Sichere Datenaustauschprozesse in der Automobilindustrie durch methodischen Know-how-Schutz
Secure Data Exchange Processes in automotive Industry by methodical Know How Protection

Herausforderung globaler Entwicklungskooperationen, Methoden und Lösungen für prozesssichere Datenaustauschplattformen
Challenge by global development collaboration, Methods and Solutions for secure Data Exchange Platforms

Dipl.-Ing. Dr. techn. **Josip Stjepandic**, Darmstadt;
Dr.-Ing. **Harald Liese,** Darmstadt;

Kurzfassung

Im Zeitalter der Globalisierung wird der Austausch der produktdefinierenden Daten zwischen den beteiligten Parteien in der Wertschöpfungskette eine selbstverständliche Form der Geschäftskommunikation. Durch die hohe Komplexität der Datenaustauschprozesse ergibt sich eine hohe Wahrscheinlichkeit zum unerlaubten Zugriff Fremder auf das besonders schützenwerte Know-how. Im vorliegenden Beitrag ist der methodische Ansatz zur Gestaltung sicherer Datenaustauschprozesse beschrieben.

Abstract

In the era of globalization, the exchange of product defining data between the participating parties becomes a self-evident form of business communication within the value creation chain. The high complexity of the data exchange processes promotes a high chance for illegal access on the particularly valuable know how by foreign parties. The article at hand describes the systematic approach to the creation of secure data exchange processes.

1. Ausgangssituation

Es vergeht kaum eine Woche, ohne dass die Meldungen über die unterschiedlichsten Formen der Verletzung des geistigen Eigentums, der Produktpiraterie, des Plagiarismus, der Fälschungen und des Diebstahls sensibler Daten veröffentlicht werden. Die Opfer dieser neuen Form der internationalen Kriminalität sind sowohl die global agierenden Unternehmen wie Daimler [1] oder MAN [2], als auch die kleinen und mittelständischen, der breiten Öffentlichkeit kaum bekannten Unternehmen [3]. Der deutsche Zoll, eine seit der Umsetzung

des Schengener Abkommens für die typischen Bürger kaum sichtbare Behörde, tritt vor nahezu jeder internationalen Messe durch Fahndungserfolge nach Plagiaten und Fälschungen auch für die breite Öffentlichkeit wahrnehmbar in Erscheinung. Der Umfang und die Häufigkeit der Verletzungen des geistigen Eigentums sowie die zu erwartenden Verluste motivierten den VDMA (Verband Deutscher Maschinen- und Anlagenbau e.V.), einen der führenden Industrieverbände, die Kampagne “Pro Original” [4] zu etablieren, um die potentiellen Kunden davon zu überzeugen, das Originalprodukt statt des Plagiats oder der Fälschung zu kaufen. Diese Kampagne konnte allerdings bislang keine Maßnahme empfehlen, wie die Verletzungen des geistigen Eigentums und Verbreitung der Fälschungen vereitelt werden können. Die einschlägigen Untersuchungen [5] brachten zum Teil erschütternde Fakten. So betrug der Gesamtschaden bei dem untersuchten Unternehmen 11,4 % des Jahresumsatzes (Bild 1).

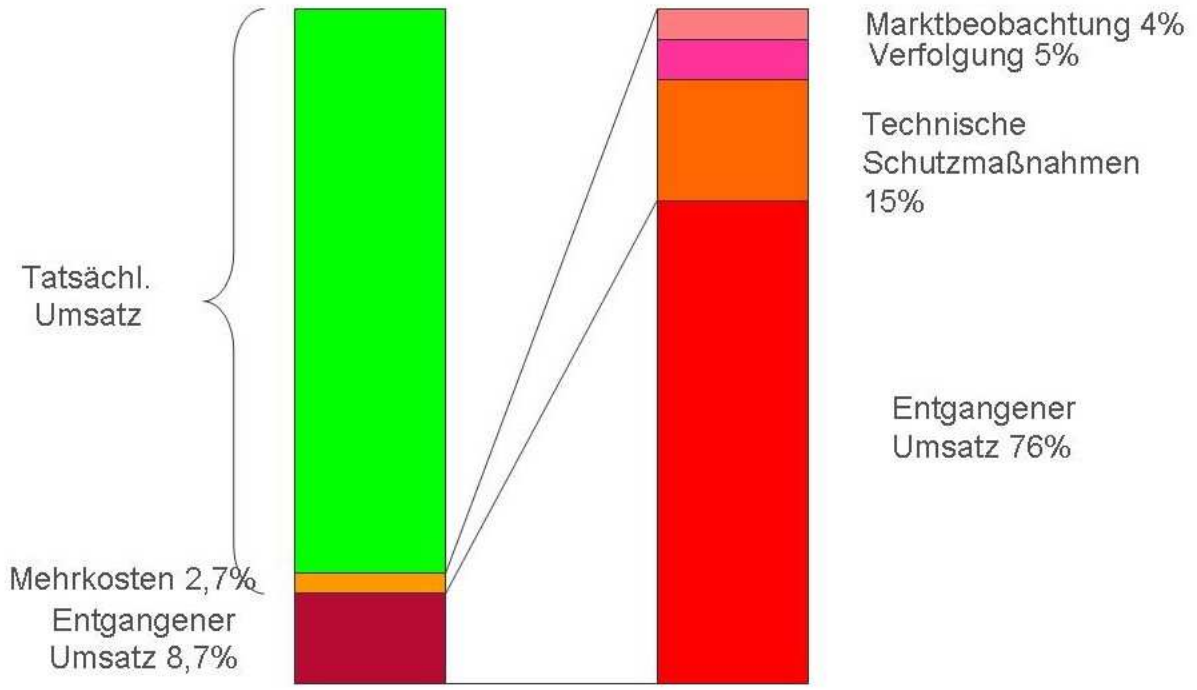

Bild 1: Betriebswirtschaftliche Schäden durch Produktpiraterie [5]

Ferner beziffert jedes dritte vom VDMA befragte Unternehmen die Umsatzeinbuße durch Produktpiraterie mit höher als 5%. Der jährliche volkswirtschaftliche Gesamtschaden durch Plagiate wird von der gleichen Quelle mit bis zu 660 Mrd. Euro geschätzt.

Besonders hervorzuheben sind die langfristigen Folgen der Produktpiraterie durch den unerwünschten und den ungesteuerten Know-how-Transfer, wodurch das in den Produkten

enthaltene Produkt- und Prozesswissen nicht mehr einzigartig ist. Der Wettbewerbsvorsprung eines Herstellers der Original-Produkte geht verloren oder kehrt sich sogar in einen Wettbewerbsrückstand um, weil der Nachahmer alleine durch die nicht getätigten Entwicklungsaufwände einen erheblichen Kostenvorteil erlangt. Daher stellt sich die Produktpiraterie als eine ernst zu nehmende Bedrohung speziell für die Marktführer dar.
Die Komplexität der Herausforderung und die vielfältigen Ausprägungen der praktischen Verletzungen des geistigen Eigentums lassen es sehr ratsam erscheinen, den Pirateriesschutz als Unternehmensaufgabe auf die gesamte Wertschöpfungskette auszuweiten mit dem Ziel, einen ungewollten Know-how-Transfer prozesssicher zu vermeiden. So betrachtete Aberdeen Group 88 Unternehmen aus verschiedenen Branchen [6], um zu bestimmen, wie die führenden Organisationen mit den Sicherheitsrisiken bei der IT umgehen. Nur die jeweils besten Unternehmen in ihrer Kategorie berichteten über die Abnahme der sicherheitsrelevanten Vorfälle.

2. Problemstellung

Diese äußerst unangenehme Ausgangssituation stellt die Markt führenden Automobilhersteller und deren Zulieferer speziell in Deutschland vor erhebliche Risiken und Herausforderungen. Hierbei sind zwei Aspekte von besonderer Bedeutung. Einerseits werden die Entwicklungsprozesse getrieben durch den immensen Rationalisierungsdruck auch unter Nutzung moderner Informations- und Kommunikationstechnologien immer weiter optimiert. Als sehr effizientes Rationalisierungsmittel hat sich mittlerweile die CAD-orientierte Wissensrepräsentation erwiesen [7] [8]. Hierbei werden komplexe Entwicklungsaufgaben (Bauteilerstellung, Integration von Gestaltung und Berechnung, Validierung, Prozesskettenkopplung) mit Hilfe von Methoden und Technologien des Knowledge-based Engineering (z.B. mittels Intelligenter Templates) im hohen Maße automatisiert und hohe Aufwands- und Durchlaufzeitersparnisse erzielt. Die Strukturierung der CAD-Methoden ist im Bild 2 dargestellt.

Auch wenn man sich dadurch dem idealen Entwicklungswerkzeug immer mehr nähert, bei dem die Produktgestalt und das Produktwissen sozusagen vereint werden, ist diese Errungenschaft mit erhöhten Risiken verbunden. Denn mit dem Zugriff auf solche CAD-Modelle erlangt man ebenfalls den Zugriff auf das Produktwissen. Im schlimmsten Fall würde der Verlust oder eine unbeabsichtigte Verteilung von CAD-Modellen bedeuten, dass das Produktwissen quasi öffentlich würde. Diesen Zustand würde sich kein Unternehmen leisten können. Nicht nur deswegen werden die CAD-Daten heutzutage durch leistungsfähige PDM-

Systeme verwaltet, die eine fein gegliederte Steuerung der Zugriffsrechte auf die Produktdaten ermöglichen.

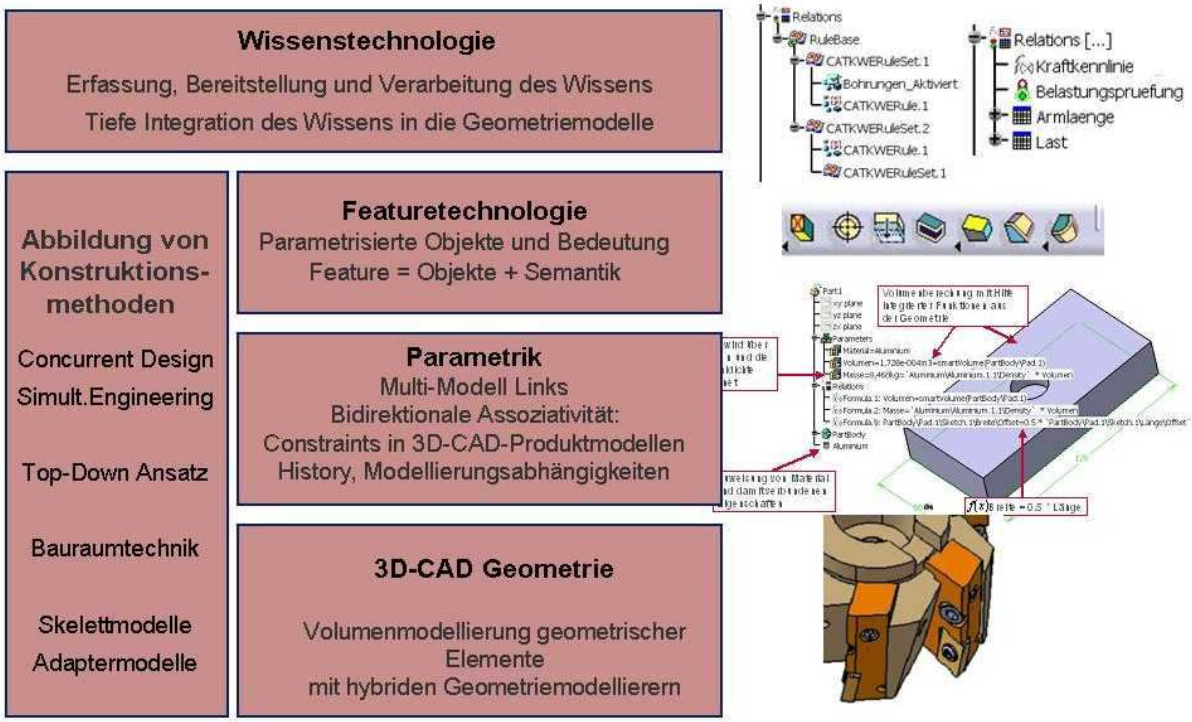

Bild 2: Wissensrepräsentation in 3D-CAD [8]

Andererseits haben die Automobilhersteller ihre eigene Wertschöpfungstiefe erheblich reduziert und beschäftigen tausende von Zulieferern und Dienstleistern in ihrer Zulieferpyramide, die sich bei den meisten OEM über die ganze Welt erstreckt. Durch die zunehmende Komplexität des Endproduktes Automobil, Verkürzung der Entwicklungszyklen, zunehmende Globalisierung der Wertschöpfungskette liegt es nahe, dass die produktdefinierenden Daten – vor allem die CAD-Modelle - praktisch um die ganze Welt in beide Richtungen (vom OEM zu den Zulieferern und umgekehrt) fließen. Auch wenn die generelle Regel Bestand hat, wonach der OEM die Prozesse und Methoden für die ganze Lieferkette vorschreibt, lässt sich diese nicht überall lückenlos umsetzen. Dies trifft insbesondere dort zu, wo sich die Zuliefererpyramiden überschneiden.

Die Integrationstiefe einzelner Zulieferer hängt stark von deren Kooperationsmodellen und der Position in der Lieferkette ab (Bild 3).
Vereinfacht gesagt müssen sämtliche Methoden und Lösungen der harten Prüfung unter den vielfältigen Praxisbedingungen in einer Lieferkette Stand halten.

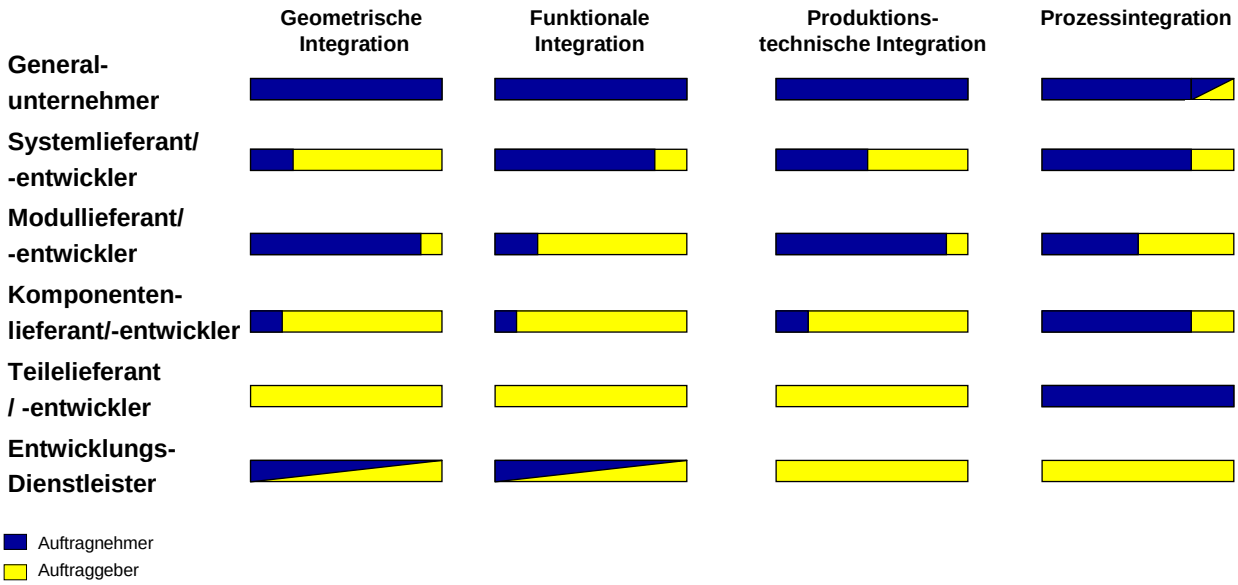

Bild 3: Gliederung der Kooperationsmodelle [9]

Als sehr vorteilhaft für die methodische Weiterentwicklung hat sich die Position mancher OEMs erwiesen, die erkannt haben, dass deren Zulieferer einen offenkundigen Bedarf haben, ihr in den CAD-Modellen gespeichertes Wissen durch geeignete Maßnahmen – auch ihrem OEM gegenüber - zu schützen [10].

3. Handlungsfelder

Wenn man bedenkt, dass die Zulieferer abhängig vom Kunden und einem bestimmten Fahrzeugprojekt unterschiedliche Rollen einnehmen können, ergeben sich drei methodische Handlungsfelder, um das Produkt-Know-how während der Entwicklung zu schützen.

Zunächst ist es notwendig, auf der bilateralen Dokumentebene (d.h. bei den CAD-Modellen) das darin enthaltene Produktwissen situationsbedingt zu verschatten oder zu entfernen. Das Knowhow, das vor dem Datenversand entfernt wurde, kann später nicht missbräuchlich verwendet werden.

Im Rahmen des globalen Datenaustausches bedarf es einer Datenaustauschplattform, die einen sicheren Datenaustausch von Massendaten mit hoher Austauschfrequenz über das Web gewährleistet.

Schließlich sind überall dort, wo sich mehrere Zulieferpyramiden durchschneiden (und dies ist in der Automobilindustrie der Regelfall), einheitliche Prozesse erstrebenswert, die selbstverständlich auch den Knowhow-Schutz einschließen.

In einer aktuellen Studie [11] des ProSTEP iViP e.V. wurden die technischen Ansätze zum Knowhow-Schutz folgendermaßen gegliedert (Bild 4).

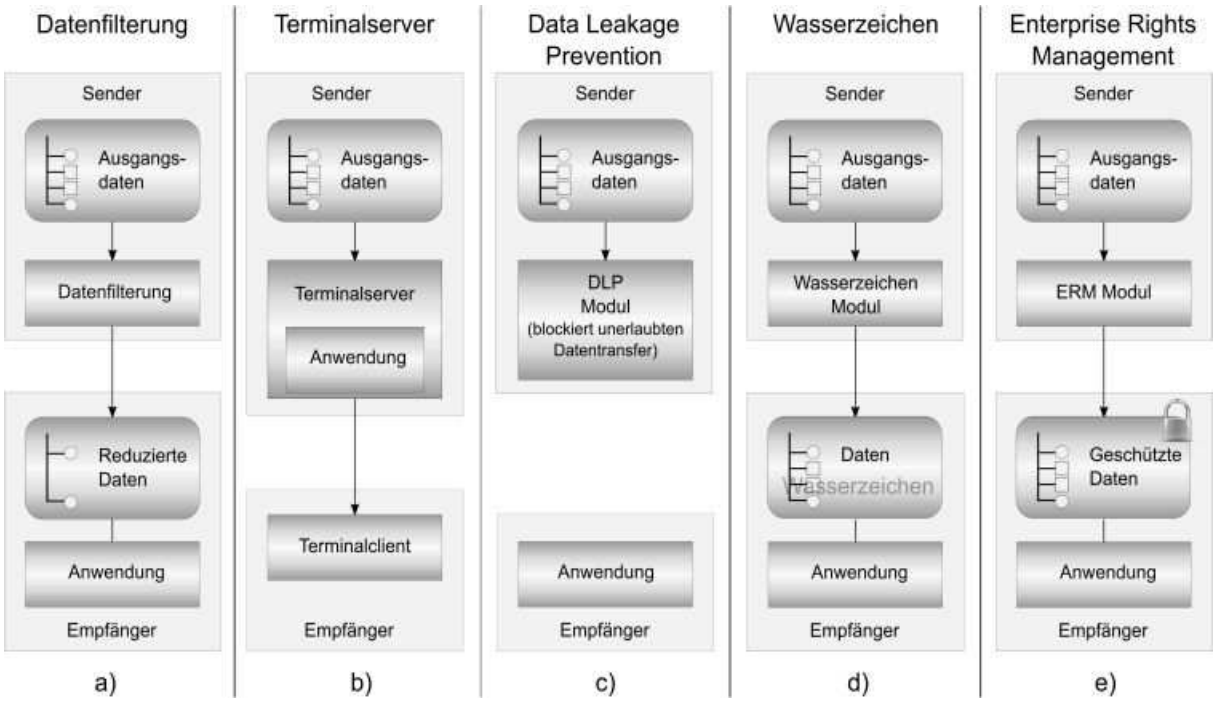

Bild 4: Technische Ansätze zum Know-how-Schutz [11]

4. CAD-Modell orientierter Knowhow-Schutz

Hierbei erfolgt der Know-how-Schutz durch den unmittelbaren Zugriff bzw. Eingriff auf die CAD-Daten. In aller Regel wird eine Austauschkopie des Originals erstellt und weiter so adaptiert, dass die Schutz würdigen Inhalte nicht mehr erkennbar sind. Für die Umsetzung des Know-How Schutzes (bzw. Intellectual Property Protection) sind generell die folgenden Funktionen von Bedeutung: Modellanalyse (die die Schutz würdigen Inhalte darstellt), Löschen und Verschatten von Wissenselementen (z.B. gesteuert durch Filter und idealerweise regelbasiert) und das Wiederanhängen von Wissen nach einem Datenaustauschzyklus.

Die Hauptfunktion der IPP-Software Knowledge Editor ist das Herausfiltern von Firmen-Know-how aus CAD-Modellen. Das Herausfiltern ist technologisch ein sehr komplexer Prozess, da das Wissen um einen definierten Umfang reduziert werden muss. Trotzdem müssen nach der Filterung die hohen Ansprüche der Partner bzgl. der vereinbarten CAD-Lieferumfänge und der CAD-Datenqualität erfüllt werden (Bild 5).

Der Knowledge Editor macht dieses Problem beherrschbar. Damit die Abläufe für den Endbenutzer einfach und verständlich anzuwenden sind, ist umfangreiches Prozess- und Entwicklungs-Know-How in die CAD-systemspezifischen Besonderheiten der Wissensverarbeitung in die Entwicklung des Knowledge Editors eingeflossen. Ein besonders hervorzuhebendes Merkmal des Knowledge Editor ist, dass die komplexen Vorgänge, die zur Filterung und Kommunikation mit dem CAD-System nötig sind, vor dem Anwender verborgen und in einer benutzerfreundlichen Oberfläche präsentiert werden. Schließlich sind die Anwender typischerweise Konstrukteure und keine IT-Experten aber das Wissen soll verlässlich und prozesssicher entfernt werden.

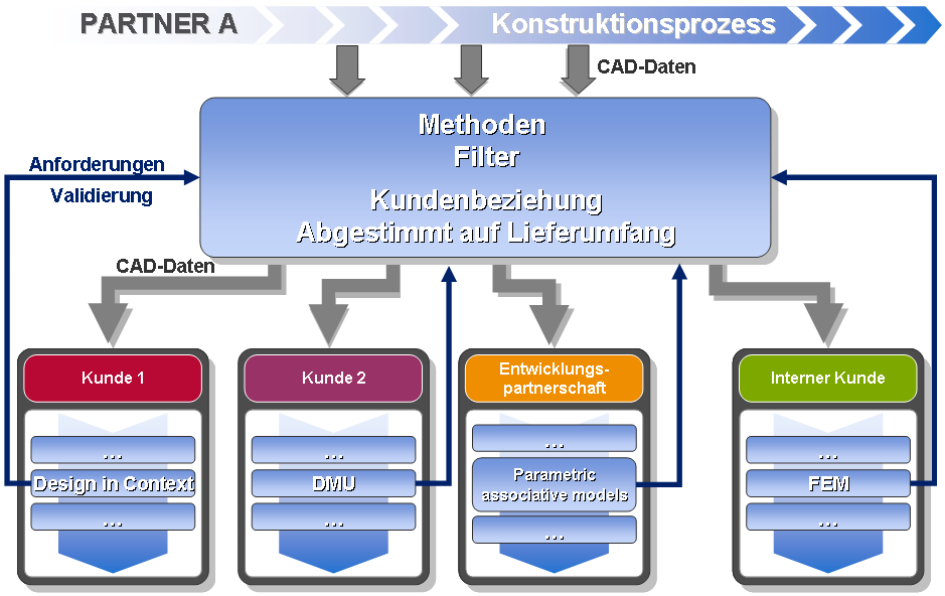

Bild 5: Prozesskettengetriebene Datenaufbereitung [12]

Die Software bietet umfangreiche IPP Funktionalitäten auf deren Basis dann weitere Funktionen aufgebaut werden können bzw. eine kundenspezifische Anpassung erfolgt.

Die Software kann aus der CAD-Oberfläche heraus gestartet werden und erscheint als zusätzliches Fenster. Mit ihm kann der Anwender zunächst seine Modelle analysieren. Als Ergebnis erhält er eine Liste oder Produktstruktursicht von Teilen und Baugruppen sowie die zugeordneten Wissenselemente bzw. Features. Nun kann er auswählen, welche Elemente oder Elementarten er als kritisch einstuft, kann sie markieren und löschen. Im Normalfall nutzt der Anwender allerdings die Analyse am Beispiel einer typischen Komponente, um generell festzulegen, welche Elemente, Geometrien und Attribute bei dieser Art von Produkt das Haus nie verlassen sollen. Dabei wird die Modellvereinfachung grob in

Strukturverschattung und Bauteilverschattung differenziert. Die folgenden Elemente können für CATIA V5 bereinigt werden: Erweiterte Parametrik (z.B. Parameter, Parameter Sets, Formeln und Konstruktionstabellen), Wissenselemente (z.B. Regeln, Prüfungen, Analyse- und Optimierungsfeatures, Aktionen, Reaktionen, Expertenregeln), Modellelemente (z.B. Materialien, Fertigungstoleranzen (PMI), Meta-Daten, Messungen), Geometrielemente, Features und Branches, sowie Strukturelemente (Constraints, Publications). Auch spezielle Wissensträger, sog. Adaptermodelle oder Skelettmodelle können entfernt werden. Die Konsistenz der Linkstrukturen kann dabei gewährleistet werden. Auch Kinematikinformationen können verschattet werden. Umbenennungsfunktionen runden die Funktionalität ab. Komplexe Löschoperationen ermöglichen beispielweise die Erstellung einer automatisierten Methode, die sowohl den Inhalt der CAD Modelle filtert als auch die Produktstruktur anpasst. Mit dieser kombinierten Filteroperation können firmenspezifische und schützenswerte Konstruktionsmethoden wie ein Top-Down-Designansatz verschattet werden. Auch das Verschatten ganzer Geometrien in Bezug auf Inhalt und Historie ist möglich. Bild 6 verdeutlicht die wesentlichen methodischen und funktionalen Eigenschaften der Software. Die Speicherung der Bereinigungsvorschriften ist hoch konfigurierbar, da die meisten Zulieferer CAD-Modelle an eine Vielzahl von Kunden (z.B. Automobilhersteller) mit verschiedenen Anforderungen an die Bereinigung automatisch versenden wollen. Daher erfolgt das Speichern der Bereinigungsvorschriften in Profilen oder Regeln.

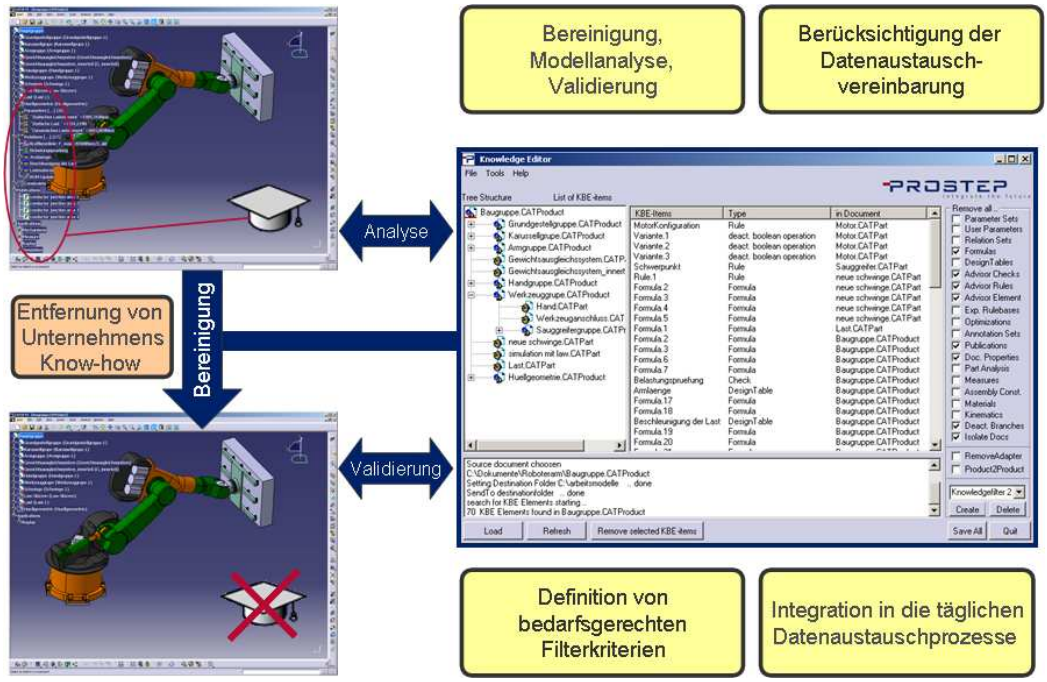

Bild 6: Knowledge Editor – Analyse, Modellbereinigung, Validierung [13]

Der Knowledge Editor ermöglicht eine regelbasierte Wissenslöschung. Diese ermöglicht die Definition hoch spezialisierter Bereinigungsregeln zur Kombination unterschiedlicher Löschoperationen und damit eine sehr detailliertere Filterung von CATIA V5 Daten. Eine stark differenzierte Behandlung der Elemente innerhalb einer Typklasse (z.B. anhand von Ausnahmeregeln) ist möglich. Somit lassen sich z.B. bestimmte Formeln in einem Template bewusst für den Datenempfänger erhalten, während andere Wissensinhalte komplett herausgefiltert werden.
Der Anwender definiert die Bereinigungsregeln mit einem sog. Rule Assistant, d.h. mit Unterstützung eines „Wizard"-Moduls. In einem Regelset können spezifische Aufbereitungen einfach zusammengefasst werden. Dabei ist von Vorteil, dass den Erstellern der Bereinigungsregeln das Denken in Regeln vertraut ist, da es sich meist um Ingenieure (z.B. CATIA key user) oder IT-Verantwortliche handelt.
Die regelbasierte Wissenslöschung für CATIA V5 Modelle ist sehr leistungsfähig. Dabei besteht eine Regel aus einem Filter und einer Aktion. Als Filter können logische Kombinationen von Kriterien abgebildet werden. Logische Verknüpfungsarten sind „and", „or" und „except", CATIA spezifische Kriterien können z.B. Featureart (Formel, Regel, Prüfung, etc.), Dokumentart (CATProduct, CATPart, CATDrawing) oder Identifier (Teilstring im Featurenamen) sein. Ein Beispiel für eine Regel die aus der Vielzahl der möglichen Filterkriterien und Löschaktionen definiert werden kann ist: „Lösche alle deaktivierten Prüfungen mit dem Bezeichner „*intern*" außer in CATParts".
Die Regeln werden in XML-Regelbasen (IPP Templates) gespeichert und werden dann vom Knowledge Editor verarbeitet. Diese führt die Bereinigungsregeln in der definierten Bearbeitungsreihenfolge aus. Die regelbasierte Wissenslöschung erhöht somit die Flexibilität und die Leistungsfähigkeit des Know-How Schutzes für den Datenaustausch mit dem Knowledge Editor.

Nach Definition der Bereinigungsvorschriften als Optionsdatei in Form von Profilen und/oder Regeln können diese dem automatischen Prozess zur Verfügung gestellt werden. Der Knowledge Editor wird dann jedes Mal als Batchprogramm aktiviert, das im Hintergrund abläuft, wenn ein entsprechendes CAD-Modell zum Kunden beziehungsweise Lieferanten übertragen wird. Somit wird auch im Batchbetrieb ermöglicht, aus einem Datensatz mit verschiedenen Optionsdateien unterschiedlich gefilterte Datensätze für verschiedene Empfänger automatisiert zu erzeugen. Die Modellqualität wird in der Software durch entsprechende Validierungsfunktionen für die Ergebnismodelle sichergestellt [13].

Um den Workflow der Batchverarbeitung zu steuern und den Know-How Schutz in den täglichen Datenaustausch zu integrieren, wird das Produkt OpenDXM® von PROSTEP eingesetzt, das auch als Front End zum Anwender dient (Bild 7). Somit ergibt sich ein durchgängiger Prozess [14], bei dem die Assistenz des Anwenders nicht notwendig ist. Seine Mitwirkung beschränkt sich auf das Auslösen des Datenaustauschprozesses und bedarfsweise Prüfen der Logfiles. Es ist auch möglich, auf Basis der Logfiles den Workflow individuell auf die Prozesse anzupassen. Somit wird Intellectual Property Protection für den Endanwender zu einem Prozessschritt in der Datenaustauschkette reduziert und gleichzeitig die Prozesssicherheit erhöht, denn was nicht durch die Leitung wandert, kann natürlich überhaupt nicht in falsche Hände geraten.

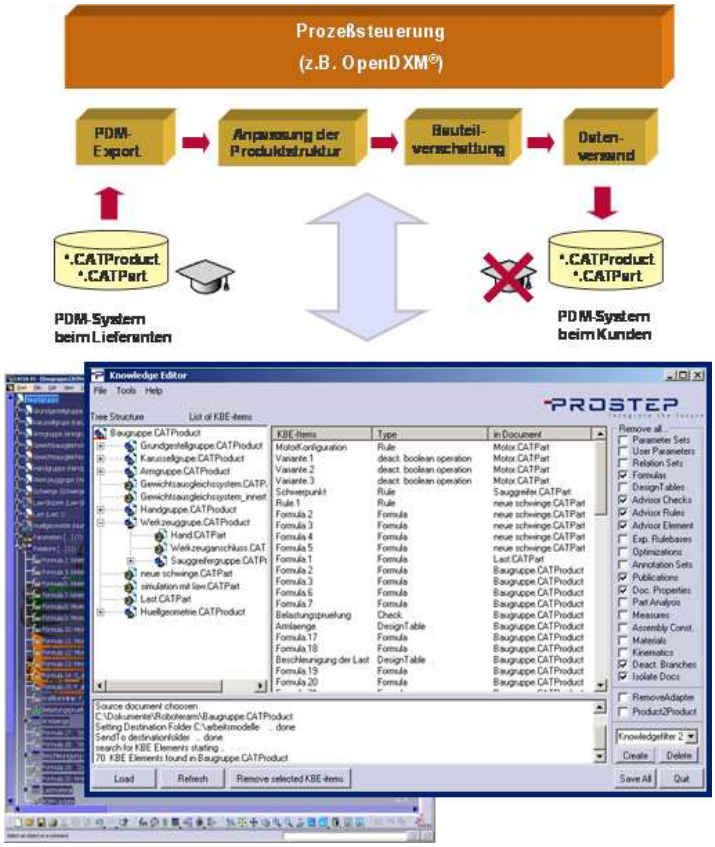

Bild 7: OpenDXM® Prozessintegration für den Knowledge Editor im Batchbetrieb [13]

Von der Bereinigung der CAD-Modelle sieht und merkt der Empfänger nichts, es liegt ein CAD-Modell ohne wertvolles Produktwissen vor, dass trotzdem gerade noch die Anforderung des Datenaustauschpartners erfüllt. Den Ergebnismodellen sieht man die Löschoperation nicht an, d.h. an den Modellen selbst kann der Empfänger nicht erkennen, ob diese vor dem

Versand präpariert d.h. vereinfacht wurden. Diese sehen so aus, als wären sie von Anfang an ohne Verwendung von Wissenselementen erstellt worden.

Verteilte Engineering Prozesse zeichnen sich zusätzlich dadurch aus, dass es mit einem einzigen Datenaustausch häufig nicht getan ist. Das verschickte und bereinigte Modell wird vom Partner verändert und kehrt irgendwann wieder zurück zu seinem Entwickler.
Aus diesem Grund ist auch für die die Re-Integration des Wissens ein Zusatzmodul - der Knowledge Rebuilder - entwickelt worden, mit denen nach Bedarf der Knowledge Editor erweitert wird. Das Thema der Re-Integration des Wissens (regenerative Wissensabschaltung) erfolgt in besonders enger Abstimmung mit dem Kunden. Da die Prozesskomplexität und Varianz beim Wiederanhängen von Wissen prinzipiell deutlich höher ist als beim Löschen des Wissens erfolgt die Lösung unter Einbeziehung der prozessspezifischen Parameter des Kunden. Typische Prozessparameter sind die zu re-integrierenden Wissenstypen (Elementtypen), Anforderungen an die Modell- und Linkstruktur, die aus dem vorangegangenen Löschprozess zur Verfügung stehenden Informationen (CAD-Modelle, Logfiles, etc.) sowie verwendete Konstruktions- und Modellierungsmethoden.

5. Sicherer Austausch von Massendaten

In der Automobilindustrie verwendet jeder OEM eine etwas andere Sicherheitstechnik und konkurrierende Standards für die Verschlüsselung der Informationen und den Austausch von Zertifizierungen, mit der Folge, dass die Zulieferer für jeden Kunden eine eigene Client-Lösung implementieren und ihre Mitarbeiter entsprechend schulen müssen. Um diesen Mehrfachaufwand zu vermeiden, wäre eine einheitliche, auf gängigen Standards basierende Plattform für den sicheren Datenaustausch erstrebenswert. Sie sollte sich in die jeweiligen Portallösungen der OEMs und ihre Enterprise-Systeme integrieren lassen, ohne die Sicherheit ihrer Intranets zu gefährden.
Die heute verfügbaren Datenaustauschlösungen wurden im wesentlichen für die unternehmensinterne Kommunikation bzw. für die Zusammenarbeit mit handverlesenen Partnern konzipiert. Sie basieren auf den klassischen IT-Sicherheitstechnologien wie Firewalls und virtuelle, private Netze (VPN) in Verbindung mit speziellen Protokollen für den direkten Dateitransfer zwischen zwei Firmen, die bei der globalen Kommunikation zunehmend an ihre Grenzen stoßen. Zu Partnern in Indien oder China lässt sich „nicht mal schnell“ eine VPN-Verbindung einrichten und auch das OFTP-Protokoll ist dort weitgehend

unbekannt. Außerdem müssen viele Informationen heute an verschiedene Partner kommuniziert werden, was über dezidierte Leitungen umständlich ist. Zwar bieten manche Datenaustausch-Lösungen schon Funktionen, um Daten zum Download auf einem Webserver bereitzustellen, aber was danach mit den Daten geschieht entzieht sich weitgehend ihrer Kontrolle. Es fehlen ergänzende Werkzeuge und Funktionen, die einen sicheren und nachvollziehbaren Datenaustausch über das Web unterstützen, wie sie seit kurzem OpenDXM® GlobalX von PROSTEP (Bild 8) bereitstellt.

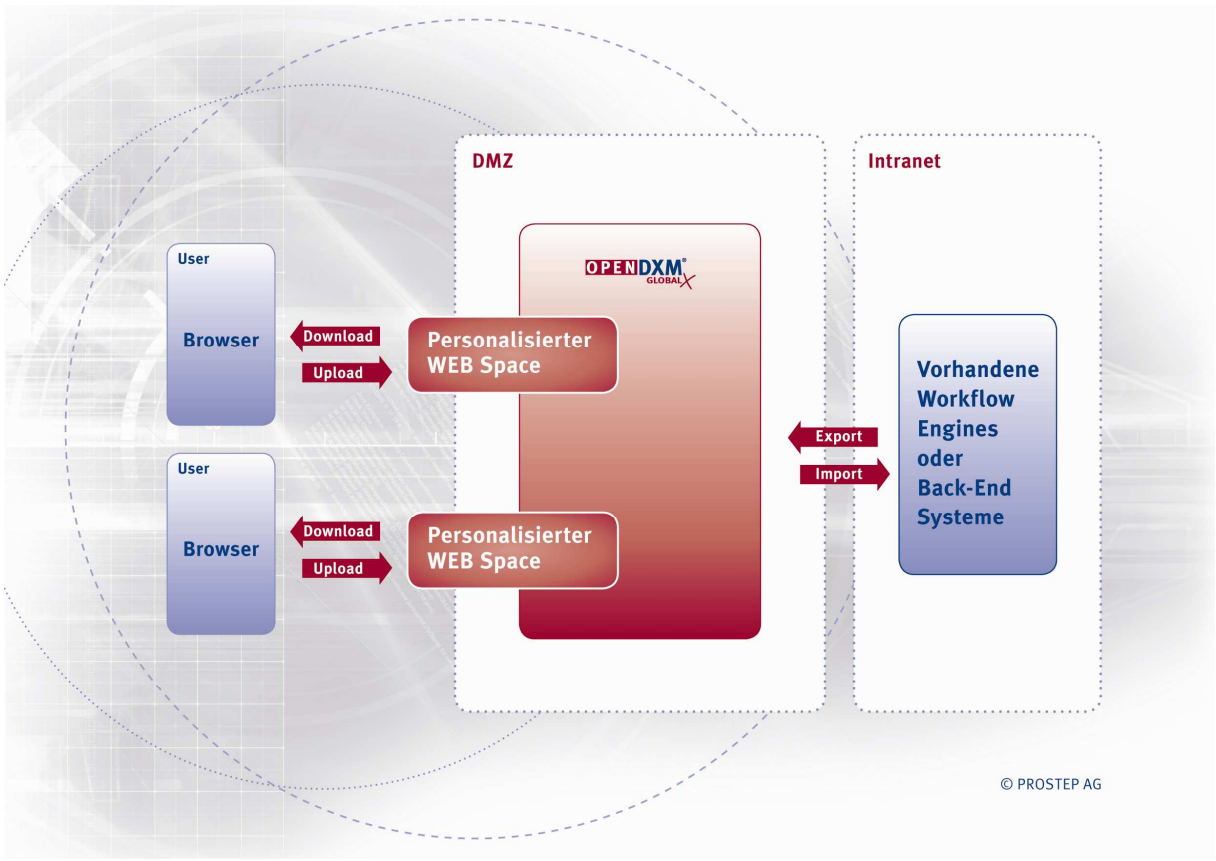

Bild 8: Sicherer Austausch von Massendaten OpenDXM® GlobalX [15]

Wesentliche Voraussetzung für den sicheren Datenaustausch ist die Möglichkeit, den Zugang zu den Daten auf einen bestimmten Personenkreis zu beschränken und bestimmten Personen bzw. Rollen gezielt Nutzungsrechte wie Lesen, Ändern, Kopieren oder Drucken zuweisen zu können. Die Rechte können entweder direkt in die Datei integriert sein wie zum Beispiel bei Adobe PDF-Dokumenten oder sind Bestandteil eines digitalen „Umschlags“, in den die zu schützenden Daten eingebettet werden. Ferner sollte sich die Nutzung der Daten für einen bestimmten Zeitraum, einen bestimmten Standort oder eine bestimmte Zahl von Nutzungsfällen limitieren lassen. Um die Benutzerrechte zu definieren und ihre Einhaltung überwachen zu können, bedarf es einer eigenen DRM-Komponente (Digital Rights

Management), die auch den Austausch der Schlüssel steuert. Gleichzeitig sollte es möglich sein, externe Directory Server für die Rollen- und Rechteverwaltung anzubinden, so dass bereits definierte Rollen und Rechte nicht mehrfach erfasst werden müssen. Über den LDAP-Standard lassen sich die entsprechenden Informationen problemlos importieren.

Als Grundlage für die Authentifizierung der Personen, die Vergabe digitaler Signaturen und die Verschlüsselung der Daten empfiehlt sich eine Public-Key-Architektur. Sie erlaubt eine skalierbare, personen- bzw. rollenbezogene Verschlüsselung der auf der Plattform abgelegten Daten, die nur der betreffende Empfänger wieder entschlüsseln kann.

Bei der Bereitstellung der Daten wird automatisch ein Inhaltsverzeichnis erzeugt, so dass der Empfänger nicht erst die Daten herunterladen und entschlüsseln muss, um beurteilen zu können, ob sie für seine Arbeit relevant sind. Wenn er über einen Schlüssel verfügt, der ihn zur Visualisierung berechtigt, kann er die Daten auch temporär auf der Plattform entschlüsseln und sich mit einem entsprechenden Viewer anzeigen lassen.

Im Unterschied zu den gängigen Collaboration-Plattformen, bei denen das Augenmerk vor allem auf der Online-Zusammenarbeit bei der Produktentwicklung liegt, ist die webbasierte Datenaustausch-Plattform in erster Linie für den (asynchronen) Austausch von großen Datenmengen gedacht, wie sie heute für die OEM-Zulieferer-Kommunikation im Fahrzeug- oder Flugzeugbau charakteristisch sind. Das erfordert spezielle Algorithmen für die Minimierung der Latenzzeiten, die sich beim Versand der vielen Datenpaketen über große Entfernungen zu erheblichen Verzögerungen aufsummieren und dadurch den Durchsatz beeinträchtigen. Die von PROSTEP entwickelte Komponente für den optimierten Up- und Download erhöht den Durchsatz beim transatlantischen Datentransfer um den Faktor 2 bis 3. Außerdem gewährleistet sie, dass die Kommunikation bei einer Unterbrechung der Verbindung dort fortgesetzt wird, wo sie abgebrochen wurde.

Entscheidend für die sichere Kommunikation zwischen Datenaustausch-Plattform und den angebundenen Unternehmenssystemen ist, dass die entsprechende Lösung als passive Komponente innerhalb der DMZ nur nach Aufforderung tätig werden darf. Die Empfänger werden über die integrierten E-Mail-Funktionen informiert, wenn Daten für sie bereitstehen, müssen aber den Download selbst veranlassen und sich nach gegebenenfalls auch selbst um den Virencheck der entschlüsselten Daten kümmern. Wer wann welche Daten herunter geladen hat, wird über die Zuordnung von IP und Benutzer protokolliert und ist damit jederzeit nachvollziehbar.

Neben der lückenlosen Dokumentation der Austauschvorgänge gehören die abgestuften Verschlüsselungsmechanismen und die Unterstützung automatisierter Austauschprozesse zu den wesentlichen Stärken einer solchen webbasierten Plattform wie OpenDXM® GlobalX.

Sie taugt damit nicht nur für die sichere Kommunikation großer Datenmengen im Engineering, sondern kann prinzipiell auch für die Kommunikation von anderen Informationen genutzt werden, beispielsweise als Sourcing-Plattform für die Ausschreibung von Entwicklungs- und Fertigungsaufträgen im technischen Einkauf.

6. Sichere, koordinierte Zusammenarbeit in Liefernetzen

Da die IT-Sicherheitslösungen und Prozesse z.T. sehr unterschiedlich sind, wurde in den entsprechenden Gremien der Automobilindustrie die Initiative Secure Product Creation Processes (SP^2) [11] gestartet, die Methoden für sichere Datenaustauschprozesse in der unternehmensübergreifenden Produktentwicklung entwickeln und etablieren soll, um diesen Aspekt der Kollaboration auf eine möglichst einheitliche methodische und technologische Basis zu stellen. Umfragen zeigen, dass Anwender in punkto IT-Sicherheit den größten Handlungsbedarf im Kontext folgender Szenarien sehen: Datenaustauch mit Dritten, Mobile Daten und Mitarbeiter sowie Langzeitarchivierung geschützter Daten.

Als technologischer Kern wurde das Enterprise Rights Management (ERM) identifiziert, das als ein technischer Ansatz (basierend auf Kryptographie) betrachtet wird, um das Know-how eines Unternehmens in verteilten Produktentwicklungsszenarien zu unterstützen. ERM erlaubt Zugriff auf bestimmte Bestandteile eines Datensatzes und auf ausgewählte Operationen (Lesen/Schreiben/Drucken/…) – im allgemeinen realisiert, indem der Datensatz in einen geschützten Umschlag eingepackt wird.

Da die Initiative durch eine Anwendergruppe im ProSTEP IViP e.V. getrieben wird, wurde ein Zwei-Stufen-Ansatz auf Basis praktischer Anwendungsfälle ausgearbeitet. Der Grundgedanke des Zwei-Stufen-Ansatzes ist, sich in der ersten Stufe auf die Bereiche zu konzentrieren, die für einen ersten Einsatz einer ERM-Lösung unerlässlich sind (kritische Datenaustauschprozesse) und erst in der zweiten Stufe einen umfassenden und modularen Ansatz zu erarbeiten, der vollständig in die Prozesse und Systemlandschaften eingebettet werden kann.

Hierbei werden drei Hauptziele verfolgt, deren Erreichung durch Industriepiloten validiert wird: Spezifikation von Referenzprozessen für unternehmensübergreifendes ERM, Erarbeitung von Empfehlungen zur reibungslosen Einführung von unternehmensübergreifenden ERM-Lösungen und schließlich Sicherstellung der Interoperabilität verschiedener ERM-Lösungen.

Bild 9 illustriert die Situation eines Zulieferers, der mit zwei Herstellern zusammenarbeitet, wie sie sich ohne einen abgestimmten Ansatz darstellen würde. Die vom Zulieferer

verwendete ERM-Anwendung muss für jeden unterschiedlichen Rechte-Server der Hersteller das entsprechende Protokoll für die Kommunikation sowie das Format für die verschlüsselten Dokumente unterstützen. Zudem muss für jeden Hersteller das entsprechende Verfahren zum Austausch von Nutzerinformationen und zur Authentifizierung unterstützt werden. Der Aufwand für die Anschaffung, Installation, Betrieb und Pflege einer solchen Infrastruktur wäre beträchtlich und könnte dem asynchronen Datenaustausch als solchen seine wirtschaftliche Basis entziehen.

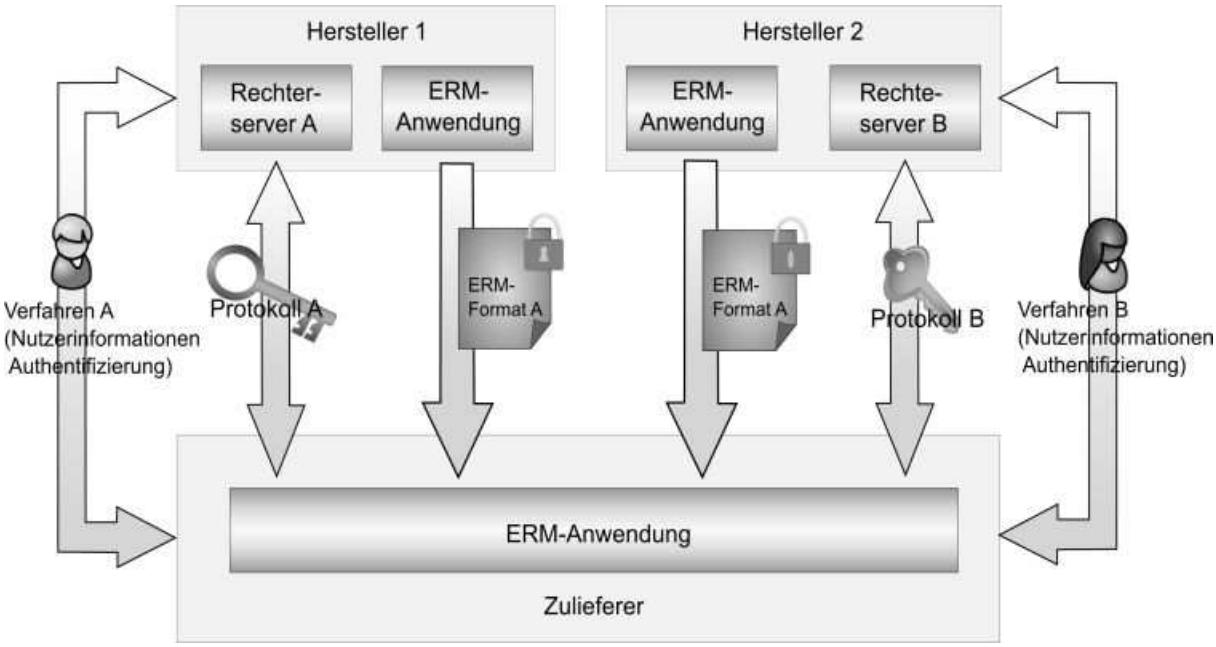

Bild 9: Koordinationsaufwand bei Implementierung einer ERM-Anwendung [11]

Eine Harmonisierung der jeweiligen Bausteine würde die Situation signifikant vereinfachen (Bild 10) und den Gesamtaufwand drastisch reduzieren. Um dies zu ermöglichen, wird im Rahmen der Initiative ein Referenzprozess erarbeitet, der die notwendigen Prozesse für die Einführung und den Betrieb von ERM definiert. Der Referenzprozess bietet einen Rahmen zur Analyse der bestehenden Systemlandschaften und zur Einbindung der ERM-Lösung in diese. Einen weiteren Aspekt bildet der notwendige Abstimmungsprozess der am Datenaustausch beteiligten Unternehmen. Zudem wird der Referenzprozess einen Prozess für die Durchführung eines Austausches von ERM geschützten Informationen definieren. Für den Einsatz von ERM muss der Rechte-Server allen Nutzern, die mit geschützten Dokumenten arbeiten sollen, eine elektronische Identität zuordnen können. Für Nutzer des eigenen Unternehmens reicht hier eine Anbindung an das interne Nutzerverzeichnis. Für externe Nutzer (z.B. Angestellte von Zulieferern) muss dagegen ein Prozess definiert sein,

mit dem für diese Nutzer eine Identität erzeugt werden kann. Zudem muss geklärt sein, wie die Authentifizierung erfolgen kann. Diese Punkte werden im Referenzprozess berücksichtigt. Ferner werden Schnittstellen zwischen ERM-Lösung und Nutzerverwaltung ermittelt.

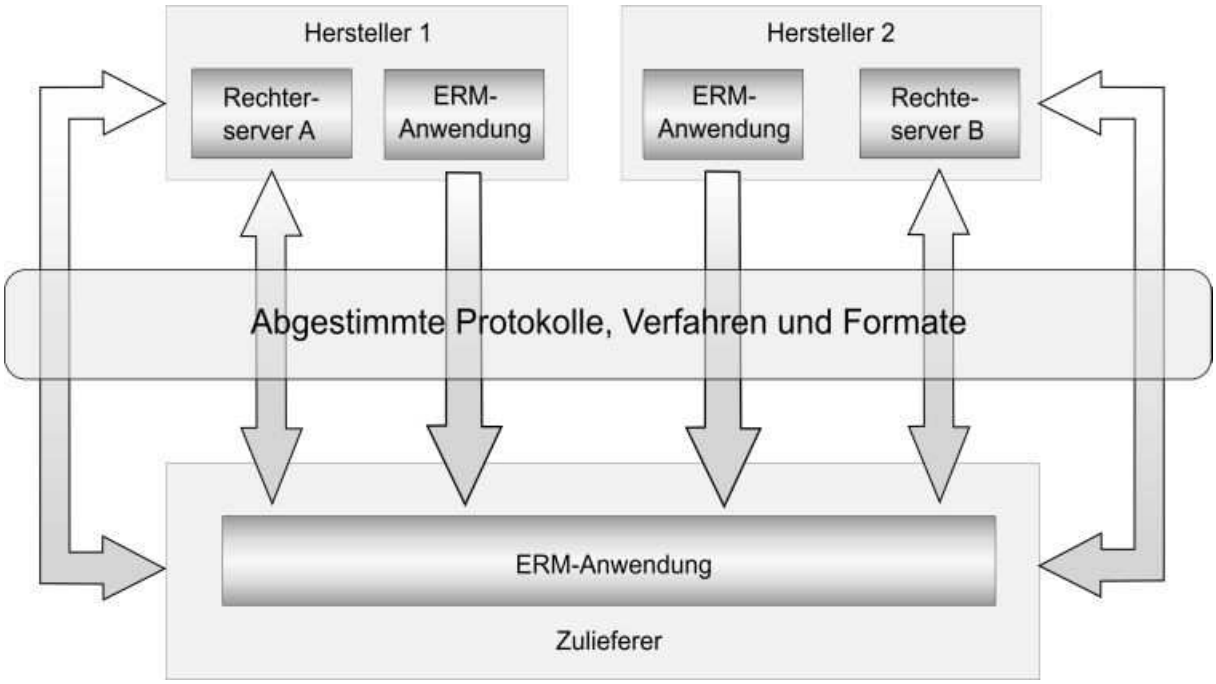

Bild 10: Branchenweit harmonisierte ERM-Architektur [11]

7. Ausblick

Im vorliegenden Beitrag sind die Probleme, die Lösungsansätze sowie die produktiven Software-Lösungen bei der Umsetzung der sicheren Datenaustauschprozesse in der Automobilindustrie dargestellt worden. Von den vielfältigen Risiken und Herausforderungen ausgehend erfordert der Know-how-Schutz ein Bündel von geeigneten organisatorischen und technischen Maßnahmen. Von der eigenen Position in der Lieferkette und der Interessenslage hängt ab, welche von vielen technischen Maßnahmen vorrangig eingesetzt werden müssen.

Die Weiterentwicklung der Methoden und Lösungen zur Bereitstellung von sicheren Datenaustauschprozessen wird in Richtung von skalierbaren, auf Basis von führenden CAD- und PDM-Systemen aufbauenden IPP- und ERM-Applikationen gehen, die sich in die existierende, voll automatisierte CA Prozesskette einfügen lassen. Durch diese Technologie

wird jedes Unternehmen in der Lieferkette sein Intellectual Property situationsabhängig schützen können, ohne den geregelten Datenfluss zu stören.

8. Literatur

[1] Manager Magazin: “Patentdiebstahl: Chinas Smart-Nachbau”, 12. Oktober 2006, http://www.manager-magazin.de/it/artikel/0,2828,442288,00.html

[2] Spiegel: „Ideenklau: MAN zieh in China vors Gericht“, 19. Oktober 2006, http://www.spiegel.de/wirtschaft/0,1518,443522,00.html

[3] Die Welt: „Doppelmayrs wundersame Seilbahnvermehrung in China“, 17. Februar 2006, http://www.welt.de/print-welt/article198743/Doppelmayrs_wundersame_Seilbahnvermehrung_in_China.html

[4] http://www.vdma.org/wps/portal/Home/de/VDMAThemen/Politik_und_Initiativen/VDMA-Kampagne+Pro+Original?WCM_GLOBAL_CONTEXT=/Home/de/VDMAThemen/Politik_und_Initiativen/VDMA-Kampagne+Pro+Original&initsearch=

[5] Wildemann, Horst: Produktpiraterie - Leitfaden zur Einführung eines effizienten und effektiven Kopierschutz-Managements, München, TCW Transfer-Centrum für Produktions-Logistik und Technologie-Management GmbH & Co. KG, 2008

[6] Quandt. S.: The Insider Treat Benchmark Report – Strategies for Data Protection, White Paper, Aberdeen Group, January 2006, http://www.aberdeen.com

[7] Liese, H.: Wissensbasierte 3D-CAD Repräsentation, Shaker Verlag, Aachen, 2004. Zugl.: Darmstadt, Techn. Univ., Diss., 2003

[8] Liese, H., Stjepandic, J.: Konstruktionsmethodik: Wissensbasierende 3D-CAD-Modellierung, CAD/CAM Report, Dressler Verlag, Heidelberg, 2004, 10, http://www.prostep.com/de/prostep/medien/cad-cam_kbe.htm

[9] N.N.: VDA-Empfehlung 4961/2, Verband der Automobilindustrie e.V., Ausgabe November 2001, www.prostep.org/fileadmin/freie_downloads/Empfehlungen-Standards/VDA/VDA4961-2.pdf

[10] Martin, H.P.: CATIA V5 & Intellectual Property Protection - “Stupid” or Parameterized Geometry – what should the supplier deliver? Workshop at ProSTEP iViP Association, Darmstadt, Februar 7, 2006

[11] N.N.: Secure Product Creation Processes (SP2) - Sichere Datenaustauschprozesse in der unternehmensübergreifenden Produktentwicklung, White Paper, ProSTEP iViP e.V., Darmstadt, 2007

[12] Antegnard, Lionel; Liese, Harald; Stjepandic, Josip: Intellectual Property Protection in Concurrent Engineering Domains; ISPE Conference on Concurrent Engineering, Antibes, IOS Press 2006

[13] Liese, H., Spitznagel, P.: Know How Schutz für CAD-Entwicklungsdaten, ProSTEP iViP Symposium 2008, Berlin, http://www.prostep.org/de/events/symposium2008/programm/080409/1445_b.htm/

[14] Liese, H., Stjepandic, J., Rulhoff, Stefan: Intellectual Property Protection im Virtual Engineering, IFF Wissenschaftstage 2008, Magdeburg

[15] Bugow, R.: Mehr IT-Sicherheit beim Datenverkehr, CAD/CAM Report, Dressler Verlag, Heidelberg, 2007, 12, http://www.prostep.com/mn/press/prostep-in-den-medien/newsdetail/artikel/299/mehr-it-sich/?L=1print.html&cHash=331ccce014