INTERNATIONAL DESIGN CONFERENCE - DESIGN 2010
Dubrovnik - Croatia, May 17 - 20, 2010.

CONCEPTUAL DESIGN OF A PROCESS STANDARD IN ANTI-COUNTERFEITING

T. Meiwald, M. Petermann and U. Lindemann

Keywords: product piracy, anti-counterfeiting, IT-security, international standards, case study

1. Introduction

Product piracy and unwanted loss of know-how, with estimated losses for Germany of 50 bn € p. a. [Blind, 2009] and 660 bn US$ p. a. worldwide [U. S. Chamber of Commerce, 2008] currently poses one of the most important challenges to industry. To face this challenge, companies can make use of single protection measures like intelectual property rights, IT-security or authentication technologies. More integrated approaches to protect companies from product piracy and unwanted loss of know-how reach from standard strategies [Fuchs 2007] to the customized design of protection systems [Neemann, 2007, Schuh, 2007, Abele, 2008, Albers, 2008, Aurich, 2008, Kleine, 2008, Meier, 2008, Meiwald, 2008]. To evaluate their approach, the authors of this paper performed case studies in six german medium size businesses.

IT-security has faced similar problems of unwanted loss of know-how for a longer time. ISO/IEC 13335, 15408 (also known as Common Criteria) and 27000 represent established procedures to achieve a systematically derived concept for the protection of company know-how from the point of view of IT-security. A standard procedure helps companies to take the right actions, avoids neglecting important steps and enables different entities (individuals, departments, companies) to work in a synchronized manner.

By applying these standards companies gain an overview over existing measures. Finally they reach higher reliability in business-to-business and business-to-customer relationship. Based on the state of the art in anti-counterfeiting (chapter 2.) and six own case studies (chapter 3.) this paper will propose goals for a potential process standard in anti-counterfeiting (chapter 4.). Established IT-security standards will be reviewed (chapter 5.). It will be discussed which aspects can be transferred to a potential process standard in anti-counterfeiting (chapter 5.4.) in order to propose an outline for such a standard (chapter 6., see figure 1.).

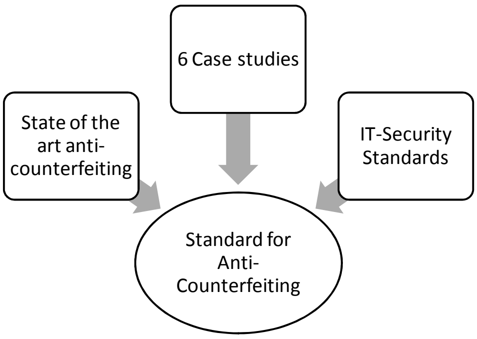
6 Case studies
State of the art anti-counterfeiting
IT-Security Standards
Standard for Anti-Counterfeiting

Figure 1. Considered factors of influence on a potential anti-counterfeiting standard

2. Current systematic approaches in anti-counterfeiting

2.1 Standard strategies

[Fuchs, 2007] emphasizes the importance of a process oriented approach for anti-counterfeiting actions. In order to pursue an according course of action, he suggests a concentration of all anti-counterfeiting actions in a special task-force, which itself composes from piracy relevant functions within the affected company. The proposed approach provides the task-force with 16 "standard strategies" applicable and purposeful in different situations: waive market entry, laissez-faire, intellectual property rights strategy, protection technologies, reactive legal measures, attack, tolerance, compensation, one step ahead, fight fire with fire, cut distribution channels, certificates, cooperation and integration, lobbying, promotion by law claims and brand strength. Each of these strategies requires – partly identical – process steps to be performed sequentially. The strategies are, however, not assigned to certain situations, in which their application is considered reasonable. Following an analysis determining purposeful strategies for a case, each strategy is allocated to a process owner. The process owner pushes strategy implementation and is held responsible for the strategy's success in regular audits.

2.2 Customized approaches

2.2.1 Not process oriented

[Albers, 2008] proposes the adoption oft the Failure Mode Effect Analysis (FMEA) on the issue of product piracy. With it's help decision making as well in the selection of alternative protection measures as in the selection of different product concepts in early design phases should be supported.

[Aurich, 2008] considers information acquisition a crucial factor to base decisions on the selection of purposeful anti-counterfeiting measures. Accordingly, he proposes an information acquisition and management system as one of three columns in their suggested model for the "holistic protection of machinery spare parts". Columns two and three are formed by a counterfeiting analysis and evaluation model and a pool of possible anti-counterfeiting measures. Each of the columns is fed by an internal and external organizational network that provides required resources and methods for implementing the columns. The presented approach aims at the completion of a control loop, allowing for selection and implementation of purposeful measures based on information acquisition and procession. In the loop, information is gathered and classified on potentially endangered components and potential imitators and their tactics. Using these classifications, links to single measures in a pool of measures are established. A selection of purposeful measures is possible via these links. Selected measures are implemented using the resources provided by the network mentioned above.

[Meier, 2008] presents a "holistic, active approach to protection against counterfeiting". Compared to protection concepts exclusively focusing on intelectual property protection or labeling techniques, they anticipate a higher level of protection through adoption of their approach, due to its focus on preemptive protection in earlier phases of product life cycle. Meier et al. declare a necessity of "coordinated" deployment of different measures, and suggest three "columns" of an integrated protection concept: Operational and organizational structure, protection technologies and knowledge distribution management. For each column, single measures are listed exemplarily. In order to attain adequate protection against counterfeiting, multiple measures are deployed – either all coming from one column or from all columns. "Maximum" protection is only promised for intertwining use of all three columns, whereas measures taken from one of the columns are predicted to provide less protection. The presented approach's aims lie in delaying market entry of counterfeiters by knowledge distribution management, and in decreasing losses in sales by operational and organizational structure, and protection technologies.

2.2.2 Process-oriented

[Neemann, 2007] proposes a six-step process to generate an individual protection system. The respective steps are identify company information, identify context information, structure technology know-how, identify potential harm, evaluate protection measures, identify potential effort for implementation and analyze consistency of potential protection measures. Especially the first two steps are supported by the following six models: a model of the company, a context model, a technology and know-how model, a model of protection measures, a model of potential harm, a model on choosing the right protection measures.

[Schuh, 2007] proposes the design of integrative protection concepts through the combination of standard measures, supported by the design of new measures through the established TRIZ-methodology. He includes these methods into a six-step process (requirement specification, conception, idea generation, detailing, implementation and pilot application). In the phase of requirement specification he classifies relevant factors of influence into the two groups of company and imitators that compose the third group of damage scenarios.

Table 1. Overview over reviewed models (customized approaches)

[Aurich 2008]	[Meier 2008]	[Neemann 2007]		[Schuh 2007]	[Kleine 2008]		[Abele 2008]		[Meiwald 2008]	
Information acquisition and management	Operational and organizational strucure	Identify company information	Company model	Requirement specification	Threat chrarcterization		Step 1	Standardized mass product	Definition of project goal	Protection of copied product
			Context model	conception				Integrated module		Protection of new product
Counterfeiting analysis and evaluation model			Technology and know-how model	Idea generation				Complete system		Strategic protection
	Protection technologies	Identify context information	Model of protection measures	detailing	Threat evaluation	Degree of threat	Step 2	Costs	Analysis of individual case	
Pool of possible anti-counterfeiting measures			Model of potential harm	implementation		External factors		Customer approval	Selection and adoption of counter	
			Model on choosing protection measures	Pilot application		Degree of product protection		Influence on the risk of product being counterfeited	Composition of alternative protection	
Control loop idea	Knowledge distribution management	Structure technology know-how			realization		Step 3	Corporate policy	Decision on final protection system	
		Identify potential harm						Corporate strategy	Preparation of implementation planning	
		Evaluate protection measures								
		Identify potential effort for implementation								
		Analyze consistency of potential counter								

[Kleine, 2008] proposes the three process steps of threat characterization, threat evaluation and realization. He evaluates the respective case of product piracy according to the three dimensions of degree of threat ("Gefährdungsgrad"), degree of product protection ("Grad Produktschutz") and external factors ("Externe Treiber Produktpiraterie"). This characterization shall limit the field of possible protection measures down to a size manageable for the companies task force.

[Abele, 2008] suggests a three-step selection process for determination of the most purposeful anti-counterfeiting measures. In the first step, one of three protection profiles is selected according to the considered type of product. These types of products are: "standardized mass product" (synonymously described as “Type I: single part”), “integrated module” (“Type II: “module”) and “complete system” (“Type III: “final product”). This first step in the decision process aims at an increase of efficiency in measure selection. The second step includes an evaluation of measures. Measures are deposited in a database as well as evaluation results. Evaluation criteria are generation of costs, customer approval and influence on the risk of products being counterfeited. Values for the evaluation criteria are determined by applying cost prediction methods, quality function deployment and scenario analysis. The second step aims at increasing effectiveness of measure deployment later-on. In a third and final step, management selects out of a pool iteratively constricted to the most purposeful measures, taking aspects of corporate policies and strategies into account. The final decision step aims at attaining sustainable measure deployment by selecting those complying with corporate strategies.

[Meiwald, 2008] describes a methodical process including six steps to derive an individual and consistent concept of measures against product piracy and unwanted loss of know-how. The single steps are definition of project goal, analysis of the individual case, selection and adoption of protection measures, composition of alternative protection systems, decision on final protection system and preparation of implementation planning. He applies a consistency matrix to analyze the protection measure’s ability to interact in the same protection system. The process uses a catalogue of about 80 protection measures for the three cases of the protection of already copied products (1), protection of new products (2) and the strategic protection of unwanted loss of know-how (3).

[Petermann, 2009] introduces a model of seven damage functions (Increase know-how drain, Degrade site related factors, Decrease sales, Decrease margin, Generate costs, Decrease corporate image, Decrease customer satisfaction) and four groups of damage avoiding functions (Decrease number of current imitations, Minimize know-how drain, Decrease attractiveness for imitator, Decrease market attractiveness for future imitations) which help an affected company to evaluate its own situation and choose the right protection measures.

Table 1 shows an overview over the elements of the different models cited.

2.3 Conclusion – state of the art in anti-counterfeiting

Almost all authors agree up on a systematic, methodically supported **process** that enables companies to derive a protection system. Only [Albers, 2008], [Aurich, 2008] and [Meier, 2008] do not make suggestions on the sequence of the proposed elements. [Neemann, 2007], [Schuh, 2007] and [Meiwald, 2008] propose six process steps, whereas [Kleine, 2008] and [Abele, 2008] choose only three steps. All of the proposed processes offer elements to analyze the individual situation in order to be able to chose potential protection measures.

[Neemann, 2007] classifies **factors of influence** on the decision which measures to implement into four groups, whereas [Schuh, 2007], [Kleine, 2008], [Abele, 2008] and [Meiwald, 2008] decide up on three groups.[Petermann, 2009] introduces a model of seven damage functions and four groups of damage avoiding functions to help an affected company to chose the right protection measures.

In almost all cases the protection system is composed of a larger number of **existing protection measures** of different domains. Only [Fuchs, 2007] offers only 16 standard strategies to the company task force.[Schuh, 2007] supposes the additional generation of individual **new protection measures** by the use of TRIZ. [Neemann, 2007] and [Meiwald, 2008] suppose a **compatibility matrix** to analyze the interaction of measures that potentially result in one joint protection system. Furthermore [Albers, 2008] supposes to include the resistancy against counterfeiting of a future product into the **variant decision** in early phases of product design process. [Aurich, 2008] aims at the completation of a control loop, which brings in the thought of potential **iteration** during the design of a protection system. [Fuchs, 2007] emphasizes the importance of **process owners** who are responsible for the implementation of the respective protection measures and manage the according budget and schedule.

In conclusion all presented attempts include highly valuable elements, but not a single one seams to be complete. For this reason the identified elements in 2.3. will be included into the proposed joint process model in chapter 6.

3. Case studies

The following chapter describes the framework, underlying process model and most important findings of six case studies. The studies were implemented to evaluate the authors' model of a process [Meiwald 2008] that supports companies in the design of an individual protection system for anti-counterfeiting. The studies were implemented with six German medium sized companies from 130 to 2,450 employees. The counterfeited products comprehend railroad crossings, electrical drives, packing machines for concrete, weaving machinery, wood processing machinery and switching elements. Their turnover reaches from 12 m € p. a. to 300 m € p. a. All of the companies generate major parts of their turnover with selling their physical products. But some of them also earn money by offering services to their customers. Counterfeiteres were located all over the world – from China over India, Russia to Europe. The studies were implemented in 2009. One study included four workshops, approx. 3h each. At an average six interviews, 90 minutes each, were realized per company. This produced roughly 50 h of audio data. The findings presented below derive from additional qualitative feedback workshops, conducted within the final presentation of each study.

Most important findings

Intense analysis of the individual case proved to be necessary in all cases in order to generate a holistic model of the individual situation. The analysis was executed by the use of guided interview to enable the exploitation of the individual knowledge of the respective interviewee. For the realization of the protection systems the criteria for the selection of counter measures needed to be adopted. For one company the external costs, internal effort and potential effect of the counter measures were most important, in other companies the counter measures were selected according to their protective effect on identified worst case scenarios. This shows that **adoption of the selection process** is important. The Case Studies showed, that all analyzed companies already implemented an average of 15 counter measures (based on a catalogue of 100 counter measures; variety: five to 22 completely implemented counter measures). The residual counter measures were clustered to 'partly implemented' and 'new counter measures'. This **assessment of** the **implementation status of counter measures** at the individual company proved to be helpful in order to limit the given catalogue of 100 counter measures down to a manageable number. A model that also seemed to be helpful in most cases was the so called "**Roadmap**". It is an vizualization of individual counterfeiting issues like 'loss of know how', 'reengineering' or others and the different counter measures to fight these issues over time. The companies were provided with **assisting questions** fo each selected counter measures which should support the implementation of these measures. These questions were considered valuable by the company partners.

4. Goal, effect, type and content class of a potential process standard in anti-counterfeiting

Concerning their general design, there are eight different types of standards as described in DIN EN 45020 [DIN Katalog, 2009]: basic, terminology, testing, product, process, service and interface standards and standards on data to be provided. Standards may make a statement, instruct, recommend or formulate a requirement. This classification scheme lays out the scope for potential standards.

Current research in anti-counterfeiting focuses on two levels: on the one hand specialists in different domains of protection measures like cryptography, law or material science analyse new approaches to expand their discipline's methods in order to achieve an enhanced level of protection of companies revenues. This field and respective attempts in standardization (e. g. ISO PC 246) will not be discussed in this paper. On the other hand the **goal** of management oriented approaches (like the ones described in chapter 3) is to ***support companies*** in terms of ***defining and managing counterfeiting protection systems.*** Such a system includes a number of protection measures, which have to be chosen according to the individual case of counterfeiting [Petermann 2009]. Crucial issues are the design of the system concerning its effectiveness and the efficiency of its generation. After implementing the system it is important to conrol it in an efficient way that guarantees its effectiveness for the future.

The **effect** of such a standard in the context of intense business-to-business relationships, as they are typical in modern supplier networks, would be to ***improve reliability*** concerning the protection of know-how. This effect would be similar to that of IT-security standards but would be achieved through measures exceeding IT-security.

Concerning the **type** of standard (compare DIN EN 45020 [DIN Katalog 2009]) the potential standard would include basic ***terminology*** in order to avoid misunderstandings. Its main character would be that of a ***process standard*** with its focus laying on a standard procedure.

The **content class** of a process standard in anti-counterfeiting is to give recommendation on which activities to accomplish to design a counterfeiting protection system as well as to provide supporting information on available protection measures. Advise of the management and controlling of implemented measures is necessary. According to the classification of DIN EN 45020 [DIN Katalog 2009] the standard has to give ***recommendation*** on a reasonable work process and controlling scheme and make ***statements*** on existing protection measures. Further recommendation on the content itself will be given in chapter 6.

5. Relevance of IT-security standards for an anti-counterfeiting process standard

As most important examples of standards for IT-security ISO/IEC 13335, 15408 and 27000 will be overviewed in the following chapters and their relevance for a potential process standard for anti-counterfeiting will be evaluated. Further examples of standards in information security include the German “IT-Grundschutzkatalog” (former “IT-Grundschutzhandbuch”), published by the German Federal Office for Information Security, ISO/IEC 17799 (predecessor of ISO/IEC 27000) and BS 7799-2 (predecessor of ISO/IEC 17799). They wil not be further analyzed in this paper. The standards in the following three chapters will be allocated to the respective types of standards as described in DIN EN 45020.

5.1 ISO/IEC 13335

Goal

According to Berlich [2005] ISO/IEC 13335 provides a management view on information security. Targeted persons are primarily security officers. ”It is not the intent of this International Standard to suggest a particular management approach to Information and Communication Technology (ICT) security.” [DIN Katalog 2009]

Structure

DIN ISO/IEC 13335 [DIN Katalog 2009] is divideded into the following main chapters:

- “Scope” (informing about the goal of the standard and defining its range)
- “Definitions”
- “Security concepts and relationships” (introducing five high-level security concepts and a model of six “security elements” (assets, threats, vulnerabilities, impacts, risks, saveguards, constraints) and their relationship)
- “Objectives, strategies and policies” (informing about “what is to be achieved”, “how to achieve these objectives” and “the rules to be observed in implementing the strategies”)
- “Organizational aspects of ICT security” (roles and responsibilities; organizational principles)
- “ICT security management functions” (planning, implementation, operations and maintenance, cultural and environmental conditions and risk management)

Content

DIN ISO/IEC 13335 defines relevant terms like “asset”, “risk” and “threat”, structures possible threats and names examples (e. g. “eavesdropping”, “incorrect routing” or “earthquake”). It builds up a model how the named six “security elements” are connected. Information on possible objectives of corporate security, their implementation, responsibilities and company hierarchy levels to include is provided. ICT security management functions are named briefly. [DIN Katalog 2009]

5.2 ISO/IEC 15408

ISO/IEC 15408 is also known as Common Criteria (CC) and contains three parts. In the following paragraphs these will be analyzed as a whole.

Goal

According to Volkamer [2007] one of the reasons for the introduction of ISO/IEC 15408 was to avoid the necessity to certify software several times for different countries in order to accept it as being secure.

Structure

ISO/IEC 15408 [DIN Katalog 2009] consists of the three parts:

- "Introduction and general model" (Introduction of the underlying model of IT-security and structure of evaluation documentation; explanation of "protection profiles" and "security objectives")
- "Security functional requirements" (introduction of the underlying "security paradigm", definition of "content and representation of the functional requirements" and a catalogue of requirements, allocated to eleven classes)
- "Security assurance requirements" (introduction of the underlying "assurance paradigm"; countermeasures, methods and techniques affecting the design process and methods; related documents, tools and certficicate; seven Evaluation Assurance Levels (EALs); compare [Volkamer 2007])

Content

Following Volkamer [2007] an evaluation according to ISO/IEC 15408 (Common Criteria) considers three aspects of an IT-product: its functionality, underlying processes for the design and production of the product and its resistance against random failure or attack. The intensity of the evaluation depends on the Evaluation Assurance Level (EAL).

5.3 ISO/IEC 27000

Goal

ISO/IEC 27000 aims at defining requirements for Information Security Management Systems (ISMS) from a process view. According to Berlich [2005] information security is seen as a holistic task. The standard recommends management of security by defining individual tasks. Target persons are company security officers.

Structure

ISO/IEC 27000 is organized in two parts. ISO/IEC 27001 introduces basic definitions and introduces a general model for the management of an ISMS. Only a brief overview on corresponding requirements is given. A more detailed catalogue including 132 possible counter measures is presented in ISO/IEC 27002 and organized into ten categories (Organization of information security, Asset management, Human resources security, Physical and environmental security, Communications and operations management, Access control, Information systems acquisition, development and maintenance, Information security incident management, Business continuity management, Compliance).

Content

According to Berlich [2005] ISO/IEC 27000 gives only a very general level of information, not directly applicable. ISO/IEC 27002 includes a vast list of applicable counter measures from very technical issues like "Session Time Out" over IT-management issues like "backup of information" to very general aspects like "working contracts".

5.4 Conclusion - relevance of IT-security standards

According to [Berlich, 2005] the level of detail of ISO/IEC 13335 is sufficient for informing the persons targeted but insufficient to serve as manual. The standard introduces a valuable model that helps understanding the different elements, influences and interdependencies of IT-security management. This thought of providing concerned persons with an **overall model** could be valuable for the focussed process standard for anti-counterfeiting. It helps to understand complex dependencies as they might appear in the analysis of counterfeiting cases and the composition of an effective protection system.

ISO/IEC 15408 emphasizes the importance of an ex post evaluation of an IT system and necessary processes to assure its usability. This principle can be transferred to a counterfeiting protection system as well. Current research focuses mainly the preparative design of protection systems. **Controlling and evaluation of an implemented protection system** has not yet been part of the main focus.

Berlich [2005] reasons ISO/IEC 27000 being appropriate for evaluating the completeness of applied measures. For a potential process standard for anti-counterfeiting the concept of a **catalogue of counter measures** has to be included (in accordance with [Neemann, 2007, Aurich, 2008, Meiwald, 2008, ...]). Additionally the presented **catalogue of ISO/IEC 27002 should be reviewed** in detail to identify measures that might not have been considered yet in anti-counterfeiting catalogues like www.conimit.de.

6. Conceptual design of a process standard for anti-counterfeiting

Based on the presented findings a potential process standard for anti-counterfeiting should include the following elements: **Terms and definitions** should be worked out by a group of specialists of the field of anti-counterfeiting to gain a shared understanding of this issue. An example for an **overall model** is presented in figure 2. It represents the underlying mechanisms of counterfeiting. These mechanisms also represent potential working points for counterfeiting counter measures. The design of an adequate overall model should be discussed in order to represent the authors' view of the future standard.

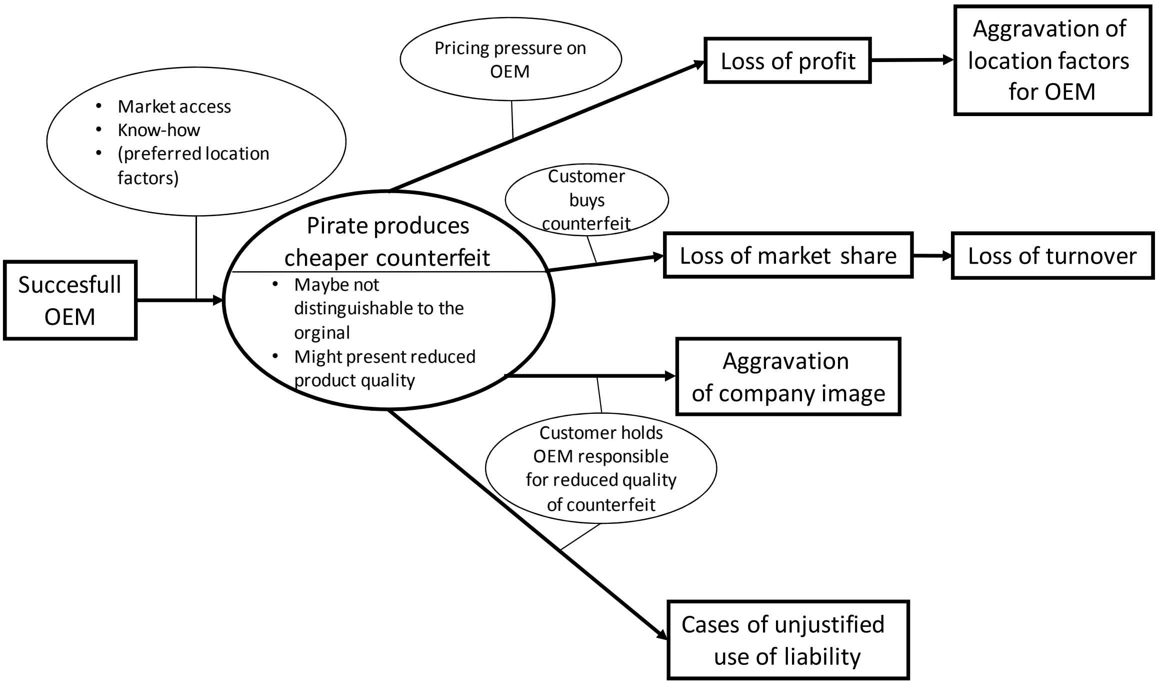
Pricing pressure on OEM
Loss of profit
Aggravation of location factors for OEM
• Market access
• Know-how
• (preferred location factors)
Customer buys counterfeit
Pirate produces cheaper counterfeit
• Maybe not distinguishable to the orginal
• Might present reduced product quality
Loss of market share
Loss of turnover
Succesfull OEM
Aggravation of company image
Customer holds OEM responsible for reduced quality of counterfeit
Cases of unjustified use of liability

Figure 2. Proposed overall model of counterfeiting mechanisms

According to literature review and own experience of six case studies the **process model** for the individual design of a counterfeiting protection system should include the following elements:

1.Requirement specification (including the definition of a shared project goal)

2. ***Analysis of individual situation*** (including interviews to evaluate the following topics: company - product and technology, currently implemented counter measures with implementation status, company strategy, production; market; counterfeits; know-how; harm; suppliers; competitors)
3. ***Idea generation*** (generate new counter measures)
4. ***Selection and adoption of counter measures*** (considering effectiveness to prevent identified elements of harm)
5. ***Composition and evaluation of alternative protection systems*** (including consistency analysis, and considering effectiveness to prevent identified elements of harm, effort for implementation and company strategy with the goal of a "Roadmap" model)
6. ***Decision on final protection system*** (including persons being responsible for the implementation of every single counter measure (process owners), planning of budget and timeline)
7. ***Controlling of the implemented system*** (to review the achievement of the defined goal of step 1. and the protection of identified harm of step 2.)

It is important to include the possibility of iterations into this model as they appear necessary in the individual project. The consideration of the resistancy against counterfeiting of a future product in the variant decision in early phases of product design process is not included in this process model as it is more or less an own counter measure by itself that could be included into the catalogue of existing counter measures. A **catalogue of existing counter measures** can be derived from literature and internet sources. The authors used a catalogue of 100 counter measures, that could be included into a future standard. For the users of such a standard it would be helpfull to include not only a description, pros and cons but also assisting questions for the implementation of the respective counter measures.

7. Conclusion and outlook

This paper presented the need for and the conceptual design of a process standard for anti-counterfeiting. It reviewed the state of the art of anti-counterfeiting, gave input of six own case studies and reviewed established standards of IT-security considering their relevance for a potential process standard in anti-counterfeiting. Aspects to be discussed in further work should include Decision Making and Competitive Intelligence as factors of influence on the design of a protection system for anti-counterfeiting. According to Decision Making, especially those fators reflecting the influence of human factors (e. g. heuristics and other biases, group think) should be regarded, as such a protection system can only be designed, by including the knowledge of several members of a company. Therefore it is necessary to incorporate their input without tampering it.

Acknowledgement

The case studies, as presented in chapter 3., were realized in the framework of the research project ConImit (Förderkennzeichen: O2PU1070) in cooperation with the Heinz Nixdorf Institut of the Universität Paderborn. The project is funded by the German Bundesministerium für Bildung und Forschung (German Federal Ministry of Research and Technology) and attended by the Projektträger Karlsruhe. We want to thank all involved persons for their commitment and support.

References

Abele, E. et al.; Aurich, J. et al.; Kleine, O. et al.; Meier, H. et al.; Meiwald, T. et al. in Gronau, N.: Industrie Management, Vol. 6, 2008, pp. 11-50.

Albers, A., Marxen, L., Oerding, J., Meboldt, M., Schäffer, T., „Piracy Risk and Measures Analysis", Proceedings of the 7th International Heinz Nixdorf Symposium Self-optimizing Mechatronic Systems, J. Gausemeier (Ed.), F. Rammig (Ed.), W. Schäfer (Ed.), W. V. Westfalia Druck, GmbH, Paderborn, 2008, pp. 231-244.

Berlich, P., Rohde, M., „Normen der IT-Sicherheit im Vergleich", DECUS IT Symposium 2005, Neuss, 2005.

Blind, K., „Die volkswirtschaftliche Bedeutung geistigen Eigentums und dessen Schutzes mit Fokus auf den Mittelstand", Harzdruckerei Wernigerode GmbH, Werningerode, 2009.

DIN-Katalog für technische Regeln - Deutsche Normen und technische Regeln, Internationale Normen, Beuth Verlag Berlin, 2009.

Fuchs, H.-J., „Die China AG“, FinanzBuch Verlag, München, 2007.

Neemann, C., “Methodik zum Schutz gegen Produktimitationen”, Shaker, Aachen, 2007.

Petermann, M., Meiwald, T., Lindemann, U., „Decision support for the selection of anti-counterfeiting measures based on modeling damage avoiding functions”, Proceedings of the 17th Internation Conference on Engineering Design, L. Leifer, Stanford, 2009.

Schuh, G.; Haag, C.; Kreysa, J.: “TRIZ-based Technology Know-how Protection – How to find protective mechanisms against product piracy with TRIZ”, Proceedings of the TRIZ-Future Conference, C. Gundlach, U. Lindemann, H. Ried, Kassel University Press, Kassel, 2007, pp. 111-115.

U. S. Chamber of Commerce, URL: http://www.uschamber.com/issues/index/counterfeiting/default (Downloaded on 4.3.2008)

Volkamer, M., Hauff, H., “Zum Nutzen hoher Zertifizierungsstufen nach den Common Criteria (I)”, IT-Sicherheit & Datenschutz, Vol. 9, 2007, pp. 692-695.

Dipl.-Ing. Thomas Meiwald
Research Assistant
Technische Universität München, Institute of Product Development
Boltzmannstr. 15, 85748 Garching, Germany
Telephone: +49 89 289 151 29
Telefax: +49 89 289 151 44
Email: meiwald@pe.mw.tum.de
URL: http://www.pe.mw.tum.de/lehrstuhl/mitarbeiter/mitarbeiter?userName=meiwald