Sichere Produktdaten

Um ihr geistiges Eigentum zu schützen, müssen Unternehmen vor allem die Sicherheit von digitalen Produktdaten im Produktentwicklungsprozess gewährleisten können. Dafür geeignete Verfahren können wirtschaftlichen und technischen Schaden durch Datenspionage verhindern. Wissenschaftler der TU Darmstadt entwickeln am CASED ein neues Konzept, um den Schutz von Produktdaten weiter zu verbessern und untersuchen aktuelle Enterprise Rights Management (ERM)-Lösungen in Hinblick auf die Anforderungen der Automobilindustrie.

Secure Product Data

In order to keep the intellectual property of a company protected, product data has to be protected during the product development process. Appropriate techniques avoid economical and technical damage caused by data espionage. At CASED, a new concept to improve product data protection is being developed, and current Enterprise Rights Management solutions are evaluated in respect to the requirements of the automotive industry.

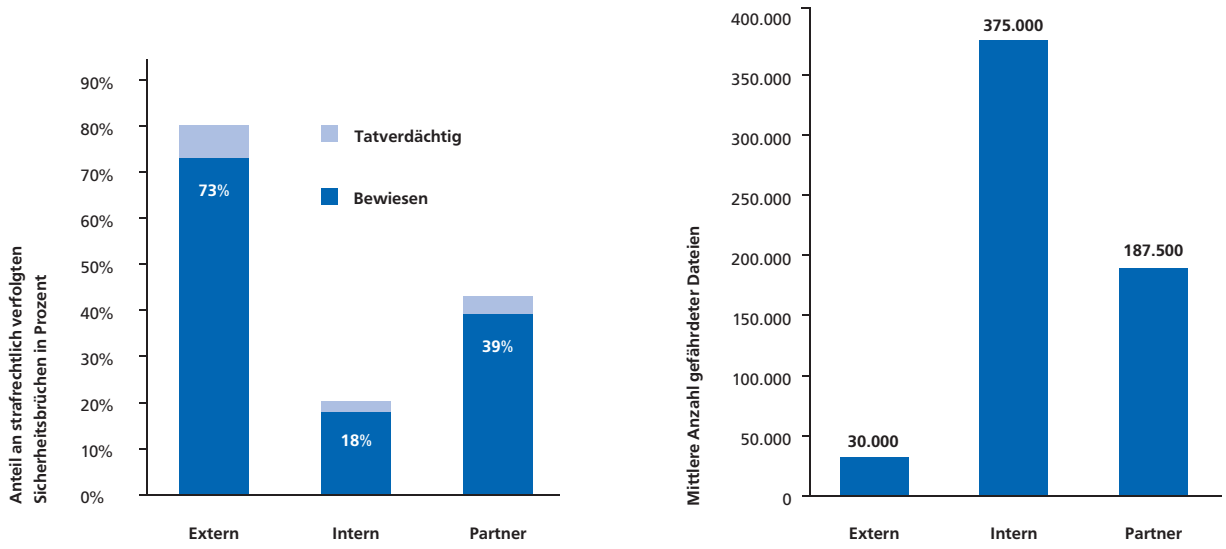
Reiner Anderl, Joselito Rodrigues Henriques • Im Ingenieurwesen ist der Einsatz des rechnergestützten Konstruierens (Computer Aided Design, CAD) in der Produktentwicklung nicht mehr wegzudenken. Es steckt viel schützenswertes Wissen – geistiges Eigentum (Intellectual Property, IP) – in den CAD-Daten, das sich einfach speichern, reproduzieren und in die Prozesskette integrieren lässt – und auf das leicht zugegriffen werden kann.

Einerseits beschleunigt die Integration von Firmen-Know-how in CAD-Daten die Produktentwicklung und ermöglicht die Zusammenarbeit von verschiedenen Unternehmensbereichen, etwa von Entwicklung und Produktion. Andererseits steigt das Risiko für Unternehmen, wenn sie die CAD-Daten neben den internen Abteilungen auch externen Partnern zur Verfügung stellen müssen.

Heute regeln die meisten Unternehmen die Nutzung und Weitergabe ihrer Unternehmensdaten durch Partner nur durch Geheimhaltungsvereinbarungen, Gesetze und technische Maßnahmen. Diese aber können die Sicherheit der Daten nicht garantieren. Sobald die Daten das Unternehmen verlassen, hat der Urheber keine Möglichkeit mehr, sie zu kontrollieren. Ohne den effizienten Schutz von Produktdaten steigt der durch Industriespionage und Produktpiraterie verursachte Schaden weiter an.

Reiner Anderl

Abbildung 1
Verursacher von Sicherheitsbrüchen und Anzahl der gefährdeten Dateien



Nach einer von der Business Risk & Crisis Management GmbH durchgeführten Studie aus dem Jahr 2007 kostet Industriespionage deutsche Unternehmen jedes Jahr zirka 20 Milliarden Euro. Über 500 Fälle von Datenspionage über einem Zeitraum von vier Jahren wurden einer forensischen Untersuchung des Verizon Business Risk-Teams zufolge gemeldet. Abbildung 1 zeigt das Ergebnis einer Analyse, in der die Verursacher von Sicherheitsbrüchen und die Anzahl der gefährdeten Dateien aufgeführt werden.

Um die Sicherheit der gemeinsam genutzten Daten zu garantieren, kann man beispielsweise sicherstellen, dass nur befugte Personen auf verteilte Daten zugreifen können. Dies kann durch die ERM-Technologie (Enterprise Rights Management) gewährleistet werden, wobei die Daten bereits bei ihrer Erstellung geschützt werden. Für den Schutz von CAD-Daten ist die Integration von ERM-Lösungen jedoch neu. In CATIA zum Beispiel, einem der wichtigsten in der Automobilindustrie eingesetzten CAD-Systeme, wurde die ERM-Technologie 2007 eingeführt. Produktdaten werden mithilfe aktueller ERM-Lösungen zwar sicherer, trotzdem kann darin enthaltenes geistiges Eigentum aber noch nicht ausreichend geschützt werden. Aus diesem Grund arbeitet das Fachgebiet „Datenverarbeitung in der Konstruktion DIK“ am CASED daran, die aktuelle ERM-Technologie zu verbessern und somit die Verarbeitung von digitalen Produktdaten sicherer zu gestalten.

Fachgebiet Datenverarbeitung in der Konstruktion
Prof. Dr.-Ing. Reiner Anderl
Tel. 06151/16-6001
E-Mail: anderl@dik.tu-darmstadt.de

M.Sc. Joselito Rodrigues Henriques
Tel. 06151/16-50778
E-Mail: joselito.henriques@cased.de
www.dik.tu-darmstadt.de

Produktdaten

Viel Firmen-Know-how lässt sich heute digital in CAD-Dateien speichern: Neben grundlegenden Informationen über die Geometrie werden verschiedene Arten von Produktinformationen in CAD-Dateien gespeichert. Dazu zählen hochsensible Informationen, wie Modellierungs- und Konstruktionsstrategien, Produktionsinformationen

und Konstruktionsmerkmale sowie Produkteigenschaften und Materialdaten. Eine weitere Form von geistigem Eigentum in CAD-Dateien sind Wissensmodelle, die in der wissensbasierten Konstruktion (Knowledge Based Engineering, KBE) eingesetzt werden. Mithilfe von KBE können Konstrukteure intelligentere digitale Produktrepräsentationen erzeugen, indem sie in die Bauteildateien komplexe Gleichungen, Parameter, topologische Informationen und andere Informationen einbinden. Mit der Integration von KBE in den Produktentwicklungsprozess werden Zeit und Kosten der Produktentwicklung in erheblichem Umfang reduziert. Die sich ergebende Produktstruktur wird in Abbildung 2 dargestellt.

Aktuelle technische Ansätze zum Schutz von Produktdaten

Die aktuellen Methoden, das geistige Eigentum der Firmen zu schützen, erfüllen nicht alle Anforderungen der Industrie. Es gibt zum Beispiel nach wie vor keine Möglichkeit, die CAD-Daten auf feingranularer Ebene zu schützen. Dies ist aber wichtig für die sichere Zusammenarbeit mit internen und externen Partnern im Produktentwicklungsprozess. Im Folgenden werden einige der aktuell eingesetzten Verfahren zum Schutz von Produktdaten vorgestellt und die möglichen Schwachstellen erläutert.

Terminalserver

Terminalserver ermöglichen es, die vollständige Kontrolle über Daten zu gewährleisten, da sie nur per Fernzugriff verarbeitet werden können. Sie können aber nur eingesetzt werden, wenn die relevanten Daten dem Unternehmen des Benutzers gehören und nur intern verwendet werden. Diese technische Methode ist hilfreich, um geistiges Eigentum innerhalb des Unternehmens zu schützen. Sie deckt allerdings nicht den in der Firmenkooperation essenziellen Datenaustausch ab (Abbildung 3a).

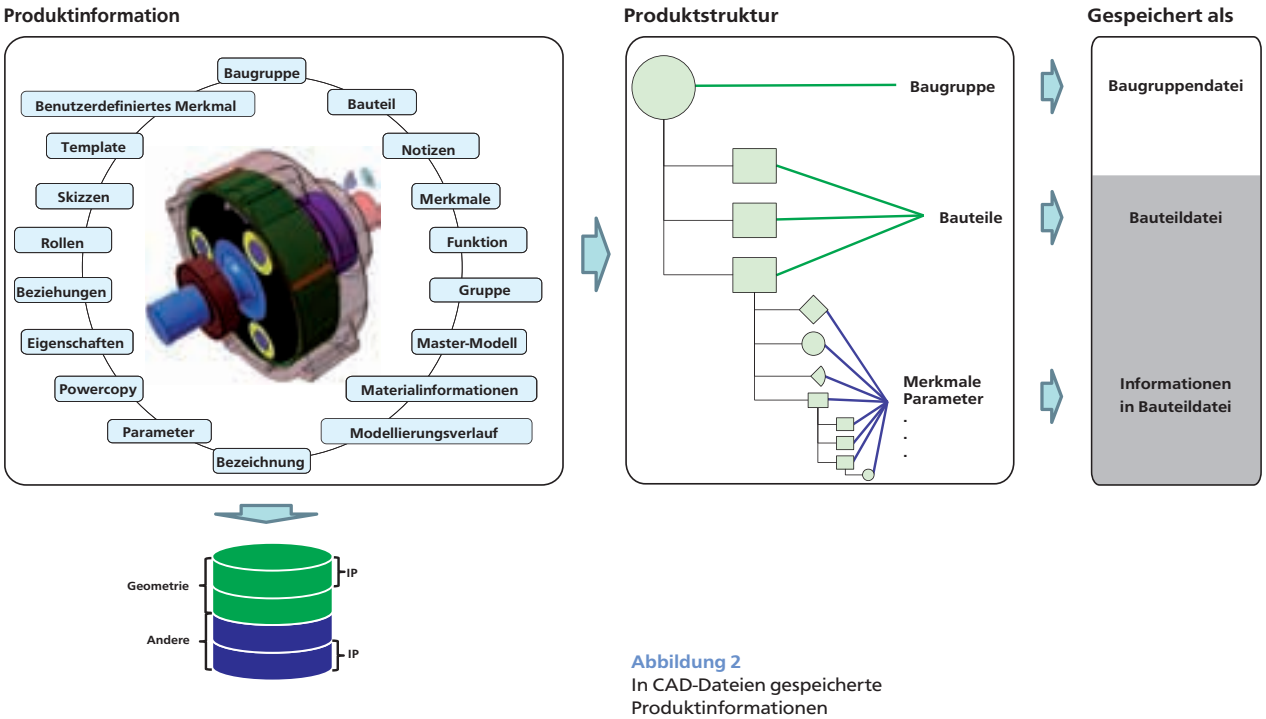


Abbildung 2
In CAD-Dateien gespeicherte Produktinformationen

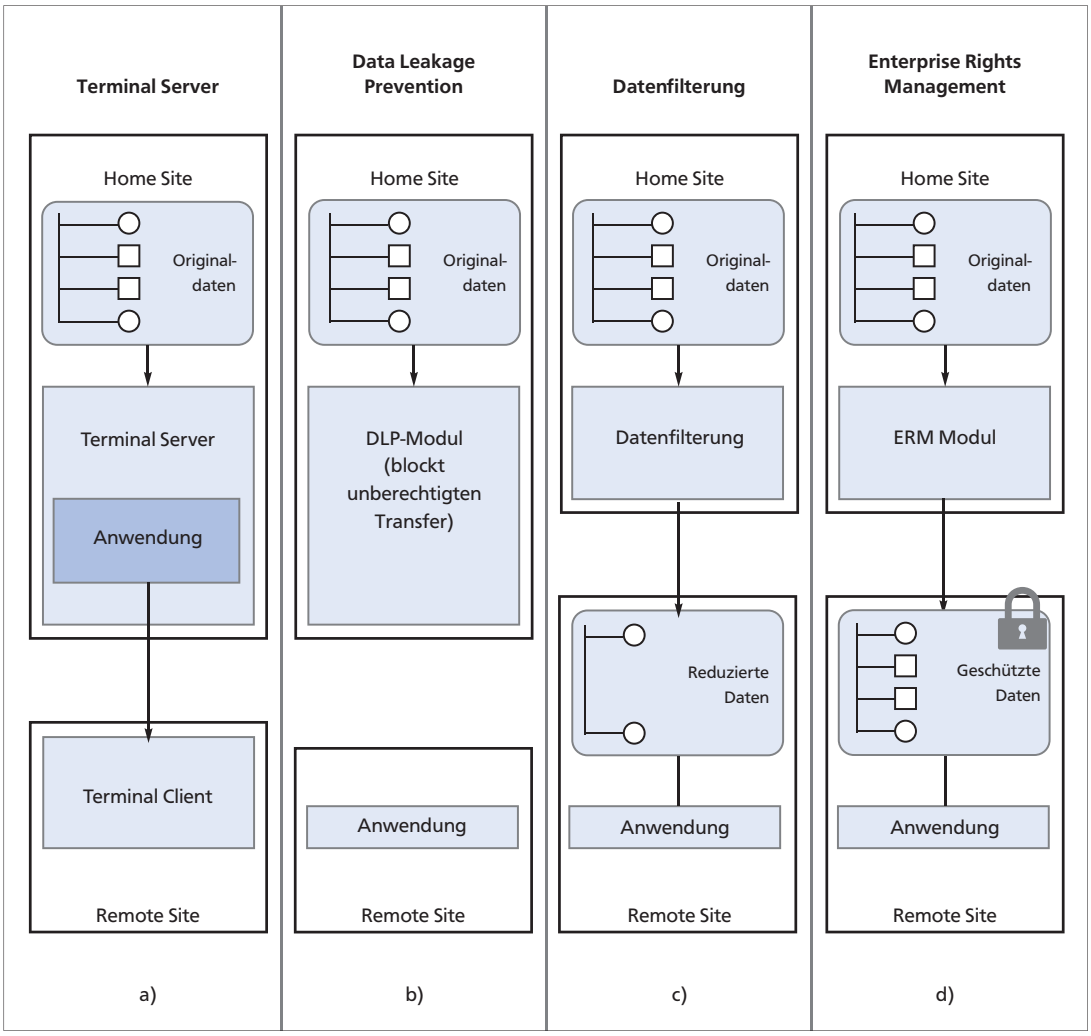


Abbildung 3
Technische Ansätze zum Schutz von geistigem Eigentum

Data Leakage Prevention (DLP)
Bei dieser Methode wird durch spezielle Software auf dem Anwendersystem kontrolliert, welche Daten über welche Schnittstellen (zum Beispiel E-Mail, über Netzwerk oder externe Speichergeräte) übertragen werden dürfen. Diese Lösung ist sehr komplex, da der Schutz von Daten nur dann vollständig gewährleistet ist, wenn die komplette Softwareumgebung der Benutzer kontrolliert wird. Sobald auch nur eine unüberwachte Schnittstelle vorliegt, und Daten darüber kopiert werden oder das Unternehmen im Rahmen des Datenaustauschs verlassen, können sie ungehindert weiter verteilt werden (Abbildung 3b).

Datenfilterung
Diese Methode reduziert den Wissensinhalt in den CAD-Daten, indem sensible Informationen gelöscht werden. Datenfilterung ist eine effiziente Methode, um geistiges Eigentum beim Datenaustausch zu schützen. Allerdings ist sie wiederum nicht dafür geeignet, um geistiges Eigentum innerhalb des Unternehmens zu schützen. Darüber hinaus erlaubt die Methode nicht, jene Informationen zu kontrollieren, die nicht gelöscht wurden

und so immer noch das Unternehmen verlassen (Abbildung 3c).

ERM – Enterprise Rights Management

Bei dieser Methode werden die Daten bereits bei der Erstellung geschützt und überwacht. Der Schutz bleibt während des gesamten Lebenszyklus erhalten. Heute ist dies die einzige Methode, die geistiges Eigentum prinzipiell innerhalb und außerhalb des Unternehmens effizient schützen kann. Allerdings ist heute ein Schutz per ERM nur auf Dateiebene möglich. In den Dateien befindliche Informationen können bisher nicht selektiv auf feingranularer Ebene geschützt werden; sobald Zugriffsrechte für eine Datei bestehen, wird dadurch deren Wissensinhalt vollständig zugänglich.

Es ist offensichtlich, dass keine der bisherigen Methoden alleine sicheren Schutz von digitalen Produktdaten gewährleisten kann. Eine Kombination der Ansätze der genannten Methoden kann die gewünschte Sicherheit ermöglichen. Als effiziente Lösung wird die Weiterentwicklung der ERM-Technologie angesehen, die um feingranularen Schutz für verschiedene Datenebenen und Benutzer erweitert werden kann (Abbildung 3d).

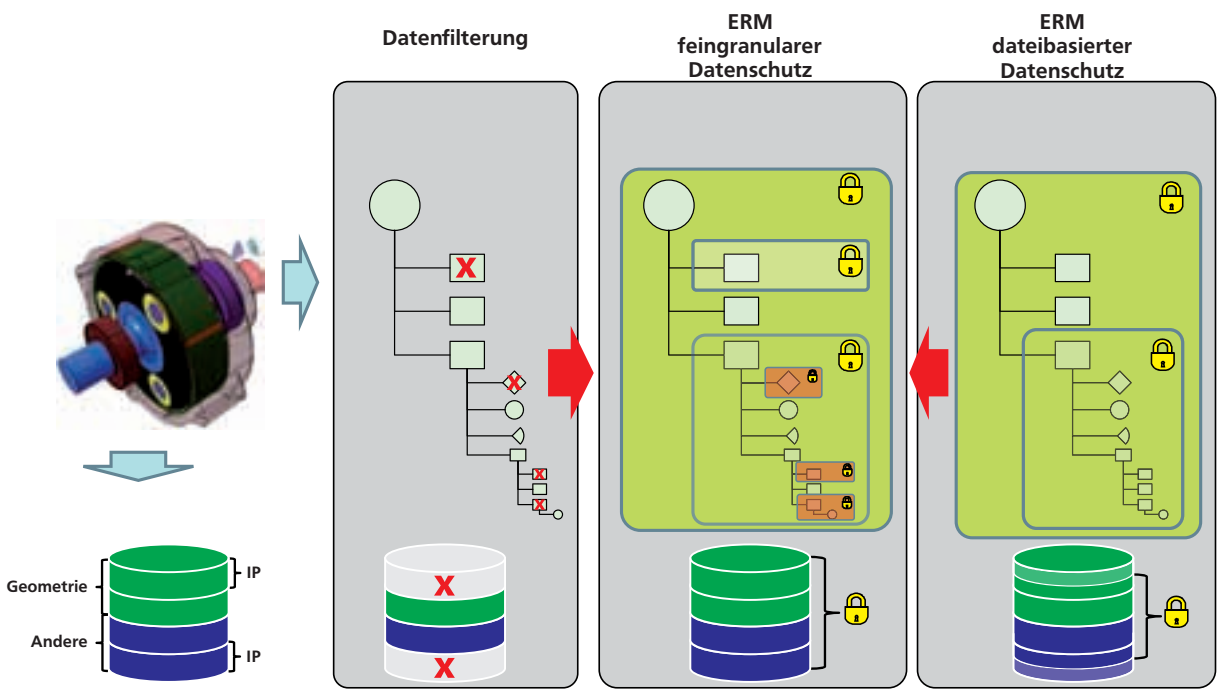


Abbildung 4
Konzept für eine ERM-Lösung für feingranularen Schutz in 3D-CAD-Daten

Zukünftiger Ansatz zum Schutz von Produktdaten

Neue Verfahren zum Schutz von Produktdaten müssen immer auch die spezifischen Anforderungen der Anwender erfüllen. Aus diesem Grund arbeiten wir in einem gemeinschaftlichen Produktentwicklungsprozess mit verschiedenen Automobilunternehmen, Forschungsinstituten, ERM- und CAD-Systementwicklern zusammen.

Unsere Forschung konzentriert sich auf zwei Hauptgebiete:

- Bewertung von aktuellen ERM-Lösungen: Aktuelle ERM-Lösungen werden entsprechend den Anforderungen der Automobilindustrie bewertet. Bisher wurden verschiedene Tests durchgeführt und deren Ergebnisse als Grundlage für die Weiterentwicklung genutzt: Automobilunternehmen entscheiden mithilfe unserer Ergebnisse, an welchen Schnittstellen und für welche Szenarien die jeweilige ERM-Lösung angewendet wird. ERM- und CAD-Entwickler verbessern mithilfe der Ergebnisse die aktuellen Lösungen, und Wissenschaftler der TU Darmstadt erforschen am CASED verbesserte ERM-Konzepte.
- Entwicklung von Konzepten zur Verbesserung von ERM-Technologien: Unser neues ERM-Konzept wird erstmals feingranularen Schutz von CAD-Daten ermöglichen, so dass autorisierte Benutzer ausschließlich auf jeweils für sie relevante Informationen zugreifen können. So soll die Sicherheit von Firmen-Know-how um ein Vielfaches gesteigert werden. Die neue Methode kombiniert ERM- und Datenfilterungsmethoden und vereint so die Vorteile beider (siehe Abb. 4).

Das gesamte geistige Eigentum in einer CAD-Datei wird entsprechend seiner Art der Wissensinformationen auf feingranulare Weise strukturiert und anschließend durch ERM-Verschlüsselung geschützt. Um Wissensinformationen selbst zu strukturieren, wird die Technik aus der Datenfilterungsmethode verwendet. Diese kann verschiedene Arten von geistigem Eigentum verfolgen und ermitteln.

Reiner Anderl ist Vizepräsident der TU Darmstadt und Leiter des Fachgebiets für Datenverarbeitung in der Konstruktion (DiK) im Fachbereich Maschinenbau. Er ist Principal Investigator des LOEWE-Zentrums CASED.

Joselito Rodrigues Henriques ist wissenschaftlicher Mitarbeiter am Institut für Datenverarbeitung in der Konstruktion und Koordinator des Anwendungslabors am CASED.