THE APPLICATION OF SECURITY TECHNOLOGY WITHIN CAX PROCESSES FOR PROTECTING INTELLECTUAL PROPERTY IN PRODUCT DEVELOPMENT

Diana Völz, voelz@dik.maschinenbau.tu-darmstadt.de
Joselito Henriques, henriques@dik.maschinenbau.tu-darmstadt.de
Reiner Anderl, anderl@dik.maschinenbau.tu-darmstadt.de
Technische Universität Darmstadt - Department of Computer Integrated Design, Petersenstraße 30, D-64287 Darmstadt, Germany
Center for Advanced Security Research Darmstadt - CASED, Mornewegstraße 32, D-64293 Darmstadt, Germany

Marco Grimm, marco.grimm@cased.de
Center for Advanced Security Research Darmstadt - CASED, Mornewegstraße 32, D-64293 Darmstadt, Germany

Abstract. *In times of globalization, companies are forced to operate in interorganizational and global cooperation to be competitive. An appropriate example is the automotive industry where an OEM needs to collaborate with several suppliers spread all over the world to make developing cars possible. In this case, sharing information by data-exchange with the partners is elementary for successful projects. Hereby the protection of companies' Intellectual Property (IP) in documents has to be taken under consideration. The distribution of highly sensitive development data contains risks. The damage caused by industrial espionage and product piracy has continually increased over the last years. Recent studies show that economic damage due to theft of information happens both internally and externally of companies. Thus the protection of IP in product development is challenging especially in cross-company cooperation. In this paper the specific task of transferring 3D-CAD files within product development cooperation is focused, because IP within the 3D-CAD model sometimes is not clearly visible for all cooperation parties.*
In this paper the researchers assume that protecting IP is influenced by both, technical and human-related aspects. Various technical approaches are available to protect IP within 3D-CAD-models. But does ongoing IP-protection technology meet industrial requirements? These solutions are normally based on IT security methods that do not support fine granular protection of IP within 3D-CAD-models.
However, protecting IP is applied in different working processes during the CAx-processes, which highly depends on the projects situation. Thus the human-related aspect of protecting IP deals with trust between cooperation partners involved in one projects. Trust in teamwork is one of the key factors for successful cooperation and enhances data exchange.
In this paper, both aspects were brought together by analyzing two current commercial enterprise rights management (ERM) solutions in terms of their ability and efficiency to protect IP within 3D-CAD-models in collaborative product development and by investigating the role of trust within protecting IP during data exchange in cooperation.

Keywords: *Intellectual property protection, Product Development, Trust, Enterprise Rights Management, cross-corporation collaboration*

1. INTRODUCTION

Today, in order to be competitive, it is essential for companies to be represented on the global market. Under the conditions of globalization and an increasing complexity of products and production methods, working in projects and within interorganizational cooperations has already become usual. Especially in automotive sector, cooperations are required to combine worldwide distributed expertise. Figure 1 draws up the interdependent relationship between Original Equipment Manufacturer (OEM), tier 1 and tier 2 in product development.

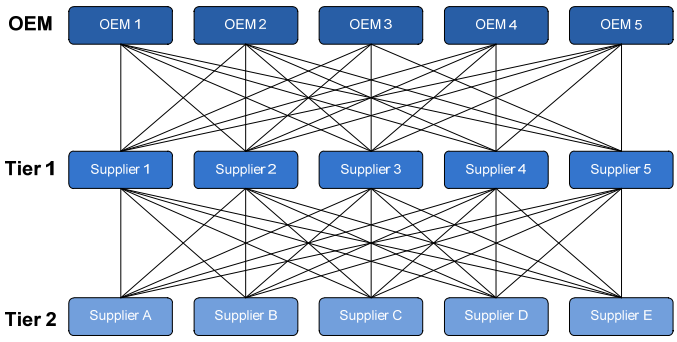

Figure 1. OEM-Supplier network in automotive industry

Cooperating in networks enables flexibility, e. g. in combining various competencies on one project and in outbalancing capacity. Despite all the advantages that arise for companies, finally globalization means limitations as well. Intransparent project structures and global virtual team settings for example, can increase mistrust in team work. Thus, companies tend to fear data-misuse and loss of captive business know-how. In this context, trust and/or mistrust especially in interorganizational collaborations becomes an important aspect and is often difficult to balance.

Today knowledge is one of the most important resources for companies to be competitive in the global market. Industrial spying and piracy of products are criminal methods of intentional misuse of companies` innovations. The damage caused by industrial espionage and product piracy has enormously increased over the last few years, for instance German companies lost around 20 billion Euros per year by industrial espionage (Corporate Trust, 2007). A recent survey, conducted by VDMA in 2010, shows that about 2/3 of the respondent 350 companies are affected by piracy of products (VDMA, 2010). The result is that "protection of IP" more and more becomes important for companies. Protection of IP can take place in different phases of the product life cycle. However, beside the management body the development department is seen most responsible to protect IP in this survey (Fig. 2), not at the least because of more and more knowledge can be integrated into the 3D-CAD-model.

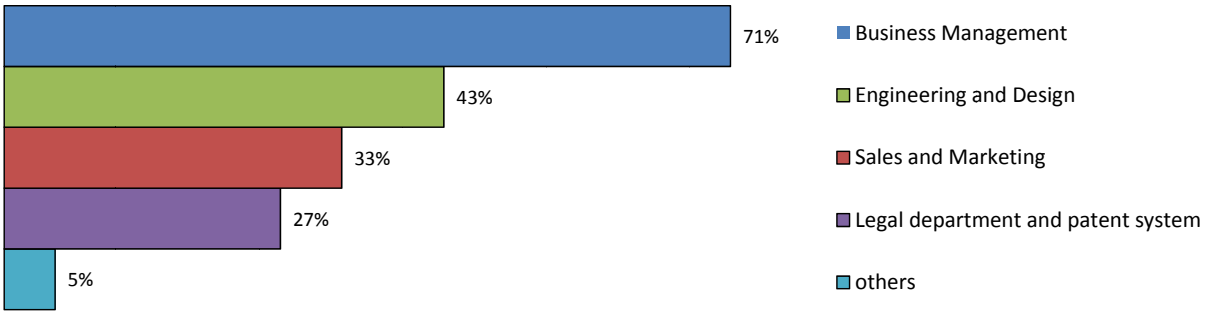

Figure 2. Responsible departments for protecting IP in companies (VDMA, 2010)

In the past, IP was stored in different conventional paper documents and of course in the mind of a company's employee as well. Today, a large amount of company's know-how can be stored highly concentrated in digital documents and CAD files. Apart from information about geometry, various types of product information are integrated in CAD files, too, including modeling/engineering strategies and product properties, like design features, power copies, model templates, material information, form or position tolerances (manufacturing IP), just to name a few. Knowledge based engineering (KBE), a generative design discipline offered by modern CAD systems, is another form to add IP to CAD models. KBE enables designers to create more intelligent digital product representations by including complex equations, parameters and adjacency information in part files. When assembling parts, the topmost assembly file contains most IP. The resulting product structure including IP (distinguished in geometric IP and others) is illustrated in Fig. 3.

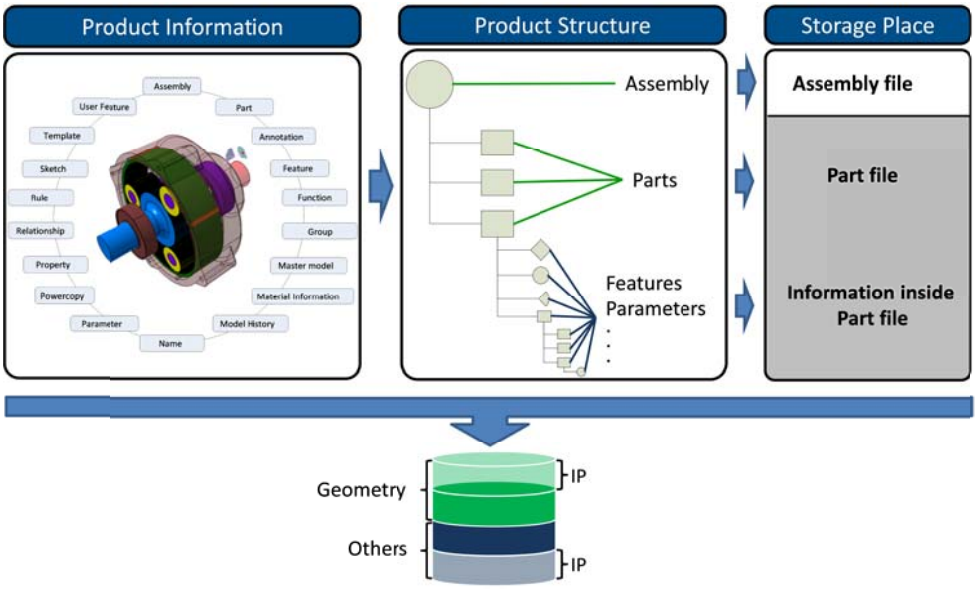

Figure 3. Product information saved in CAD files

As a result, the large amount of IP contained in CAD data makes CAD files very valuable for companies. In order to avoid theft, plagiarism and abuse of IP, it is very important to efficiently protect them in the whole product life cycle and within the CAx processes.

In this paper we assume that in practice both, the human-related and technical dimension in the process of data exchange should be taken into consideration. Hence, after having explained the relevance of protecting IP in interorganizational cooperation, we demonstrate our research objectives in more detail in section 2. Section 3 contains the state of the art of ongoing IP protection methods within 3D-CAD data used in CAx-process and researches in trust. The results of both perspectives will be combined to one common concept in paragraph 4.3. This paper ends with an outlook and an overall conclusion in section 5.

2. RESEARCH OBJECTIVES

The key point of research is IP loss during data exchange and the hereby applied measures of IP protection within cooperation as well as the technical objects to do so. Current research on IP protection focuses either on technical or on human-related aspects of IP protection. In this paper we assume that the technical as well as the human-related aspects in protecting IP stick together. Thus, both aspects can't be taken under consideration separately. We assume that the behavior of employees in protecting IP is mostly influenced by two aspects: The availability of IP protection methods in the company and the trust between people in teams in different dimensions as well. The resources of technical objects to protect IP define the granularity of the exchanged IP whereas trust is responsible for the amount of knowledge which is transferred within these processes. The technical aspect goes hand in hand with the human-related factor trust. The research questions of this paper are:

- How can trust be measured in cooperations and which are the influencing factors?
- How do ongoing technical IP protection technologies meet the requirements of industry?
- How granular can IP be protected within 3D-CAD-models and
- Finally, how do both challenges fit together?

For the human-related aspect, the interviews, which were conducted, mainly point out IP protection as part of working processes and the application of IP protection technologies within cooperation practice, respectively.

To analyze the technical aspect, two ongoing ERM-systems supporting the IP protection of CAD-data were tested. The outcomes show how these ERM-systems technically support IP-protection and in what extent they meet the requirements of automotive industry's IP protection.

The synthesis of this paper depicts both the technical as well as the human-related requirements within IP-protection in CAx-processes of interorganizational product development cooperation.

3. LITERATURE REVIEW

Firstly, current technical approaches to protect IP within CAD-models are described. After that background of trust aspects for cooperations is described and the scope for this research is defined in order to integrate various trust aspects in the concept of IP protection.

3.1. Technical approaches to protecting intellectual property

There are different technical approaches in order to protect and secure IP saved in product data (3D-CAD data) during the collaborative product development process. Ongoing technologies to protect IP can be distinguished in these different approaches below:

- Terminal Server (TS)
- Data Leakage Prevention (DLP)
- Data Filtering (DF)
- Enterprise Rights Management (ERM)

Those technical approaches provide different ways to protect IP in the product creation process. Figure 4 illustrates the systems' structure and the way product data is processed in order to provide IP protection/security for each approach. Whereas Terminal Server and Data Leakage Prevention are commonly used in the product design process, Data Filtering and ERM in general are widely used to protect (DF) and secure (ERM) IP in interorganizational data exchange.

Terminal Server is an application which distributes a graphical user interface over a network connection, so that the design software which processes CAD data is located at the "home site" of a company. Authorized people connect remotely to that application and work with the data through a client application without physically possessing the files.

A disadvantage of this method is that it does not cover the data exchange between OEM and suppliers in collaborative product development.

By applying Data Leakage Prevention (DLP), the distribution and storage of CAD files by a user is controlled by a software module. The module manages users as well as devices and blocks unauthorized distribution or storage of the files in order to avoid data leakage. Even with strong system restrictions, there can be ways to bypass the DLP modules – then there is no control over the file anymore.

Data Filtering is used for reducing IP amount inside CAD data files by deleting IP, mostly applied before the file is distributed to a supplier according to Mullingan et al. (2003). Deleted IP cannot be automatically recovered completely, when changed data returns from the supplier. In this case, data filtering means more management effort in the development process. Since data filtering is only applied when sending files to suppliers etc., internal data theft can't be avoided with this method.

Using ERM, CAD files and contained IP is secured by encryption. Hereby a rights server, which logically owns the file, controls access permissions during the whole data life cycle (Arnab et al., 2008). The content of an ERM protected file can only be accessed when ERM server authorizes access. Protection is kept, even if the file is outside of the company.

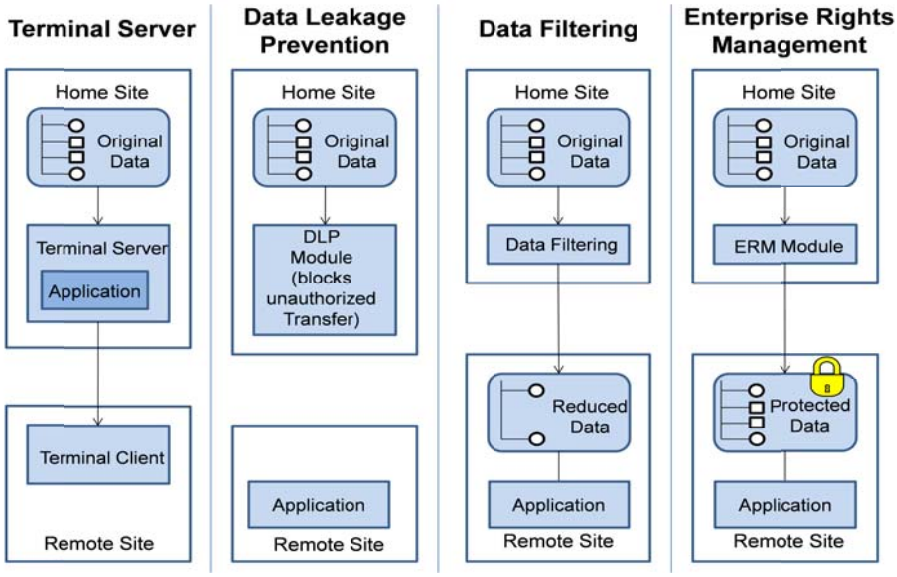

Figure 4. Technical approaches for protecting intellectual property (ProSTEP iViP, 2008)

Today, it is necessary to combine different technical approaches to reliably protect IP. Data filtering is technically the only way to protect IP in CAD data in a granular level by deleting content. In order to maximize productivity and reduce management effort in data exchange, ERM is the only way to secure IP with encryption. In addition to that, protection can be advanced by DLP, which can be used to prevent that unprotected files leave the company.

3.2. Impact of human-related aspects during the IP protection process

As mentioned in section 2, technical measures and methods can be available in one company but beside rules, contracts and guidelines, the mindset of the employee is the deciding factor to protect IP within the data exchange process. In this paper the human-related aspect is based on trust wherein impact of endogenous and exogenous trust is taken under consideration. This paragraph will give a quick overview about ongoing research in the field of trust. There are a couple of definitions with different focuses for the term trust. Many studies on trust under specific conditions were conducted in selected areas, for example social sciences, business administration as well as computer sciences over the last years. This is caused by the fact that trust is deeply entangled with complex personal and interpersonal relation, which essentially impacts economic efficiency in cooperation projects. As a result in product development, there are plenty of research reports concerning "collaborative engineering" touching trust without having the main focus on this aspect (Pander & Wagner, 2005; Heitmann, 2007 and Weissflog, 2005).

There are mainly three different fields of trust which were investigated in the past: finding several of types of trust and define the scope of the terms, developing models of trust and investigating trust empirically in different fields and situations. Basically trust is a well-known concept in everyday life that simplifies many complex processes. Our understanding of trust is mainly based on Luhman's, (1979) perceptions where trust is defined as *"a mechanism to stabilize insecure expectations and helps to reduce the complexity that adheres to an action"*. One advanced general definition of trust is that *"trust is a particular level of the subjective probability with which an agent assesses that*

another agent or group of agents will perform a particular action, both before he can monitor such and in a context in which it affects his own action" (Gambetta, 2000). The main statement of the last definition is that trust is always subjective and includes an element of prediction and expectation (Ries, 2009). Furthermore the definition of trust can be distinguished in reliability and decision trust. Decision trust extends the definition in additionally considering trust in dependence of the situation and about environmental factors and risk (Ries, 2009). In this case uncertainty arises by exogenous conditions, which can adopt four dimensions: trust in organization, trust in people, trust in profitability and trust in relationship between organization respective cooperation. This part of trust can be formalized. However trust is also endogenously influenced through interaction of actors. At least Jarvenpaa et al. summarize that trust is based on the expectation that others behave as anticipated (Jarvenpaa et al., 1998).

4. RESULTS WITHIN THE RESEARCH PROJECTS: CASED AND TRUST

In the beginning of this section, results of the research projects TRUST and CASED separately represented. The research project TRUST –Teamwork in Interorganizational Cooperation. The research project focuses on the influence of organizational, technical, and cultural terms on building trust in interorganizational projects and their impact on the balance between flexibility and stability (for further information www.trust-teamwork.de). The research center CASED was established, which is an internationally important cluster for IT security, located in Darmstadt (for further information www.cased.de).

As an introduction the setting of every research investigation is shortly described. After that results of the investigations are summarized and an intermediate conclusion within both projects is drawn. In section 4.3 the synthesis integrates both points of views to an integrated solution.

4.1. TRUST

To tackle the challenges of trust the application of IT-protection in cooperation an empirical investigation was carried out. In the first research period 44 interviews were conducted in eleven small and medium-sized enterprises (SMEs). We found 12 diverse cooperation types within the interviews. The high number of international cooperation depicts that globalization has an increasing influence on today's working processes. During the interviews the interviewees, working in different fields, e.g. project manager, design engineers, employees from human resources department, business management and work councils, reported about their experiences in cooperation and the relevance of trust in teamwork. The following paragraph summarizes the results of this investigation with focus on IP-protection.

4.1.1. Human-related IP protection in a collaborative project (TRUST intermediate results)

Information and knowledge exchange is the key factor for successful cooperation in product development, because beside interpersonal communication knowledge transfer takes mainly place by the exchange of data. During data exchange the respondents fear that the cooperation partner is often informational brought up on the same page as the own company. Thus on the one hand, the degree on information appoints the success of a project but on the other hand can jeopardize companies' profit. IP-protection is needed, all interviewee confirmed. Hereby the challenge arises to transfer the appropriate degree on information in product development data.

The need to coordinate data exchange and knowledge sharing within cooperation poses a challenge, too. In every participating company product development data is organized on different security levels: confidential, internal and public data. Data that is set "confidential" is usually never exposed to external parties whereas "public" data are accessible by everyone, even for persons not involved in the cooperation. "Internal" data is accessible for companies` employees (Heitmann, 2007). However, there exists a grey area between the levels "confidential", "internal" and "public" data. Data exchange in this area lies at the discretion of the developer which is responsible for successful collaboration with the cooperation partner. At this point, it has to be verified to what extent (e.g. restricted or unrestricted) data may be exchanged respectively accessed at all. What needs to be clarified is the question - concerning a cooperation's general objective - how important the approval of access rights actually is? In other words: At what risk does a company share it's captive business knowledge with other cooperation parties? And at least, how important is the data for reaching the project goal? Companies encounter these problems in the "grey area" by letting employees individually coordinate the data exchange with the cooperation partner. The person responsible will decide about the extent of data exchange solely based on the strength of his past experience and by having trust in the cooperation partner. At this point, a certain level of trust is needed in order to keep up a project. Trust is therefore an inevitable factor that shapes the future development of a cooperation. If the employee approves access to business data that has been manipulated (restricted access), this decision will derive from experiences in the past. Even though formal data exchange rules exist (e.g. on the intranet) and are often communicated in employee trainings, people tend to replace them by practical experiences respective by having trust or mistrust. This is due to the fact that guidelines are too general for individual application, and thus are only helpful to a minimum extent. (Anderl, 2010)

Wherever information in corporate product development data needs to be reduced, deleted or converted in order to protect IP, the selection of knowledge entities is done by hand. As a result a big discussion between the interviewees was launched if the benefit of IP-protection justifies the effort. In the field of modeling data (3D-CAD-models) an automated knowledge reduction technology has not been developed yet. Thus formalized standards that allow the employees to bypass cooperation partners' access to IP could be one way to tackle the challenge of information sharing. But on the one hand fine granular manipulation of knowledge entities within 3D-CAD-models is not technically possible and on the other hand the gist of the interviews show that in fields of IP-measurement application, it means, not to decide once for data exchange regulations but to adapt them depending on the situation. Data exchange always is leaded by win-win situations in product development cooperation. Deep insight in development data may lead to trust but can be shortchanged too.

As a result a comprehensive privilege management, defined by roles and groups does not include the relationship between to cooperation partners as a social factor and its relationship shift. As mentioned before, factors that characterize a cooperation, such as cooperation type, country of origin, or duration can be indicators for trust and allow a better understanding of the cooperation relationship. As shown above, exchanging data systematically strongly depends on the level of trust between cooperation partners at a given point of time.

Particular attention is paid to minimize the risk of data-abuse in cooperation. However what happens with data respectively company's IP after the data has exchanged? Data is mostly saved in the cooperation partners' file system or product data management (PDM) system with the original nomenclature. Thus according to the rights management by the cooperation partner employees have or haven't access to this data. Interviewees pointed out, that it is not unusually to get into a situation where spying on data is possible, either by getting the data from a third party or having insight in the cooperation partners' repository. As a result development data sometimes ends in competitors' hands and can be processed during the CAx-chain.

In general, the survey shows that companies participating in collaborations tend to allow deeper insight into development data and confidential business knowledge than they initially intended to. Rules within cooperations are crucial in collaboration (Weissflog, 2005). This particular form of standardization is supposed to produce stability, transparency, reliability, and trust. But simultaneously, standardization can lead to mistrust. An open and straightforward interaction with rules in cooperation is very important.

4.1.2. Summary

The interviews indicate that trust can adopt various dimensions and there are factors to measure trust as well. After having collaborated several times, once can have a high degree of trust in the cooperation partner within product development projects. This kind of trust is mainly experience-related. For example, the cooperation setting can advance trust too. Difficult to measure is the interpersonal trust within cooperation. Of course, suitable team arrangements based on experience and characters may avoid trouble in teams, but interpersonal trust will always exist in the mind of individuals.

One method to outbalance trust is the use of IT-protection technologies. Within data exchange the application of IT-security may help stabilizing trust in teamwork that nobody is profiting by anyone's IP. The other way around trust can help simplifying complex teamwork structures and advance project efficiency. In that context, trust is the leading factor. In a joint project build on trust all data exchange may be handled easily. In general, trust and IT protection technologies may coexist in cooperation. However, many external circumstances have to be taken into account to measure the amount of trust like the degree of dispersion of the cooperation partners, the repetition level and experiences of forehand cooperation, the profit of the cooperation and – very important - individuals involved. When there is a lower level of trust within a joint project, IP protection may be necessary.

4.2. CASED

In this section, results are presented from CASED in specific of the subproject Information Rights Management (IRM). The research focuses on the protection of IP in product development within CAx processes. The IRM subproject has two main objectives, analyze the quality of ongoing IP protection and IP security methods, and to propose a new solution for IP security.

4.2.1. Analysis of technical aspect of IP security in current ERM systems

To achieve maximum protection for a company's intellectual property, an ERM solution has to provide protection for all critical data generated during the development process, which includes office documents, sketches in image formats and also product data saved in CAD files. Previous studies (Mullingan et al., 2003 and Arnab & Hutchison, 2008) generally evaluate ERM systems focusing on different requirements, but an investigation of IP-protection within CAD data has not been realized yet.

The requirements used to evaluate the technical solutions in this paper are based on the Secure Product Creation Processes Project Group (SP²) from ProSTEP iViP, (2008). In this project a study has been carried out to identify requirements within ERM systems in the automotive industry. The six companies which has been participated the project group are listed in Fig. 5. In general, the group identified 82 ERM requirements. However this paper focuses on IP protection within CAD data. Thus only 42 requirements (Henriques et al., 2010) are covered by this paper, which are classified into the six following categories (see also Fig. 5).

Right Expressivity: This category includes requirements relating to the effectiveness with which rights can be defined – especially the extent of the possible access data restriction.
Format/Application Support: In this category the most important applications and file formats are defined that should be supported by / or being compatible with the ERM system.
Integration & Interoperability: This defines the requirements relating to the integration and interoperability of ERM systems in the companies. For example, the implementation of an ERM solution into a company's IT environment should be easy and fast, it should support different external certificates and it should run in batch and bulk processes.
Functionality: Within this category, the requirements regarding the functionality of an ERM solution are defined, such as functions to grant and deny access permissions to a specific content, the ability to check user rights online every time when a protected file is being accessed or the function to allow a user work offline for a specific time.
Usability: This category defines usability requirements of an ERM solution, for example rights should be assigned simply and efficiently and there should be the possibility of applying the rights automatically.
Organizational: This category describes the organizational requirements including the needed infrastructure in order to allow external users access on the ERM system for authentication, support for different software versions and revisions and firewall compatibility of the system, to name but a few.

In order to analyze the ERM systems, a test scenario was defined and an environment of infrastructure, architecture, scenario, model and polices was set up to simulate a typical automotive collaborative engineering environment containing OEM and supplier domains (Henriques et al., 2010). The test scenario included the generation, the protection and the storage of CAD data on OEM's file server, respectively sent via e-mail to outside located suppliers. According to the requirements listed above, the receivers (employees of OEM or a supplier) evaluate the ERM functions by using test-CAD-files. Several tests were performed to verify the security of the ERM functions (e.g. open the file, attempt to edit it, attempt to open the file after its offline time has expired, and many more) in securing IP. The results of the tests were categorized in three levels:

Full support: The system fully meets the requirement
Limited support: The requirement is met partially
No support: The system doesn't meet the requirement

The results of the evaluation are presented in Fig. 5. It illustrates that the tested ERM systems only fully cover 17% of the requirements, 47% partially and 36% not at all. Both ERM systems show the same behavior regarding the requirements so that the results of the evaluation are described together.

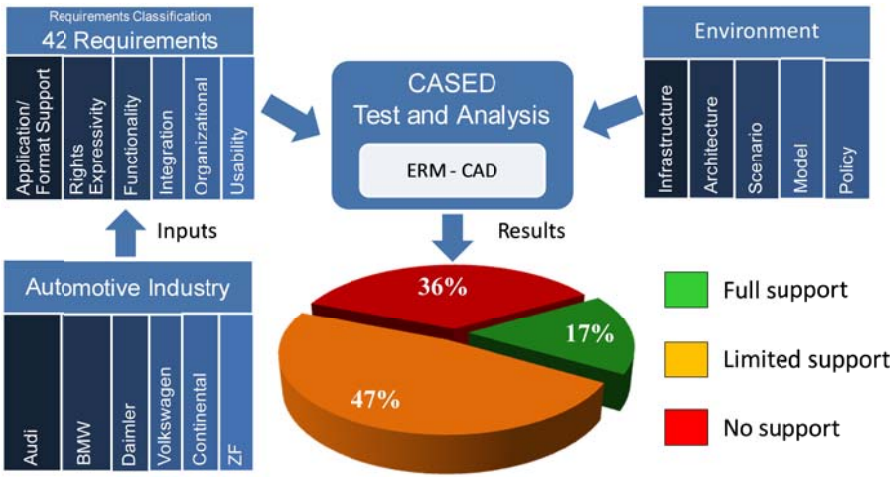

Figure 5. Result of technical aspect analysis of current ERM systems

In summary, it can be stated that both releases didn't meet the requirements of the automotive industry concerning IP protection. For future development, the most important improvement must be support interoperability between the

different system releases. At least backward compatibility of the newer ERM software releases is expected by industry. In addition to that, another important task is to refine the read-only permission which had issues so users could still modify the secured file. Moreover group and template based access permissions centrally manageable through the rights server need to be developed for future releases to improve usability and enable rights expressivity and mainly organizational reasons. Even the basic rights permissions on the file level are fully implemented, the systems will not be able to completely secure IP in the part. Therefore, future developments must focus on extending the ERM functionality to a fine granular level in order to achieve reliable IP protection.

4.2.2. New approach to protect intellectual property in product development process

As described above, both analyzed ERM systems work on file level and do not provide granular IP protection yet, because this is a relatively new technology (Dassault, 2007). This paper presents a new concept that combines ERM and data filtering methods in an advanced method – Engineering Rights Management (EngRM) of CAD data. This concept bundles the advantages of both technologies and moderates the disadvantages (see Fig. 6). EngRM is primarily based on ERM methods but is extended by the ability to granularly protect IP entities by using CAD-data filtering methodology. First, the entire IP in CAD files has to be structured by its type of knowledge in a fine granular way and finally, secured by ERM encryption. The technical approach for structuring knowledge entities data filtering methods to trace and identify different types of IP is used. But which rules follows the structuring process?

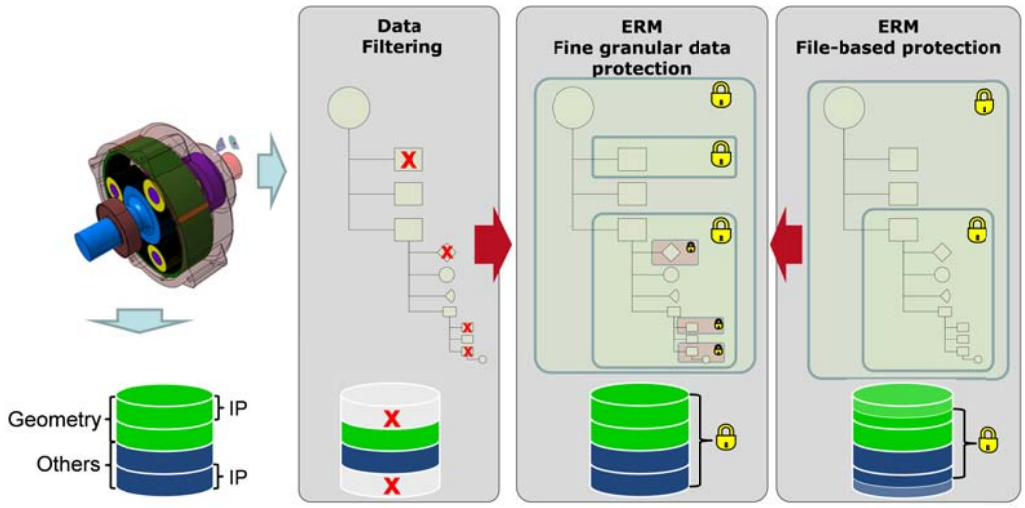

Figure 6. Concept for an ERM solution for fine granular protection in 3D CAD data

4.3. Synthesis

The synthesis of both, the technical and the human-related approach is illustrated in Fig. 7. One goes hand in hand with each other in building a common secure data exchange process.
In practice it is almost impossible to guarantee such high level of trust in a cooperation that involves a very large number of individuals and companies like in the automotive sector (Fig. 1). For this reason the technical approach is necessary in order to increase the IP protection in the cooperation between companies. Concerning the ERM systems analysis and the new concept proposal, it was important:

- To evaluate in what extent the automotive industry requirements are provided by current ERM systems
- to give feedback to the ERM solution developers
- to develop a new approach to protect IP in the collaborative product development process which improves the protection to an entity level.

One main key point of the interviews was that trust and the application of technical measures always coexist. However, a positive mindset towards cooperation or, in other words, having trust has the big advantage to reduce complexity in teamwork leading to less application of technical approaches to protect IP. But how can we steer trust or mistrust in cooperation? There are several basic conditions that either strengthen a trustfull cooperation or leading to mistrust and cooperation failure.
Concept to evaluate the trustworthiness of a cooperation environment:

- ***The cooperation setting:***

In times of flexibility the cooperation setting can stabilize the cooperation. Cooperation partner's cultural diversity, the dispersion degree and the time shift between the cooperation partners as well are obvious factors. The business competition between the cooperation partners is an additional factor which should be taken into account. However these factors can't be changed, but improvements of interfaces and processes in cooperation, a strict assignment of responsibilities and the division of work are impacts lying in the hand of cooperation initiators.

- ***The story behind the cooperation:***
  Additionally the experience of forehand cooperation is a crucial point to evaluate the trustworthiness of a cooperation environment. This can be integrated in using case based reasoning method in the evaluation process.
- ***The trustworthiness of the cooperation partner:***
  The evaluation of cooperation partners' trustworthiness can be solved reputation based. A social ranking depict results of estimations among each other's work and reliability.
- ***The relationship between individuals:***
  This factor is most difficult to measure. Trust that is based on the relationship is often leaded by the mindset of individuals. On the one hand this is also influenced by experience of forehand collaboration but on the other hand it is just a stance on each other, in good terms spirit.

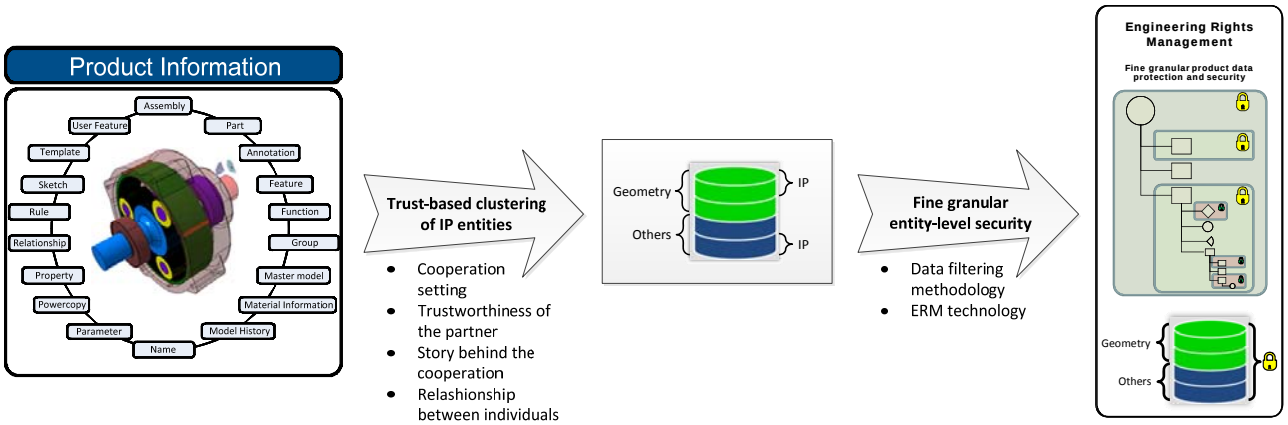

Figure 7. Product information entities clustering and securing

These factors can enhance trust-based clustering of IP entities. Of course the extension of these conditions has to be measured and validated in practice. One approach to evaluate the findings within the interviews has already been initiated by the online questionnaire, which will give quantified results and will find interdependencies and correlation between these dimensions. In the end the results should lead to a trust-based clustering of IP entities from a trust based point of view. The results of trust based clustering should be implemented in the process of fine granular security of entities.

5. CONCLUSION

IP protection is a process of application IP protection technologies. In that context, trust is the determining factor. In an environment of trust, IP protection measures may only play a minor role - although, that may not be necessarily be the case. An open approach to measures of IP protection may clearly promote mutual trust. However, such a substantial amount of trust may not be appropriate within some joint projects. Many external circumstances have to be taken into account like the degree of dispersion, duration of cooperation, repetition level, and individuals involved. When there is a lower level of trust within a joint project, measures of IP protection may be applicable in a granular way of protecting IP.

A technical analysis of ERM-systems shows that two ongoing ERM-systems do not fulfill the requirement to granularly protect IP entities within CAD-files. This would be a great step forward in IP-protection processes in practice, especially for the automotive industry. This paper discusses two new concepts in IP-protection. On the one hand the new technical approach to granularly protect IP entities in CAD-data in using ongoing ERM and Data filtering methods and on the other hand the integration of the human-related aspect trust within the IP exchange process providing rules for the structuring process of IP in CAD-files.

In the end, the implementation of this solution would improve IP protection in the automotive industry collaborative product development especially in CAx-processes.

6. ACKNOLEDGEMENTS

The work described in this paper has been funded by CASED Center for Advanced Security Research Darmstadt (www.cased.de) supported by the Federal State of Hessen, Germany, through the LOEWE program and by the Research project TRUST financed by the BMBF (Federal Ministry of Education and Research) and the ESF (European Social Fund).

7. REFERENCES

Anderl, R., Völz, D. and Spieß, D.; Schilcher, C.; Petendra, B., 2010: A multidisciplinary research on Trust in interorganizational virtual product development. In: Tools and Methods of Competitive Engineering. Faculty of Industrial Design Engineering, Delft University of Technology, Eurotech, Ancona, Italy.

Arnab, A., Hutchison, A., 2008, An Evaluation Framework for DRM. Proceedings of the 6th International Workshop for Technical, Economic and Legal Aspects of Business Model for Virtual Goods incorporating The 4th International ORDL Workshop. October 16-18, 2008, Poznan, Poland/ ed by Rüdiger Grimm and Susanne Guth, Poznan University of economics publishing house. Poznan, Poland, pp 176-199. ISBN 978-83-7417-361-2, 2008.

Corporate Trust, 2007, Industriespionage: Die Schäden durch Spionage in der deutschen Wirtschaft. <http://www.corporate-trust.de/pdf/STUDIE_191107.pdf>. Accessed on 3 Dez. 2010.

Dassault Systèmes, 2007, Dassault Systèmes bringt Version 5 Release 18 seines Product Lifecycle Management (PLM) Portfolios auf den Markt (Dassault Systèmes Announces Version 5 Release 18 of PLM Portfolio), news item, Paris, France, <http://www.3dsevents.de/download/071015_V5R18_final.pdf>. Accessed on 3 Dez. 2010.

Gambetta, D., 2000, Can we Trust Trust? In Diego Gambetta, editor, Trust: Making and Breaking Cooperative Relations, electronic edition, chapter 13, pages 213-237.

Heitmann, M., 2007, IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie, Wiesbaden, GWV Fachverlage GmbH, Zugleich Dissertation Bochum

Henriques, J. R., Anderl, R. and Grimm, M., 2010, Analysis of Enterprise Rights Management solutions for CAD data according to the requirements of the automotive industry and a proposal to increase the ERM security level. In: Proceedings of ASME 2010 International Mechanical Engineering Congress & Exposition.

Jarvenpaa, S. L., Knoll, K. and Leidner D. E., 1998, Is Anybody Out There? Antecedents of Trust in Global Virtual Teams. In: Journal of Management Information Systems, Springer, Vol. 14, No. 4, pp. 29-64.

Luhmann, N., 1979, Trust and Power. Wiley, Chichester

Mullingan, D., Han, J., Burstein, A, 2003, How DRM based content delivery system disrupt expectations of “personal use”. Proceedings of the 2003 ACM workshop in Digital Rights Management, ACM, pp. 77-89.

Pander, S.; Wagner, R., 2005, Unternehmensübergreifenden Zusammenarbeit in der Automobilentwicklung – durch erfahrungsgeleitete Kooperation die Grenzen der Planbarkeit überwinden. München/Mering, Heiner Hampp Verlag.

ProSTEP iViP, 2008, Secure Product Creation Processes (SP2), White Paper, ProSTEP iVip. <http://www.prostep.org/en/medialibrary/publications/white-paper-studies.html#c1079>. Accessed on 3 Dez. 2010.

Ries, S., 2009, Trust in Ubiquitos Computing, Dissertation Informatik TU Darmstadt. Online publication.

VDMA, 2010, VDMA-Umfrage zur Produkt- und Markenpiraterie, <http://www.vdma.org/wps/portal/Home/de/Branchen/P/PKS/PKS_A20100416_Umfrage>. Accessed on 3 Dez. 2010.

Weissflog, U., 2005, Bestimmen oder Gestalten? Möglichkeiten zur Organisation von Wissensarbeit im Unternehmen, Korbach, Arrangement-Verlag.

8. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.