5
Discover the secret ingredient: automation

3 Create a process for quality assurance

While you try to prevent security and quality assurance (QA) shortfalls via automation and configuration, there's still a chance something will slip through the cracks. Build a "catch-all" QA process to make sure security vulnerabilities and errors are caught before the data exchange occurs. There are a number of great third-party solutions out there, such as TECHNIA Q-checker for Dassault Systèmes CATIA® and Heidelberg® CAx Quality Manager (HQM) for Siemens NX®, that help ensure CAD data complies with a given customer's quality demands. Some of these solutions will even plug directly into your PLM and/or PDX process to run automatically.


1 Create roles and access rights within PLM

2 Map data models

3 Create a process for quality assurance

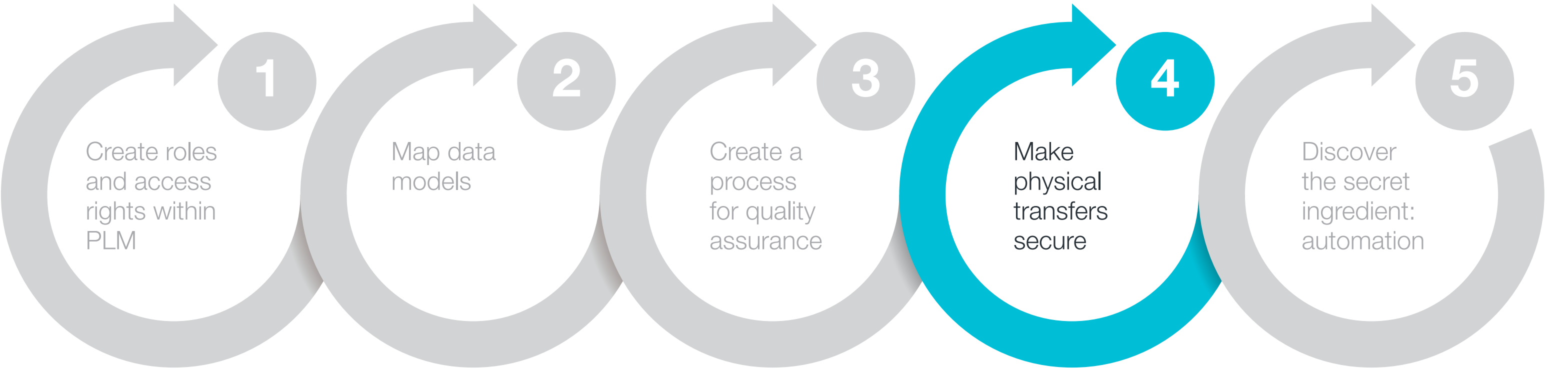
4 Make physical transfers secure

5 Discover the secret ingredient: automation

4 Make physical transfers secure

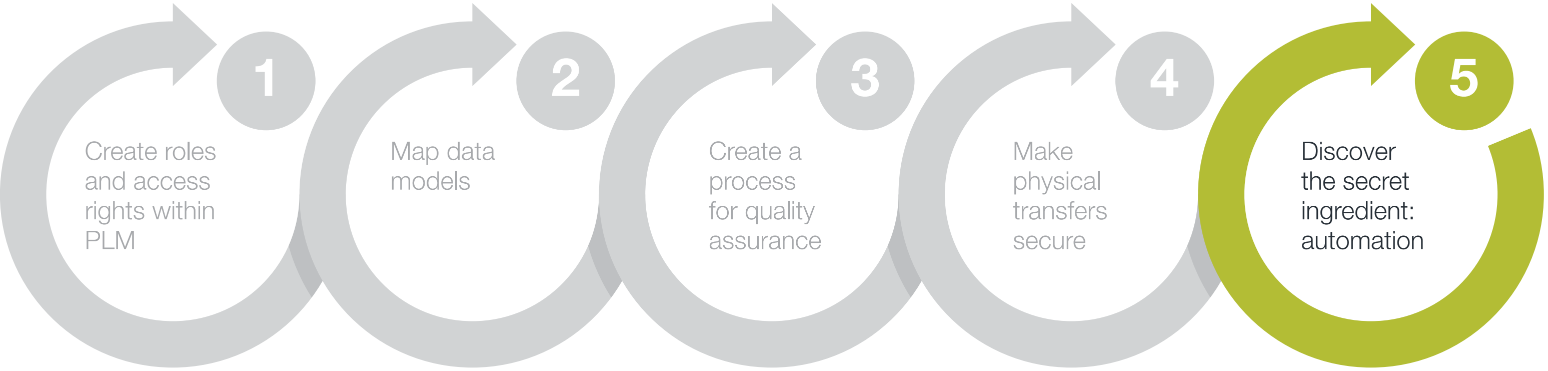
Physically transferring IP files is the most visible part of the security policy, and one of the more critical steps to get right. Standardize how your company processes and exchanges product design data with partners across all projects by configuring your system to automatically make decisions for the user. In addition, eliminate any high-risk delivery processes such as email, FTP, and B2C cloud file sharing services. Ensure your standard process includes the appropriate level of data encryption, such as public/private key encryption for person-to-person needs.

Don’t forget to consider a secure process for receiving and storing data files, as well as sending them. Secure data sharing is only half of the equation; you also need the ability to import and house product design data securely. This is one of the most challenging aspects of keeping a secure data exchange process in place.


1
Create roles and access rights within PLM
2
Map data models
3
Create a process for quality assurance
4
Make physical transfers secure
5
Discover the secret ingredient: automation

5 Discover the secret ingredient: automation

By now you've probably noticed that automation is a common theme across many of these steps—with good reason. The most impactful step you can take to minimize security risk in your PDX process is to automate as much as possible. Human error is the number-one threat to IP security for any company; minimizing human interaction with the PDX process will make it more secure. Automation is an inherently secure option precisely because it limits the chance for human error.


1
Create roles and access rights within PLM
2
Map data models
3
Create a process for quality assurance
4
Make physical transfers secure
5
Discover the secret ingredient: automation

How to create a secure product data exchange process ***with Siemens Teamcenter and Rocket Software***

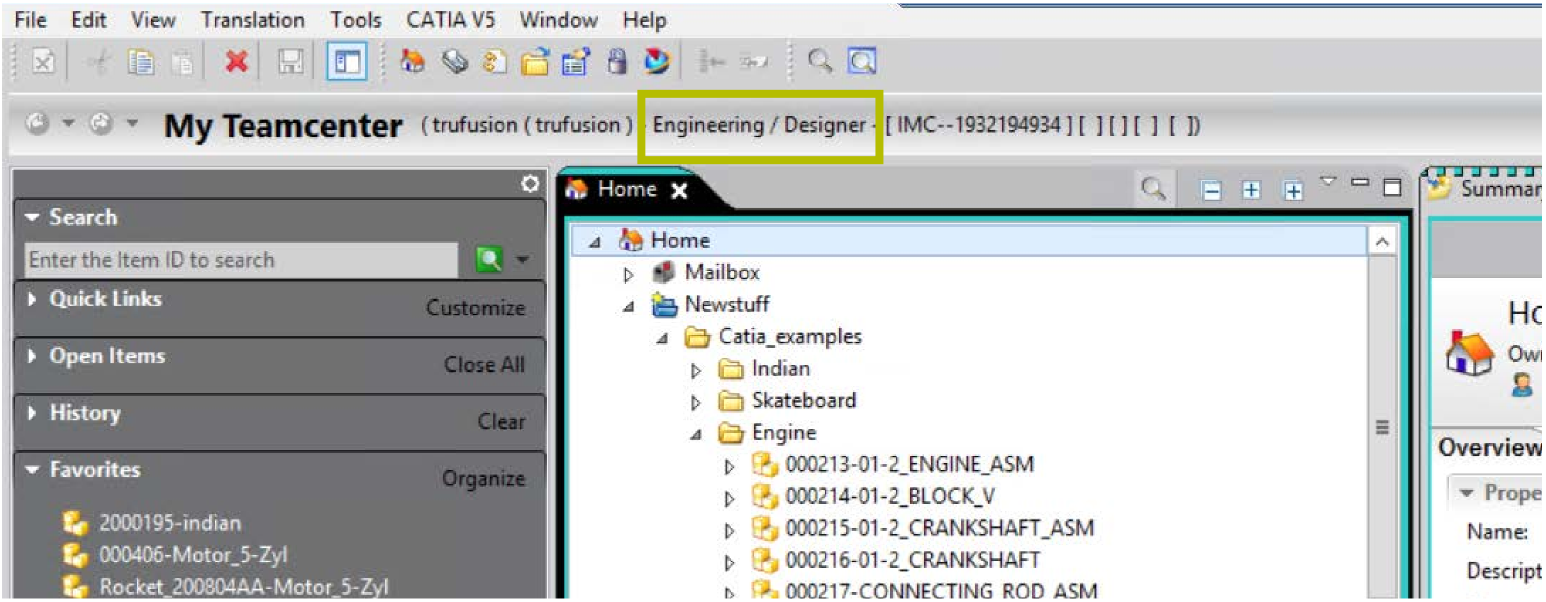
Rocket® TRUfusion™ Enterprise is a comprehensive, secure product data exchange solution that helps Teamcenter customers worldwide exchange product design data and other IP with supply chain partners as well as internal remote manufacturing sites. TRUfusion Enterprise customers minimize the inherent risks of sharing design data by replacing disconnected, manual data exchange tasks with automated processes built to run directly in Teamcenter. Automating with TRUfusion saves potentially thousands of hours annually for engineers—administrative time that can be redirected towards more valuable tasks that support business objectives.

The following pages demonstrate how combining Rocket TRUfusion Enterprise with Teamcenter together can help you address each of the five recommendations introduced above.

1 Create roles and access rights within PLM

You can configure your TRUfusion Enterprise integration with Teamcenter to consider the security models in Teamcenter, and only allow users to select the appropriate files when communicating with supply chain partners.

We recommend including role creations and filters when initially deploying Teamcenter or adding new projects to your Teamcenter implementation. Your administrator or implementation consultant can easily add the roles to your Teamcenter instance. Groups, Roles, and Users can be created within the Organization section of Teamcenter, one being a subset of the other. For example, if User1 is assigned the role of “Product Manager A” and the “Product Manager A” role is part of the “Customer A” Group, then User1 should inherit all the access capabilities within the Product Manager Customer A Role, and so on.

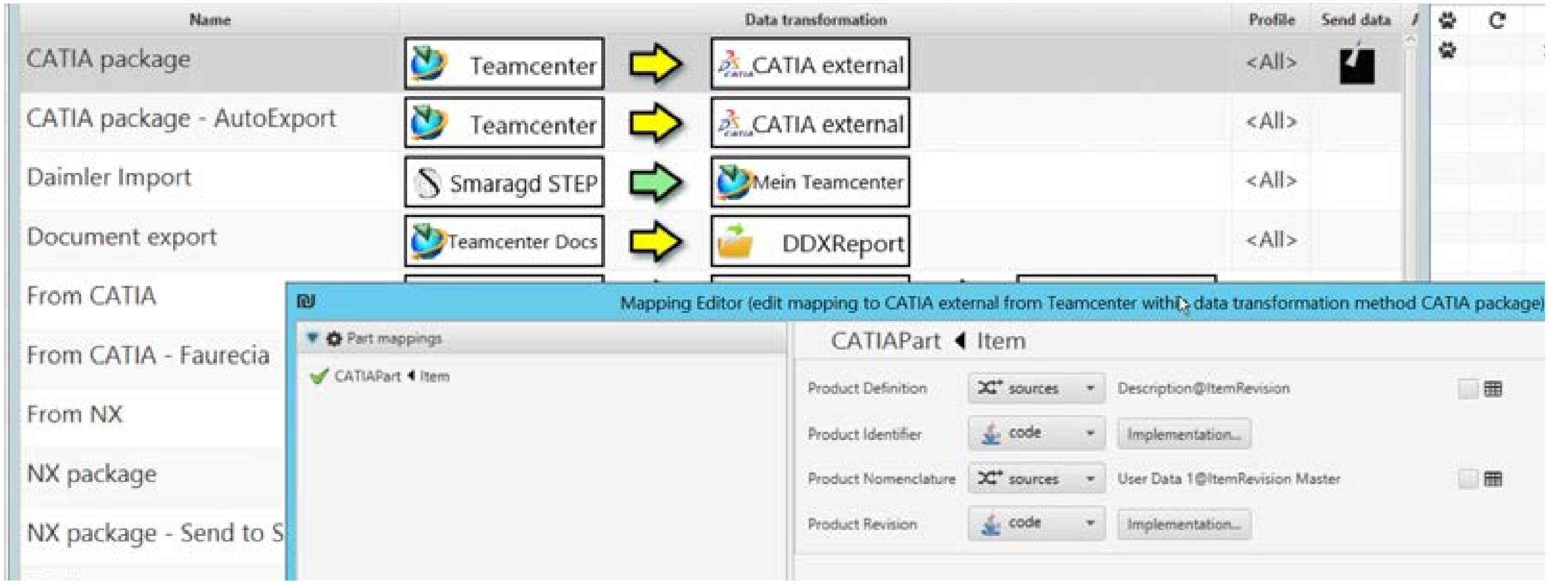


My Teamcenter (trufusion (trufusion) Engineering / Designer [IMC--1932194934] [ ] [] [ ] [ ])

When roles are set up in Teamcenter, they are clearly visible within the program

2 Map data models within Teamcenter

You can set up the Teamcenter integration to map data attributes and packages between your Teamcenter data model and the OEM or partner's data model for both sending and receiving data. This is a more technical step and requires writing scripts to map attributes and other product data from one program to another.



Name	Data transformation	Profile	Send data
CATIA package	Teamcenter → CATIA external	<All>	
CATIA package - AutoExport	Teamcenter → CATIA external	<All>	
Daimler Import	Smaragd STEP → Mein Teamcenter	<All>	
Document export	Teamcenter Docs → DDXReport	<All>	
From CATIA			
From CATIA - Faurecia			
From NX			
NX package			
NX package - Send to S			

Mapping Editor (edit mapping to CATIA external from Teamcenter within data transformation method CATIA package)

Part mappings

✓ CATIAPart ◀ Item

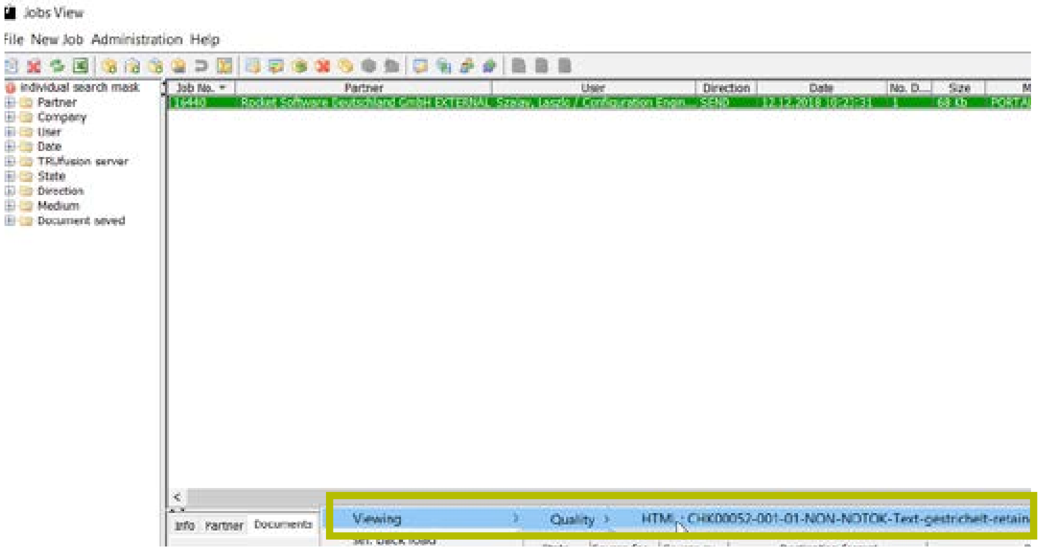
CATIAPart ◀ Item

Product Definition	sources	Description@ItemRevision
Product Identifier	code	Implementation...
Product Nomenclature	sources	User Data 1@ItemRevision Master
Product Revision	code	Implementation...

Mapping between internal models and OEM or partner models for exchanging data is easy

3 Create a process for quality assurance

Consider using additional CAD quality assurance tools to prevent any security oversights, and to comply with you and your partner's CAD/CAM quality standards and naming requirements. TRUfusion Enterprise provides integrations with Q-Checker (for CATIA V5) and HQM (for NX) to run checks as part of the usual data exchange workflow. For each job, the integration will set the correct environment (CAD version, Q-Checker-/HQM-version, check profile) to run Q-Checker/HQM in batch mode and provide results through the TRUfusion Enterprise interface if it needs to be reviewed. If everything looks OK, the job is further processed and completed; if an error or alert occurs, the job is halted so the CAD data can be corrected and re-submitted.



Jobs View

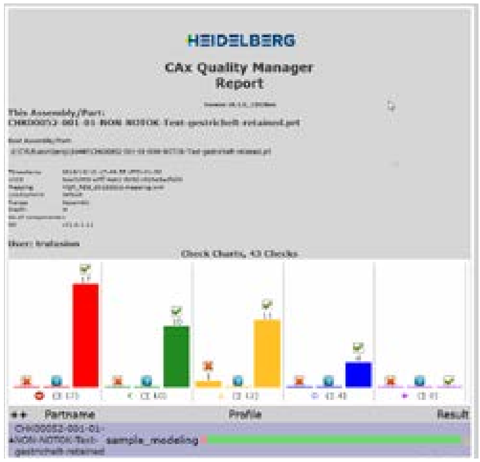
File New Job Administration Help

Individual search mask
- Partner
- Company
- User
- Date
- TRUfusion server
- State
- Direction
- Medium
- Document saved

Job No.	Partner	User	Direction	Date	No. D...	Size	M
16440	Rockit Software Deutschland GmbH EXTERNAL	Szalay, Laszlo / Configuration Engin...	SEND	12.12.2018 10:21:31	1	68 Kb	PORTAL

CHK00052-001-01-NON-NOTOK-Text-gestrichelt-retain

Access CAD QA tools directly within TRUfusion Enterprise



HEIDELBERG

CAx Quality Manager Report

This Assembly/Part:
CHK00052-001-01-NON-NOTOK-Text-gestrichelt-retained.prt

Check Charts, 43 Checks

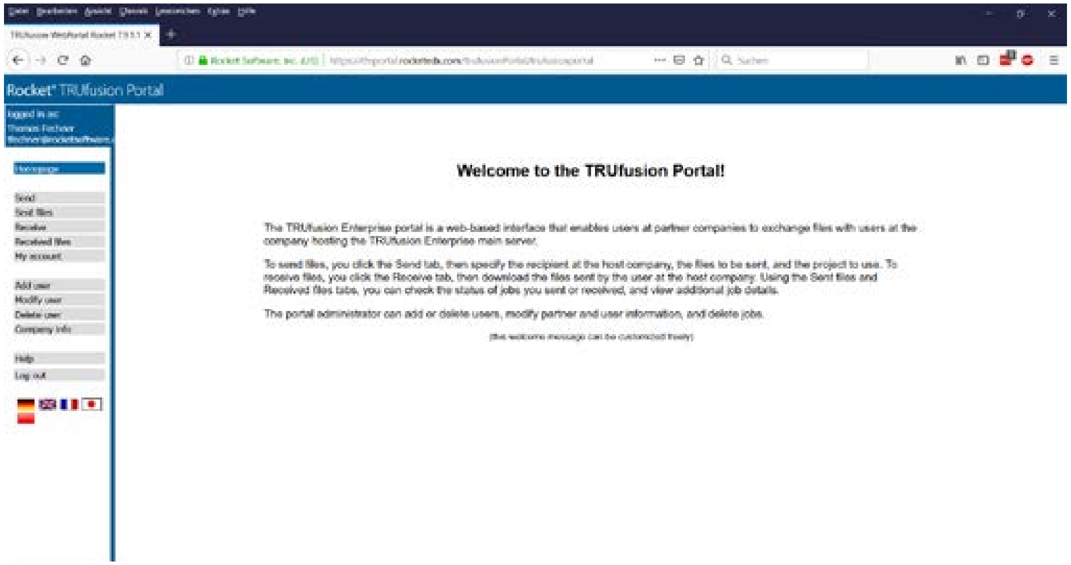
Partname	Profile	Result
CHK00052-001-01-NON-NOTOK-Text-gestrichelt-retained	sample_modeling	

CAD QA tool reporting example

4 Make physical transfers secure

TRUfusion Enterprise is configured to handle your selected data types, the data processing steps for them, and the packaging and delivery required. Both you and the partner can use the data as needed once it's received. We offer multiple solutions that work in tandem with TRUfusion for secure physical file transfer:

- Odette File Transfer Protocol (OFTP2) across the internet via Rocket Eurex-c
- A web portal, via the Rocket TRUfusion Enterprise Portal
- A SaaS file exchange solution, Rocket TRUexchange



Welcome to the TRUfusion Portal!

The TRUfusion Enterprise portal is a web-based interface that enables users at partner companies to exchange files with users at the company hosting the TRUfusion Enterprise main server.

To send files, you click the Send tab, then specify the recipient at the host company, the files to be sent, and the project to use. To receive files, you click the Receive tab, then download the files sent by the user at the host company. Using the Sent files and Received files tabs, you can check the status of jobs you sent or received, and view additional job details.

The portal administrator can add or delete users, modify partner and user information, and delete jobs.

(this welcome message can be customized freely)

The TRUfusion Portal is a secure way to receive and send CAD and other data to partners and remote site workers

5 Discover the secret ingredient: automation

Automation is at the core of TRUfusion Enterprise, letting you automate the entire data exchange process between Teamcenter and the partner, including:

- Import/export into Teamcenter
- Mapping attributes and naming conventions between CAD and PLM systems to convert between different data models
- CAD quality checks
- Conversion to/from neutral formats (e.g. STEP, IGES, 3DPDF, JT)
- Conversion between native CAD file formats from the leading vendors (e.g. CATIA V5 to NX), using embedded 3rd-party translators
- Format-specific packaging
- Secure file transfer
- Email notifications
- Documentation of the full audit trail
- Archiving

Secure product data exchange with Rocket

Following these steps will help keep you competitive in the marketplace, letting you respond promptly to RFQs and turn critical projects around quickly. And, of course, you'll save your engineers hours of time per project.

With TRUfusion Enterprise, you can be confident that your team will be able to exchange data with partners quickly and easily, follow consistent processes, minimize errors, and keep product design data safe.

Request a TRUfusion demo >

Rocket®

rocketsoftware.com
info@rocketsoftware.com
US: 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

2019-02 EB 5 Steps to Secure PDX Teamcenter V5