Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 16 (2013) 571 – 580

Procedia Computer Science

Conference on Systems Engineering Research (CSER'13)
Eds.: C.J.J. Paredis, C. Bishop, D. Bodner, Georgia Institute of Technology, Atlanta, GA, March 19-22, 2013.

Intellectual Property Protection and Secure Knowledge Management in Collaborative Systems Engineering

Marco Grimm[a,]*, Reiner Anderl[a]

[a] *Technische Universität Darmstadt - Department of Computer Integrated Design, Petersenstraße 30, 64287 Darmstadt, Germany*

Abstract

Developing complex systems with the Systems Engineering approach requires a close collaboration between engineers. Today, this collaboration is often globalized and performed beyond enterprise boundaries. In order to maximize the engineering outcome and manageability, it is necessary to share and transfer engineering knowledge and intellectual property in a digital form. Knowledge is valuable and easy to copy hence it is often subject to intended theft or loss. This leads to substantial economic damages worldwide due to product piracy and plagiarism. The goal conflict between a wide availability of knowledge to system engineers and a secure management and usage of intellectual property is still unsolved. Legal and organizational measures, such as nondisclosure agreements and facility surveillance, are insufficient to solve the problem alone. Therefore industrial companies demand for new measures that effectively protect their intellectual property.

This paper presents an analysis of current technical approaches that are applicable on securing knowledge in collaborative Systems Engineering. It shows that all approaches do not sufficiently cover the industry's knowledge security requirements. Hence a new knowledge security concept is introduced. It covers the specific requirements and constraints in the Systems Engineering context and provides a knowledge security improvement over the current technical approaches.

Selection and/or peer-review under responsibility of Georgia Institute of Technology

Keywords: Intellectual Property Protection; IPP; Knowledge Management; IT-Security; Knowledge Protection; Knowledge Security; Knowledge Based Engineering; KBE; Systems Engineering; Enterprise Rights Management

1. Introduction

Successful realization of complex and innovative systems requires systems thinking, decision-making competency, team-orientation and specialist expertise. System complexity is not only expressed by volume of work but also by multidisciplinarity of the engineering task. In Systems Engineering, knowledge and competencies of various engineering disciplines and involved stakeholders are combined so that synergies establish and broader and

* Corresponding author. Tel.: +49-6151-16-75176; fax: +49-6151-16-6854.
E-mail address: grimm@dik.tu-darmstadt.de.

Selection and/or peer-review under responsibility of Georgia Institute of Technology
doi:10.1016/j.procs.2013.01.060

better solution spectra are created [1]. Knowledge sharing and exchange between involved parties is essential for a successful accomplishment of the engineering task. Globalized markets as well as increasing cost and innovation pressure lead to heterogeneous, distributed engineering environments, which require intense knowledge exchange via Internet communication across enterprise boundaries. In this regard, protection of innovative knowledge and intellectual property (IP) plays a decisive role because corporate knowledge is crucial for economic success and competitiveness of enterprises. Moreover, knowledge theft and plagiarism result in substantial economic losses and damages to a company's public image [2].

Knowledge-intense product data created and utilized in Systems Engineering is particularly at risk, because many different stakeholders access sensitive content. Strong access restrictions are not always advantageous because cooperation between participants is interfered as well as ability and efficiency of the Systems Engineering thought is compromised. In the area of conflict between knowledge provision and knowledge protection, industrial enterprises demand appropriate protection means that solve the problem. Practice shows that, until now, organizational and juridical protection means are not capable of solving the goal conflict and the piracy and plagiarism situation alone. Hence, over the past years, industry demands concentrate particularly on technical protection means.

This paper picks up this challenging problem and provides a comprehensive analysis of the most important technical protection means for product data with regard to their application in Systems Engineering. The analysis presents an estimation on how the evaluated technical protection means perform relating to criteria relevant in Systems Engineering. Based on these results, a concept is presented that contributes to the design of a knowledge protection system particularly adapted to the specific requirements in Systems Engineering projects.

Section 2 of the paper provides a classification of the related protection means and categories. Sec. 3 describes the definition of requirements, testing infrastructure and use case for the analysis and discusses the results. Sec. 4 introduces the proposed concept that is based on the analysis results. Finally, sec. 5 concludes the paper.

2. Background

2.1. Knowledge protection means and classification

Protecting valuable knowledge and intellectual property of companies is assisted by various existing protection means. These can be distinguished in different categories depending on their type of utilization and implementation into corporate processes and infrastructure.

Fig. 1 presents an overview of the different categories and corresponding examples. It highlights technical data protection means with preemptive concepts that are the focus of this paper.

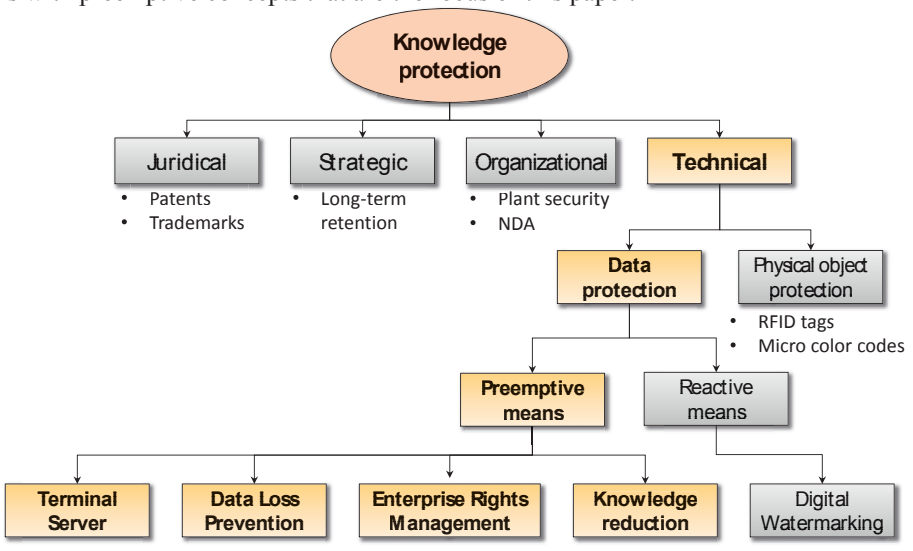

Fig. 1. Knowledge protection categories, paper focus is colored

Juridical protection means, such as patents, copyright or trademarks are well-established instruments to protect own intellectual property. They set a legal framework for the utilization of protected knowledge and enable the copyright owner to pursue economic interests by civil law in case of illegitimate plagiarism or piracy. Juridical protection means are not suitable for preemptive knowledge protection because they do not actively prevent knowledge from being stolen or misused. In addition to that, they can be circumvented and even legitimate actions for injunction or compensation often take a long time [3].

Strategic protection means are targeted at controlling knowledge and knowledge bearer in context of a long-term company strategy. This includes retention of any stakeholder that is directly or indirectly involved with company's own knowledge. Usual means in this category are long-term retention of partner firms or suppliers as well as own employees, that act as implicit knowledge bearers [4].

Organizational protection means are means that are used to protect knowledge in a preventive manner. These methods focus on controlling behavior of personnel accessing knowledge inside and outside the company. Typical examples for this kind of measures are: Spatial separation of company departments, video surveillance, personnel identification, physical access controls and non-disclosure agreements (NDA). This category of means has a direct and wide impact on corporate environments and collaboration experience. Protection efficiency, implementation cost and reasonability have to be examined on an individual basis and under consideration of legal aspects [5].

Technical protection means are designed to provide protection of knowledge in physical objects or product and engineering data.

Physical objects such as prototypes or complete products contain and represent knowledge in a materialized form, which can be protected by obfuscation methods (disguised prototype cars), copy-protection methods (high functional integration, software copy protection) and design methods (specialized manufacturing process, surface technology). In addition to that, different identification technologies, such as radio-frequency identification tags (RFID tags), bar codes, micro color-codes, can be used to tackle plagiarism, piracy and loss of knowledge in cooperation and supply chains [6].

Digital product data can be protected by using methods that influence the processing of data, manipulate data or use IT security techniques. This sub-category can be divided into reactive and preemptive protection methods. Digital Watermarking is designed for reactive protection and can be used for identifying where data loss occurred or who forwarded sensitive content [7].

The most important preemptive methods are: Terminal Server (TS) connection, Data Leakage Prevention (DLP), Data Filtering (DF) and Enterprise Rights Management (ERM). Fig. 2 presents a schematic overview of how they work in exchange between home and remote side.

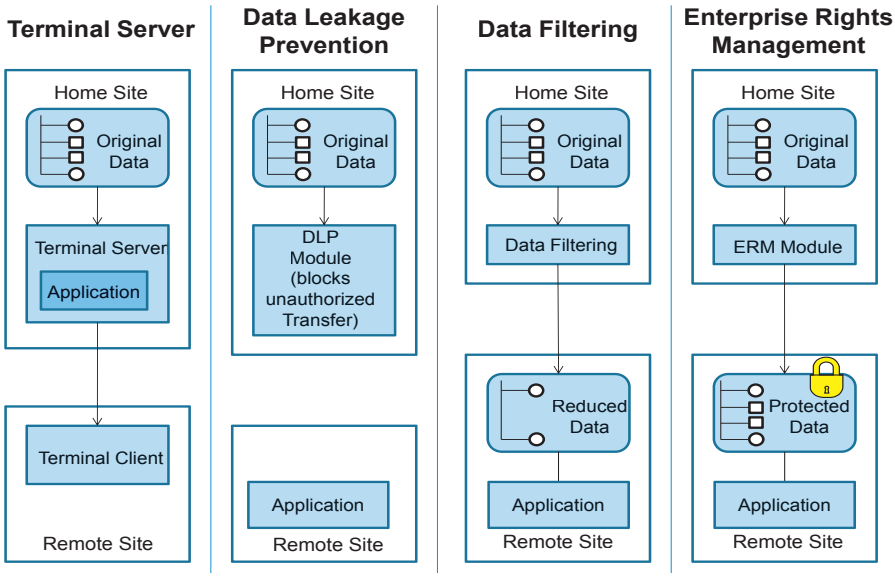

Fig. 2. Methods to protect digital product data - schematic view of operation [8]

2.2. Technical knowledge protection means for product data

Terminal Server is an application that receives user inputs and transmits graphical user interface output via a network connection. The engineer connects to the server and works remotely on the provided environment. Advantages of this method are scalability and central manageability of the server. On the other hand, compared to workstation usage, performance limitations exist when running graphically intensive tasks, such as 3D CAD [9].

Data Leakage Prevention monitors data and controls distribution ways in the system. DLP systems are implemented at host or network level. The DLP module controls any possible data channel and restricts accordingly. Examples for controlled channels are removable storage media, network file transfers, e-mail attachments, printers, etc. Many different DLP systems are available that suit corporate data protection requirements and allow permanent detailed tracking of information and user activities. However, due to the latter, utilization may be problematic in respect to employee data privacy regulations.

Data Filtering is the most important engineering knowledge protection approach that is based on knowledge reduction principles. Individual elements containing valuable knowledge are intentionally removed from documents before these documents are exchanged. Hence, the overall knowledge amount stored in specific documents is decreased to minimize risk of knowledge loss. Prior to removing parts of documents, knowledge containing elements have to be identified and classified first. Examples are removal of confidential parts in documents (e.g. pages, pictures and tables), feature or part information in CAD files (user defined functions, sketches, equations, parameters) or product data information (assembly plans, bill of materials, manufacturing information and material composition) [10].

In addition to Data Filtering, other CAD data focused knowledge reduction methods exist, such as geometric manipulation, model tessellation and exportation to exchange formats (e.g. STEP, IGES). These approaches (partly) transform feature-based or parameterized models into more primitive geometric models with decreased knowledge content [11]. As these methods only process geometry, they are less flexible compared to Data Filtering.

Enterprise Rights Management is an approach based on data encryption and usage control mechanisms. A typical ERM infrastructure consists of a rights server and clients. The rights server manages usage policies and user identities. Furthermore, it provides cryptographic keys to authorized clients, which request access to specific content. Installed ERM software decrypts the protected content in trusted end-user applications on the client and enforces the permission policy assigned to the particular user [12]. Unauthorized users will not be provided with the required decryption keys and protected content cannot be accessed. Centralized permission management and policy enforcement directly in end-user applications distinguish ERM from regular cryptography protection, such as encrypted container and electronic vault solutions, in which these functionalities are missing [13].

3. Analysis

The different technical protection methods that have been described in the previous section are commonly used in data exchange in collaborative product development. However, modern Systems Engineering is characterized by heterogeneous engineering environments and cross-enterprise collaboration settings. This leads to new specific requirements and higher demands on protection methods. In order to verify and evaluate applicability and efficiency of different state of the art technical protection means in Systems Engineering, an analysis was performed in a typical environment and collaboration process.

3.1. Analysis setup

In order to perform the analysis, different prerequisites were necessary. Firstly, qualitative evaluation criteria were formulated to assess and compare the strengths and weaknesses of the different protection approaches. Secondly, a simulated corporate environment was set up in a special laboratory in which investigations took place. Lastly, a typical Systems Engineering collaboration scenario in terms of a practical use case was composed. This use case sets the process framework for the analysis.

3.1.1. Evaluation criteria

Industrial companies that want to protect their intellectual property in engineering collaborations have different

requirements and criteria regarding the application of protection means. Fulfillment of these criteria is one of the main success factors for a successful introduction of technical protection means. However, specific requirements often vary, as collaboration use cases and processes depend on industrial sector and existing corporate infrastructures and environments. To cover a typical Systems Engineering scenario, criteria were formulated from a range of requirements defined by German automotive manufacturers participating in Secure Product Creation Processes (SP²) and ERM.Open working groups of ProSTEP iViP Association (http://prostep.org).

The evaluation is focused on following formal criteria:

- Usability of protection means
- Effectiveness of knowledge protection
- Process efficiency in collaboration

Usability covers seamless integration of protection measures into the end-user workspace and application. It is important that the end-user, who creates or consumes protected content is not distracted or disturbed by protection functions and working with protected data or in protected environments does not slow down the actual engineering work. Users have to actively support application of technical protection means. This support is generally based on two main factors: Users need to be aware that knowledge is valuable so they realize the importance of protecting it and at the same time, acceptance of protection processes is required. In addition to that, protection means only work efficiently if they are easily managed. If users need to address themselves to complex and inconvenient protection tasks, acceptance is decreased and provided protection guidelines are not carefully utilized any longer.

Effectiveness of a protection measure is a degree for the level of security it provides to specific content. A high protection level means that system and process are strong against intrusion attempts, exploits or breaches and are able to preserve security of protected content during its whole lifecycle. Negative examples for low protection levels are short encryption keys and weak passwords, unencrypted internet communication and protected documents that can be manually exported into unprotected documents. For evaluating effectiveness, the current state of the art regarding Information Technology always has to be taken into account. Methods offering high security today may be broken in some years (e.g. cryptosystems) hence evolution of those protection techniques with general progress in IT is essential. In this context, strong knowledge protection over long periods of time, e.g. in long-term archiving and retrieval, is an open issue, but is not covered in this paper.

Process efficiency of protection methods in collaboration implies that protected content can be processed in the same way as unprotected content. It is important that utilization of protection measures does not decrease collaboration flexibility. Protection methods have to be adaptable, e.g. if personal changes in a project take place. A transparent integration of the protection process into actual collaboration would be optimal, so management of protection processes can be offloaded to the corporate knowledge management. Furthermore, security holes and inconsistencies arise when engineers need to follow different processes, depending on whether protected or unprotected content is treated.

3.1.2. Evaluation environment

The evaluation was conducted at a specially set up IT environment at the Center of Advanced Security Research Darmstadt (CASED), Germany (http://cased.de). The testing environment is presented in Fig. 3.

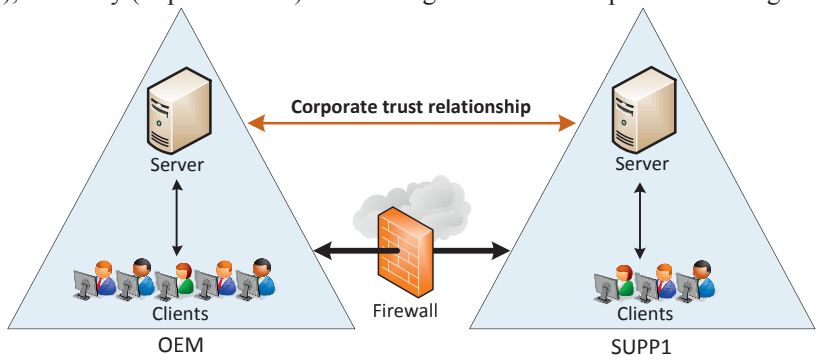

Fig. 3. Overview of IT environment used for the analysis

It simulates a productive corporate environment, which consists of a typical server-client infrastructure with Ethernet connectivity. Servers that provide engineers with the required services are running virtualized instances of Microsoft Windows Server 2008 R2. A company domain OEM (original equipment manufacturer) and a secondary domain SUPP1 (supplier) are controlled by two domain controllers (DC), which are separated by a Netfilter Iptables firewall. Both controllers run separate user directories (based on Microsoft Active Directory) and share a project-bound two-way trust relationship. Each DC deploys services and settings depending on which organization unit or role a specific user is assigned to. Users use their personal credentials (account/user name, password) to log into the system [14].

3.1.3. Evaluation use case

The analysis use case covers a simple collaboration process between OEM and suppliers SUPP1+2. Project target is the development of an Electronic Stability Program (ESP) enabled brake system. OEM acts as main developer of mechanical brake system parts and cooperates with its two suppliers, one electronics supplier (SUPP1) and one software supplier (SUPP2). All three create a network to solve the engineering task together by combining their specific expertise from different fields into a unified engineering effort.

Each company has several internal stakeholders involved in cooperation and assigns them to the project in respect to their specific roles and functions. These people are in charge of system development and corresponding data exchange. Fig. 4 illustrates the most important roles of specific employees in the different companies and how they interact with others, both inside and outside their company. Blue arrows show the information exchange between expert teams and systems engineer, red arrows indicate the data exchange in component development.

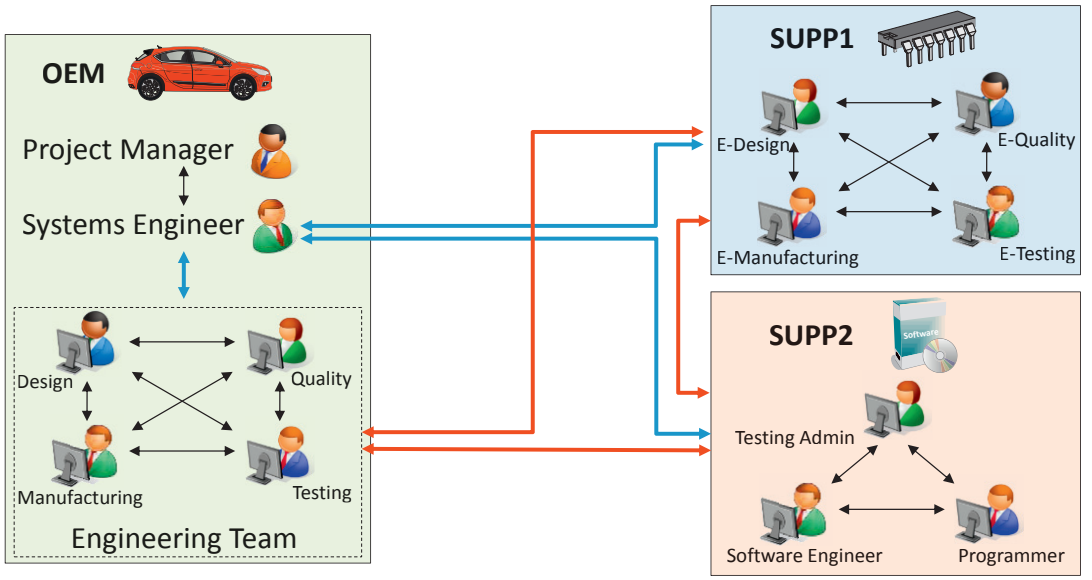

Fig. 4. Stakeholder view of the engineering setting

The types of knowledge that are to be protected during data exchange are presented in Fig. 5. OEM's IP generally consists of design and manufacturing knowledge of mechanical brake components and peripherals. SUPP1's IP worth protecting is knowledge of electric circuit and silicon design for brake control hardware. SUPP2 has software knowledge, such as proprietary code, compiler and algorithms that should not leave the company.

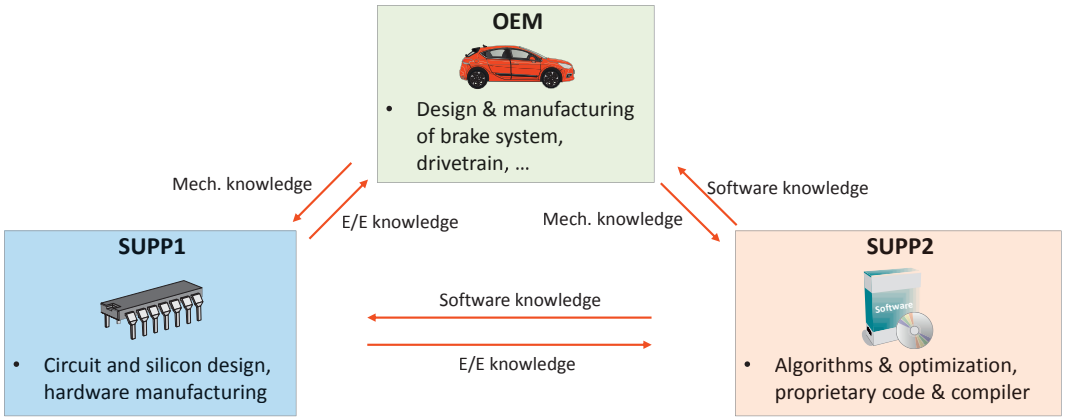

Fig. 5. Knowledge view of the engineering setting

In order to simplify the evaluation, the corporate environment is reduced to data exchange processes between OEM and SUPP1. Further multidirectional data exchange and protection scenarios between OEM and SUPP2, between SUPP1 and SUPP2 and between others, such as second tier suppliers and subcontractors, exist in reality. However, they are not considered for the evaluation in this paper.

Based on the stakeholder and knowledge view, the detailed use case is defined as follows: Collaboration takes place by exchanging data. This data exchange is done by transferring digital content over the network. Digital content can either be stored locally or at the remote site in the form of files. These files represent digital documents in different formats. Knowledge and intellectual property, which is classified as confidential is part of the files. Collaboration partners want to restrict access to confidential content as much as possible but allow access to all specific content required by the other party. The target is to utilize protection methods to effectively prevent data theft, forwarding of documents to third parties and unauthorized access.

Fig. 6 clarifies what data is exchanged between OEM and SUPP1. OEM shares various system requirements specifications in textual/table form, as well as brake and actuator design documents with the corresponding simulation data in 3D CAD. SUPP1 provides interfacing requirements data of the supplied electronic components in textual/table form, geometric data of the electric components in 3D CAD format and simulation data in form of MATLAB/Simulink plots exported to PDF files.

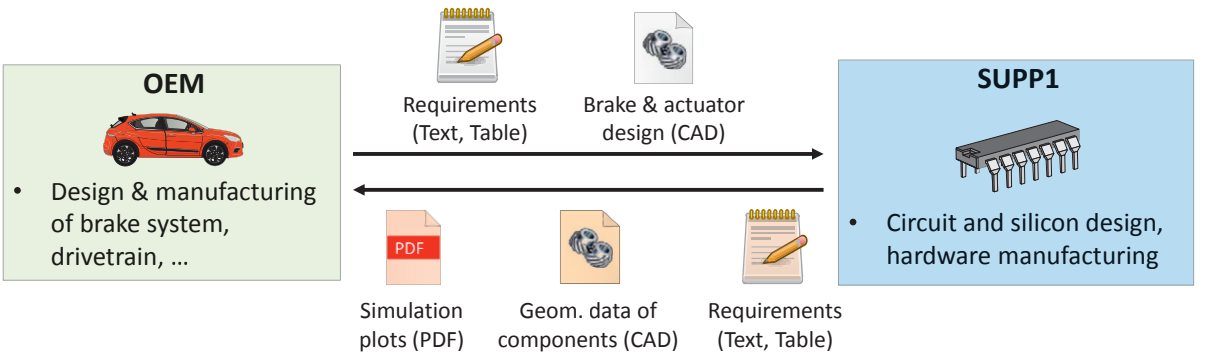

Fig. 6. Evaluation use case – data exchange between OEM and SUPP1

3.2. Results

Table 1 provides an overview of how the analyzed knowledge protection methods performed in the described collaboration use case. The single ratings refer to the formal criteria presented in section 3.1.1.

Table 1. Evaluation results overview (arrows show ratings with tendencies in the respective criteria; up = good, down = bad)

Protection measure	Usability	Protection effectiveness	Process efficiency
Terminal Server	↘	↓	↓
Data Leakage Prevention	↗	↓	↓
Geometric manipulation (CAD)	↘	↑	↘
Data Filtering	↘	↑	↘
Enterprise Rights Management	↗	↑	↑

Terminal Servers performed worst in the scenario. OEM users remotely connect to SUPP1's server (and vice versa) to work in a provided guest workspace. Specific knowledge embedded in documents is not protected as the terminal session alone cannot distinguish between confidential and non-confidential content. Own software and functions, especially important for CAD data, are not integrated at the remote side and cannot be used. Network bandwidth limitations lead to slow work in CAD data exchange. Overall data exchange is limited to viewing content because remote data cannot be transferred in a protected form. Reintegration of processed data requires redundant work at both systems.

Data Leakage Prevention modules transparently integrate into user workspace. However, some legitimate data exchange attempts were blocked. Users get distracted by permission error messages. In some cases, DLP does not recognize protected content (e.g. when stored in compressed or password-protected archives) so protection was bypassed. Data itself is not protected by DLP, only distribution is controlled. Users were restricted to exchange information via permitted channels only, which makes them lose much flexibility in the collaboration process.

Geometric manipulation applies on CAD data exchange only. Manipulation features need to be applied and reviewed for each CAD model prior to exchange. That was a complex and time consuming task, especially when assemblies were manipulated. However, manipulated documents do not longer carry design knowledge (features, parameters, etc. are entirely removed), so protection is strong. On the other hand, once manipulated, the CAD file becomes useless for the own company. In scenarios where SUPP1 made model changes or added annotations and suggestions, OEM engineers had to manually reintegrate all these alterations to the internal, full-featured model. In some cases, model changes were not possible due to removed parameterization. Regarding the process efficiency aspect, duplication and management of redundant content was very inefficient in the given use case.

Data filtering performed similar to geometric manipulation. However, it is not limited to CAD files. During CAD data exchange, partly automated knowledge reduction based on predefined rules support users when removing knowledge and leads to a better usability compared to geometry manipulation. Manual filtering of the requirement lists and plot files was a time consuming and error-prone process. Like with geometric manipulation, once knowledge is removed, filtered documents can be securely distributed. In the process aspect, data filtering performed as bad as geometric manipulation. Duplicated documents (filtered and unfiltered) and required reintegration processes are very disturbing and inexpedient in collaborations.

Enterprise Rights Management performed best in the analysis. Protection functions are directly integrated into the end-user application but need to be manually managed and utilized by the document creator. Engineers do not need to take care of additional steps during work with protected documents. Therefore, using and modifying ERM-protected documents works the same as with unprotected documents. All analyzed ERM systems used state of the art cryptosystems with long keys and provided a high technical knowledge protection level. Personal access permissions need to be assigned by the document owner. Assignment of rights requires E-Mail addresses of specific users that are supposed to gain access to the ERM-protected content. However, user authentication and permission management are not standardized between different solutions. OEM and SUPP1 need to use the same ERM system or exchange user credentials before content can be used at either side.

4. Concept

As discussed, Enterprise Rights Management offers strong knowledge protection, good usability and high

efficiency in data exchange processes during Systems Engineering collaboration. Based on information gained in the practical analysis, usage of ERM provides many benefits compared to other protection means. However, the fact that personal access permissions have to be manually assigned and administered is a major problem. In large-scale projects that are much more complex than the presented use case, management of rights policies and user credentials is a challenging, if not infeasible task. To enhance the capabilities of ERM for Systems Engineering collaboration, a new concept is proposed. It is schematically presented in Fig. 7.

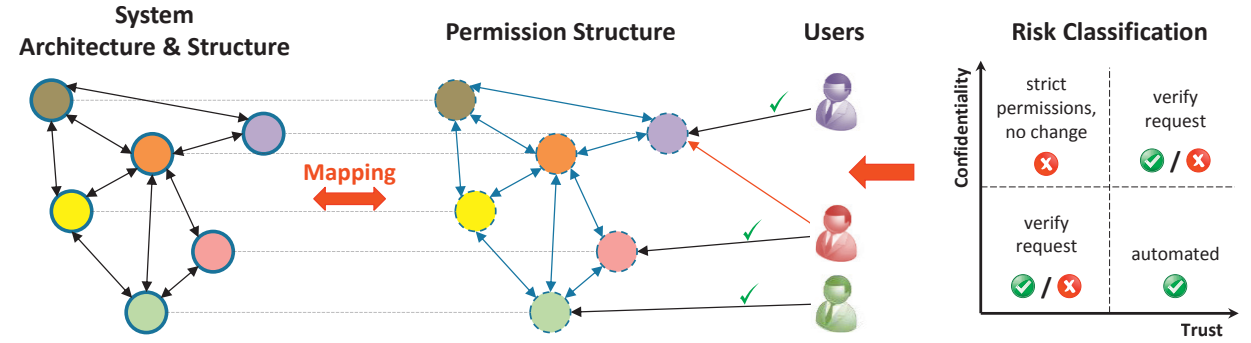

Fig. 7. Schematic view of proposed concept

Instead of using individual access permissions manually assigned to users, the top-down structure and architecture view of the system is mapped to access permissions. Relation and collaboration changes during system synthesis and component development directly apply to the permission structure. Permissions are dynamically linked to logical organization units and user roles in respect to the project structure, so engineers are not required to manually assign personal identities to documents any longer. For data exchange in collaboration, partners and suppliers are included in the system permission structure in respect to their specific roles and in which specific sub-projects and components they are involved.

Furthermore, assignment of permissions builds on trust relationships [15]. Users and content are classified according to trustworthiness and confidentiality. This risk classification supports decision making when rolling out and changing individual permissions. Results of the classification, hence system inputs can be:

- Automated expansion of rights to other sub-project content is allowed (high trust, low confidentiality = low risk)
- request must be verified and decision making on an individual basis is required (low trust, low confidentiality or high trust, high confidentiality = medium risk)
- no changes are made and strict permissions are kept (low trust, high confidentiality = high risk).

These two elements allow the extended ERM system to abandon static permission policies, which are hard to manage in large projects. Dynamic, mapped permission structures offer more versatile policies that are easier to manage. The assessment of risk factors allows an automated customization of access policies on one hand and support confidentiality classification of specific data in critical project structures.

As future work, it is planned to implement the concept into a detailed data model in the next step. Based on this model, ERM system extensions will be implemented and deployed in the testing environment described in this paper. This implementation will then be used to evaluate the concept in practice.

5. Conclusion

This paper presents a practical analysis of different technical knowledge protection approaches applicable in Systems Engineering collaborations. The analysis was performed in a typical Systems Engineering environment and use case with various engineering stakeholders involved. The evaluation results show that each technical protection approach has specific strengths and weaknesses. Enterprise Rights Management performed best due to its advanced features and strong protection based on cryptography. However, ERM reaches its limits in complex Systems

Engineering projects in terms of user and permission management. A concept is introduced that eliminates this issue by mapping the top-down system structure to content access permissions. This results in a dynamic permission structure and less management effort during exchange processes. Manual error sources are eliminated and knowledge protection is improved.

Acknowledgements

The authors would like to thank the Secure Product Creation Processes (SP²) and the Enterprise Rights Management Open (ERM.Open) working groups from ProSTEP iViP Association for providing industry requirements regarding knowledge protection. Special thanks go to Joselito R. Henriques for his advice and assistance in this project. We also thank the anonymous reviewers for comments to improve the paper.

This project was supported by CASED - Center for Advanced Security Research Darmstadt (www.cased.de), which is funded through the LOEWE program by the Federal State of Hessen, Germany.

References

[1] R. Haberfellner, W. F. Daenzer, and M. Becker, *Systems engineering : Methodik und Praxis*, 12. ed. Zurich: Verl. Industrielle Organisation, 2012.

[2] Corporate Trust. (2007, last accessed: 2012/10/08). *Studie: Industriespionage*. Available: http://www.corporate-trust.de/pdf/STUDIE_191107.pdf

[3] N. Bosch, *Geistiges Eigentum und Strafrecht*. Tübingen: Mohr Siebeck, 2011.

[4] T. Pütz and E. von Rundstedt, "Personalpolitik und Technologieschutz: Zufriedenheit ist entscheidend," in *Produkt- und Konzeptpiraterie : erkennen, vorbeugen, abwehren, nutzen, dulden*, N.-P. Sokianos, Ed., 1. ed Wiesbaden: Gabler, 2006, p. 340.

[5] H. Meier, O. Völker, and S. M. Binner, "Ein ganzheitlicher aktiver Ansatz zum Schutz gegen Produktpiraterie," *Industrie Management 6/2008,* pp. 11-14, 2008.

[6] E. Abele, P. Kuske, and H. Lang, "Maßnahmen für den Know-how-Schutz," in *Schutz vor Produktpiraterie*, ed: Springer Berlin Heidelberg, 2011, pp. 40-91.

[7] M. Mitrea, "Toward robust spread spectrum watermarking of 3D data," Institut National des Télécommunications - ARTEMIS Project Unit, Evry, France, 2004.

[8] ProSTEP iViP Association, "Secure Product Creation Processes (SP²) White Paper," 2008.

[9] Microsoft Corp. (2012, last accessed: 2012/10/08). *Terminal Services overview*. Available: http://technet.microsoft.com/en-us/library/cc770412%28v=ws.10%29.aspx

[10] S. Kleiner, "Knowledge based Engineering and Intellectual Property Protection," in *Knowledge Sharing and Collaborative Engineering*, St. Thomas, USA, 2006, pp. 86-91.

[11] E. Claassen, "Protection of Intellectual Property in the Product Development Process," presented at the 11° Seminário Internacional de Alta Tecnologia, Piracicaba, Brazil, 2006.

[12] J. R. Henriques, R. Anderl, and M. Grimm, "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 the ASME 2010 International Mechanical Engineering Congress & Exposition IMECE2010*, Vancouver, BC, Canada, 2010.

[13] Avoco Secure IT Alliance, "Choosing an Enterprise Rights Management System: Architectural Approaches," 2007.

[14] A.-R. Sadeghi, M. Winandy, C. Stüble, R. Husseiki, Y. Gasmi, P. Stewin, and M. Unger, "Flexible and Secure Enterprise Rights Management Based on Trusted Virtual Domains," in *3rd ACM Workshop on Scalable Trusted Computing*, Alexandria, VA, USA, 2008.

[15] D. Völz, J. Henriques, and R. Anderl, "Data Exchange Processes based on Trust and Rights Management," *Proceedings of TMCE 2012, Tools and Methods of Competitive Engineering,* 2012.