Solving PLM Security Concerns Using Teamcenter

Sassan Khoubyari
Chief Program Manager
Global Powertrain C3PNG Methods & Deployment
Ford Motor Company
skhoubya@ford.com
www.ford.com

Suresh Somisetty
C3PNG PIM Security Specialist
Mechatronics Inc.
ssomiset@ford.com
www.mechatronics-us.com
### Evolution of the Ford Product Creation Process

<table>
<thead>
<tr>
<th>Year</th>
<th>Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1985</td>
<td>CTC</td>
<td>Concept to Customer</td>
</tr>
<tr>
<td>1992</td>
<td>WCT</td>
<td>World Class Timing</td>
</tr>
<tr>
<td>1993</td>
<td>WCP</td>
<td>World Class Process</td>
</tr>
<tr>
<td>1996</td>
<td>FPDS</td>
<td>Ford Product Development System</td>
</tr>
<tr>
<td>2005+</td>
<td>GPDS</td>
<td>Global Product Development System</td>
</tr>
</tbody>
</table>

- **MBJ#1**
  - 72 MBJ#1 (1985)
  - 68 MBJ#1 (1992)
  - 65 MBJ#1 (1993)
  - 43 MBJ #1 (1996+)

* <KO> equivalent timing for S4/P4 program

---

*PLM World ‘06*
Key Business Drivers – Commonality (Before C3PNG)

**Requirements:**
- Common PDM
- Common Product Structure
- Common CAD

**Current Situation:**
- Different PDM
- Different Product Structure
- Different CAD

Manual Processes and Resources

Our current Methods/Tools/Data environment inhibits cross brand programs
C3P-Next Generation (Ford PLM Initiative)

CATIA V5 (excluding PT), IDEAS, Teamcenter Engineering (TCe) & Teamcenter Manufacturing (TCm), AVBOM, Vismock, Tecnomatics, etc.

- **Security** is probably one of the most important issues during migration from C3P Classic (Metaphase/TDM) to C3P Next Generation.
- The real challenge was to customize the TCe security module to comply with the Ford Motor Company’s C3P Security policy.
- Users acceptance to the changes is always a challenge.
When FMC Powertrain decides to be part of the single/shared data management tool (C3P-NG), there were many concerns/requirements from users about the security

**Over exposure of data to many users**
- Many groups need to use/share same database for their daily work
- Work In Progress data of any user gets exposed to beyond his/her group
- Proper Naming & Numbering is must from beginning

**Multiple Roles & Responsibilities**
- Demand for following types of Roles
  - Engineer, Designer, Team Designer, Viewer, CAE Analyst, Data Admin, Plant Engineer, etc…
Challenges

Restricting access to highly “Secret” data only for authorized users

• Any data that is classified as highly ‘Secret” should be protected from unauthorized users including FMC users
  Example:
  • Tooling data
  • Research & Advanced Engineering data

Restricting write privileges on data to only few set of users or group of users

• A demand for clear definition of who should have write access & Who should have read access

• Limiting Data Admin roles
Challenges

Restricting Suppliers to only data that they are supposed to view/work

• Supplier users should have access to the data only on need basis
• Protecting competitive suppliers data from each other
• Availability of required data to suppliers with no delay

A secured place for Joint Ventures to store & collaborate their work

• Ford Joint Ventures usually work with many OEMs
• Provision to store Ford & Non Ford data in a single database & provide access to Ford users only for their data
• Secret data should be protected from access by non-JV personnel
• A provision to store/organise Catalog Parts & restrict access to only JV users
Security in Legacy Environment

- Legacy environment (FMC calls it as C3P Classic) provides two step/level data management.
- In first level, a group of users manage their working data in the localized Team Data Manager i.e IDEAS TDM. Users feel their data is secured here by limiting access to only TDM users.
Security in Legacy Environment cont…

- Users share/send the data to second level of data management (Metaphase) only on need basis & users are comfortable to share their data since data reached certain maturity.

- Legacy approach gave users to work in their domain without exposing the work in progress data to other downstream users in the organization and only share data that is mature enough. This provides indirect security to Work In Progress data.

- Ford Joint Venture companies are able to work with this model and keep data secured as required.
Following diagram shows how Ford JVs operate in C3P Classic environment.

Metaphase (PTO- Merk)

Ford Data TDM’s
(operated by Ford IT)

Non Ford Data TDM’s
(operated by Ford IT)

Secured Network Nodes
(accessible only through JV subnet)

JV Data Coordinator

Supplier Agencies

FDX Odette
When FMC Powertrain started thinking about the C3P Next generation tools, following were major requirements:

- Business operations approach has changed and now OEMs are spawned across the globe.
- Several groups in the organization doing similar type of job and faster to market approach.
- Demanding re-usability of company product data as much as possible to reduce cycle time.

PLM tools seem to be providing better solutions to today's OEMs security needs but needs reasonable amount of customization.
C3P-NG Security – Key Concepts

Security module for C3P NG is built/configured in compliance with the FMC CAD/CAM/CAE/PIM Security Policy

Following are the few key PLM Security concepts implemented as part of C3P-NG.

- **Groups**
  - Ford
  - Supplier

- **Data Classification**
  - Secret
  - Confidential
  - Proprietary

- **Project Based Security**
  - Create / Manage Projects on-the-fly
  - Only read access is controlled based on the Project

- **Restriction Lists**
  - To restrict competitive suppliers viewing each others data
C3P-NG Security – How does it work?

• For every Engine/Transmission family of programs, a project in TCe would be created.

  Ex: MODENG

• There are three sub-groups created for Powertrain users under each CBG.
C3P-NG Security – How does it work?

- Powertrain users could request a role in TCe for any specific project using a web based user access request system.
C3P-NG Security – How does it work?

- Powertrain users could request a role in TCe for any specific project using a web based user access request system. **Cont...**
C3P-NG Security – How does it work?

A snapshot of TCe My Navigator for user role, group & project

Notice that user got a Designer role under ENGINE group in FNA for ‘MODENG’ project
Every project in TCe gets an associated product structure to store the data.
C3P-NG Security – How does it work?

- Apply Security Data Classification

The purpose of the Data Classification is to apply a value to the Item that denotes its Security Classification based on Ford's Global Information Standard 2 (GIS2). This Security Classification is used to control viewing privileges on the data.

![Diagram of C3P-NG Security](image-url)
C3P-NG Security – How does it work?

View access to the data is decided based on it’s association to a Project

TCe Projects are an OOTB concept that allows for the assignment of Users and Data Objects to a Project or Projects. By comparing the User and Data Object assignments, Project based security controls view access to Data objects.

View access Privileges

<table>
<thead>
<tr>
<th>User Type</th>
<th>Data Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secret</td>
</tr>
<tr>
<td>Ford</td>
<td>P</td>
</tr>
<tr>
<td>Supplier</td>
<td>P</td>
</tr>
</tbody>
</table>

View Access Key:

A = Across all Programs/Projects
P = Per Program/Project
C3P-NG Security – How does it work?

- Applying Restriction List (if necessary)

A Restriction List is applied to a TCe object so that the object is not viewable by Suppliers on the restriction list. Although any user may request a restriction list for their data, only a Data Admin may approve and implement the restriction. Once imposed, only a DBA may remove a restriction list. Another thing to notice here is that the user can request a Restriction List only for those objects owned by him/her.

Choose who should not see the data
Case Studies

1) Protecting Highly Secret Data
2) Program Based Data Management
3) Competitive suppliers working on same Project
Problem: Casting & Forging Engineering (CFE) Team needs a secure place/environment in TCe to store their concepts & tooling suppliers data.

Business drivers:
- Only authorized Ford Motor Company employees should have access to CFE data
- All Casting & Forging suppliers and Joint Ventures should interact with TCe through a data coordinator
- CFE data access will be granted on a proven business case

Challenges:
- Required security is much granular than as defined in the FMC C3P Security Policy
- Highly secured data is sharing Product structure with other data
- A completely new scenario….different from rest of the majority of Ford Internal groups
Case Study 1 --- Protecting Highly Secret data

Solution to store highly secured data in TCe

Create PTO specific secure group

Assign Users to secure group

Create Data in secure group

Transfer WIP data to non-secure group

Manage Project and Data Classification

Restriction List for suppliers

Isolated group with data only accessible to members of the group

Standard UARS request process

All data created by members is automatically owned by the group

Many idiosyncrasies in transfer process from secure to non-secure group

Once transferred to non-secure group normal TCe viewing behavior exists

Where required, use Restriction lists to block Supplier access

- Pros:
  - Maintains extremely tight control of data within Secure group

- Cons:
  - There is no cross-group access to data, including other secure groups within the PTO discipline
    - Cross group access could be created, but would be a permanent condition. PTO would not have access to grant or revoke this access “on the fly”.
    - Any change to the original set-up between secure groups would require a CR with an extended timeline for deployment of the change.
  - Once an Item Revision is transferred to a non-secure group and frozen, it is not possible to restrict it again.
  - This set-up violates the current corporate security policy and a change to the policy would require Engineering Director approval from all functional areas.
Case Study 2 --- Program based data management

Problem: Program based data management to support Powertrain Program life cycle

Business drivers:
Powertrain needs top level program nodes for all engine/transmission families/programs in TCE. This enables Powertrain to develop Powertrain commodities based on the P/T product development process. Furthermore, this allows Powertrain to operate multiple engine/transmission programs under top level program nodes and provide data to vehicle programs as needed.

Solution:
Creation of a Project for each engine/transmission program family and Utilize project based security concept that exists in TCE
Restricting competitive suppliers working on same project viewing from each others data

**Business drivers:**
FMC agreements with Suppliers prohibit to share competitive suppliers data with each other

Supplier’s are working on different data for the same Powertrain program
FMC is making use of Access Control List (ACL) or Restriction List concept available in TCe
FMC is making use of Access Control List (ACL) or Restriction List concept available in TCe.