protect-ing.de

Product and Know how Protection Guidelines

A Generic Process Model for
Introducing Means of Protection against
Product Piracy and the Loss of Know-How

VDMA Working Group Product and Know-how Protection

A Working Group within

VDMA

Preface

Situation

Despite massive potential damages and the constantly growing threat posed by product piracy and the loss of know-how, few companies make sufficient use of technologies or other measures to prevent and protect against these threats. There is a lack of transparency about the commercial viability, the procurement costs, and the feasibility of integrating such measures in established processes. For many companies who would benefit particularly from preventative measures, their implementation often appears too complicated.

Explaining the added value of solutions or concepts for preventing product piracy and the loss of know-how is not simple. The specific benefits too often only become evident when applied to a specific use case or company's situation.

Purpose

These guidelines offer a selection of viable measures for protecting against product piracy and the loss of know-how in the form of a structured procedural model that reveals the requirements and possible protective means for relevant key areas of business. The recommendations included in these guidelines give an overview and a first source of information concerning the effective use of such protective measures.

Target Group

These guidelines are intended for all manufacturing businesses, their suppliers, and their clients who plan to introduce measures to protect against product piracy and the loss of know-how. The guidelines are written for use by executive management, process managers, and technical developers as well as users.

Contents

These guidelines review the current potential threats and offer solutions in the form of a structured procedural model, designed to reveal the requirements and possible protective means for relevant key areas of businesses. Using a generic model allows the definition of pragmatic solutions and offers the affected companies a sound basis to start from.

What is not covered by these guidelines?

These guidelines are intended solely for manufacturing businesses. They do not include legal means of protecting intellectual property.

Working Group Product and Know-How Protection
Lyoner Strasse 18
60528 Frankfurt am Main
Germany
Phone +49 69 6603 1978
www.protect-ing.de

1st edition, Oct. 2013

This document was originally published in German language, April 8th 2013.

Contents

1 Management Summary

The competitiveness of German businesses in the mechanical and plant engineering industry in particular depends to a considerable degree on their ability to protect their research and procedural know-how.

Competition is becoming more global, more intensive, and tougher. This makes protecting products and essential know-how more than a challenge: it is a requirement.

Because the perpetrators are often working in the background, the threat seems abstract. Once a product has been counterfeited and brought to market or essential know-how been lost, the effects in terms of lost market leadership, reduced market share, or falling margins are serious.

Protecting the future viability of a business means knowing the interests, modus operandi, and resources of the perpetrators. Understanding the threat helps understand the relevant risks.

In order to mitigate or even remove those risks, WHAT we are doing is important. Even more so, HOW we are doing it is fundamental.

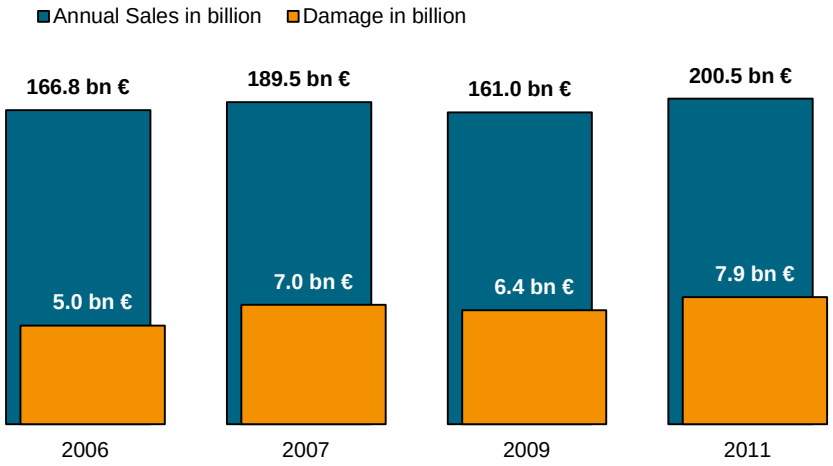
These guidelines were written to make business executives aware of the threats and risks in the area of product and know-how protection. They are meant to help people develop and implement an effective protection concept with the “right” combination of methodically sound and practically tested means.

A standard protection strategy and a risk assessment made on that basis help select the right measures and activities across disciplinary or organizational boundaries and reduce the overall risks with due attention to questions of costs and benefits. The following guidelines introduce a case study to show how different measures combine to form an effective protection strategy.

2 Status Quo

The State of Product Protection

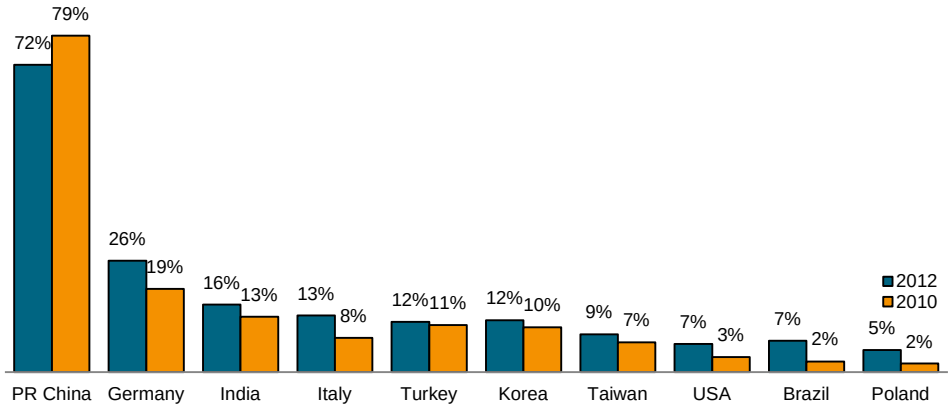
Product piracy can cost companies millions of euros. For Germany's mechanical and plant engineering businesses, estimates put the damage in 2011 alone at approx. €7.9 billion. Generating regular turnover in these dimensions would protect approx. 37,000 jobs.[1]



Many of the victims are businesses who sell predominantly to customers in the Asian hemisphere. Nine in ten makers of textile, plastic, or rubber processing machines are victims of product piracy.

The size of a company also plays a major part: 90 percent of large mechanical and plant engineering businesses employing over 1000 people are already affected. Their smaller peers, employing fewer than 250 people encounter plagiarized or counterfeit products in "only" 52 percent of cases.

Most counterfeits are components or spare parts, although approximately half of all mechanical engineering firms have discovered copies of entire machines.



Place of origin of counterfeit products (from: VDMA study on product piracy 2012)

[1] The complete VDMA study on product piracy is available for download at pks.vdma.org.

The place of origin of those counterfeits is a controversial topic. Most entrepreneurs readily point to Asia, China in particular, but the second most common place of origin is in fact Germany, which might be due to the easier access to the relevant know-how (e.g. from former employees) and the absence of major language barriers.

Trends show that large companies who operate in China are particularly favorite victims of product pirates. It has to be assumed that Chinese product piracy will be declining in the long run, as other emerging economies are filling in the void.

Considering the growth of the world economy and the constant demand for new and innovative branded products, it seems likely that the shadow economy of counterfeiters and plagiarizers will continue to make up a considerable part of the world's markets, estimated at more than five percent. For the companies affected by this, protecting against piracy with innovative and intelligent technologies and strategic measures, particularly on the communication front, is becoming a major focus.

The State of Know-How Protection

Information security is a necessity in all areas of businesses. By contrast, applications of real know-how protection are still few and far between. For the purposes of these guidelines, know-how refers to the knowledge and abilities that have a direct impact on the market performance of a company.

The loss of know-how or other sensitive information like Intellectual Property can have many different causes with many different effects. The following scenarios are possible:

- Involuntary disclosure of know-how by the carelessness of the holders of certain know-how;
- Individual employees switching to a competitor or working with competitors as freelance agents;
- The use or disclosure of information by consultants to the detriment of the business;
- The misuse of information by clients e.g. to create price pressure
- Competitors monitoring who the company in question employs and which goods it purchases from whom to get insights about operational or strategic activities;
- Suppliers disclosing know-how to competitors;
- Direct attacks on know-how or information by competitors, e.g. through corporate intelligence or competitive espionage;
- Attacks as part of the many state-run industrial espionage programs, especially in the emerging economies.

Many threats are the result of the growing trend towards outsourcing certain processes or using outside personnel. In some instances, companies put themselves in positions of dependency that removes the necessary control over their know-how.[2]

The essential implications of lost know-how can include:

- Losing a competitive advantage with medium to long-term financial losses as a result of lower turnover or increased innovation by

[2] Federal Office for the Protection of the Constitution, publication "Wirtschaftsspionage - Risiko für Ihr Unternehmen" ("Industrial espionage – Risks for businesses"), June 2008, p. 16

competitors
- Entire business units being pushed out of certain markets that are subject to organized industrial espionage or protectionism, e.g. by competition from state-run enterprises or massive price dumping;
- Breach of operational or legal regulations, which is particularly problematic in the case of know-how or information leaked to rogue states or terror organizations.

3 Potential Threats

Who is counterfeiting products?

When investment assets are concerned, attention needs to be paid to suppliers, license holders, and partners in joint ventures. These groups might be counterfeiting products of their partners or commissioning others to do so – often with the cognizance of official authorities.

The victims of the theft of intellectual property, product piracy, or the theft of sensitive data include globally active corporations and small-to-medium-sized enterprises that are known only to specialists. The rising number of counterfeit items suggests a constant, extensive stream of construction data leaking during development processes.

Counterfeit products are often produced by large operations with substantial investments of materials and technological know-how. In some cases, the industrial-scale production of forgeries is the only commercial activity of those businesses.[3]

A look at China shows that the victims include not only foreign investors. In some cases, Chinese producers are being copied by their compatriots, e.g. the Chinese knife maker Wangmazi[4] or the solar panel maker Suntech.

The counterfeiters reveal a high degree of professionalism and technical skill. Even high up-front investments do not stop them from counterfeiting, which is particularly true in the copying of electronic devices.[5]

How does counterfeiting work?

There are signs indicating that counterfeiters tend to change their strategy over the course of their business life. Initially acting in a ‘Me-too’ sense, they soon move to ‘application engineering’ or ‘follow-the-leader’ strategies. They go beyond simple copying and try to better understand and improve on pirated products. As the Japanese example shows, it is conceivable that former counterfeiters can later become pioneers with a ‘first-to-market’ strategy.[6]

The results of their activities are partially reinvested in production facilities to handle more resource demanding products or high-tech products.[7]

The business model of most counterfeiters relies on benefiting from low overhead

[3] BLUME 2006, p. 47

[4] FUCHS et al. 2006, p. 15

[5] AVERY et al. 2008, pp. 262, 318

[6] SEIDENSCHWARZ et al. 2008, IMPULS FOUNDATION 2007, PARADISE 1999, p. 73

[7] WINKLER et al. 2007, p. 69

costs (avoiding one-off costs like R&D, licensing, etc.) and high-volume production. This applies in particular to counterfeiters with limited technological expertise who get their product designs from reverse engineering or the theft of know-how. Their lacking or insufficient competencies prevent them from making custom products. This target group includes counterfeiters who target only selected market segments (specific countries or companies with low investment resources) and larger players who distribute their products on a comprehensive level.

Considering China as the place of origin of many counterfeit products, one can see that a focus on re-innovation (emulation) in the tenth five-year plan (2001 – 2005) of the Chinese central government has shifted to a focus on developing domestic innovation in the eleventh five-year plan (2006 – 2010)[8]. This trend is reaffirmed in the twelfth five-year plan (2011 – 2015)[9]. Investments into research and development are to double from now until 2015. Strategically key areas include the development of environmentally friendly cars, new energy sources, energy efficiency, the development of new materials, biotech, and IT. In these key industries, China intends to use a massive growth push to become technology leader. The know-how for this purpose is acquired by buying or taking over German companies (e.g. the 2012 takeover of Putzmeister, Kiekert, and Schwing), or by other means, such as the illegal transfer of know-how or product piracy.

Barriers for New Business Areas

When a counterfeiter decides to establish a new business area, he has to master certain challenges like any normal entrepreneur. HAUSCHILDT identifies the following forms of resistance that a company has to overcome in the sense of barriers to market entry:[10]

- “the cognitive resistance of not-knowing-how,
- the mental resistance of not-wanting-to,
- the organizational resistance of not-being-allowed,
- and the financial resistance of not-being-able.”

The mentioned “mental resistance of not-wanting-to” is presumably the easiest step to overcome or rather a question that is never posed. Studies show that counterfeiters work quite systematically to find an original product whose reproduction could be a viable business model. The “cognitive resistance of not-knowing-how” is sometimes not explicitly present or ignored deliberately. The “finance resistance of not-being-able” can be considered part of the counterfeiter’s business planning. Their access to finance is closely related to the legality of their operations. Their assets can come from regular sources like banks or be the product of criminal activities[11]. It should be noted that financial barriers to market entry are often impossible to overcome, for counterfeiters in particular. They can be considered an effective protection against piracy[12].

[8] IMPULS FOUNDATION 2007, pp. 11f, 94f

[9] DELOITTE CHINESE SERVICES GROUP 2009

[10] HAUSCHILDT 1998, p. 3

[11] Cf. AVERY et al. 2008, pp. 66 and pp. 87ff; PARADISE 1999, p. 21; BRAUN 1993, p. 29

[12] SCHEWE 1992, pp. 98ff and pp. 224f

3.1 Acquiring Know-how

The following chapter will look at the various means that counterfeiters use to access know-how. Their tactics vary: reverse engineering, the unintentional loss of know-how by espionage, the leaking of design data or CAD drawings, hacking or company takeovers.

Reverse Engineering

One method of emulating a successful product is reverse-engineering[13]. In many cases, acquiring the necessary originals is simple, as they are available on the public market. In some instances, however, counterfeiters are prepared to use armed robbery to acquire particularly enticing models[14].

The precondition for any successful reverse engineering is the availability of certain fundamental technical expertise. The more technologically complex the product to be plagiarized is and the less evident certain functionalities are in the disassembled product, the more challenging such reverse engineering becomes. Any successful reproduction of a product might be rendered impossible as a result of production processes that are difficult to comprehend (such as heat treatment). In other cases, disassembling the original product might require its physical destruction, which in turn complicates or prevents a reconstruction of that product[15].

When reverse engineering is successful, it often includes a certain transfer of know-how from the original manufacturer to the counterfeiter. Every successful counterfeiter learns something from a reverse-engineered product.

Counterfeiters who gain such production know-how from reverse engineering have an opportunity to improve the product in the process of product design. They can simplify components or assembly units that might have been over-engineered. This can make the product more suited to the target market or to the available production facilities. A side benefit to the counterfeiter is that the production costs can be reduced, which again allows for lower sales prices. While the superficial functionality stays the same, the cost-benefit ratio for the unwitting customer improves considerably[16].

Industrial Espionage

In the case of state-supported espionage, intelligence is gained by covert individuals who might be recruited as agents to betray or spy on their target. Professional members of the intelligence services with fake identities are also employed. Human intelligence is supported with modern signals intelligence – the wiretapping of the digital age – which is used for electronic or communication espionage or as a tool for handling agents in the field.[17]

[13] JOHNANSSON 2006, p. 132

[14] Cf. BRAUN 1993

[15] Cf. HARTE-BAVENDAMM 2000, pp. 1 and 8

[16] Cf. WINKLER et al. 2007, p. 80

[17] Federal Office for the Protection of the Constitution, Publication “Wirtschaftsspionage - Risiko für Ihr Unternehmen” (Industrial espionage – Risks for businesses), June 2008 p. 14

Unintentional Loss of Know-how

The unintentional loss of know-how by leaks in knowledge that cannot be secured with commercial proprietary rights can occur in various business areas:

Business Area	Possible Loss of Know-how
Procurement	Counterfeiters purchase materials and semi-finished goods from the same suppliers as the original manufacturers.
Production	Uncontrolled access to design plans, materials, and machine specifications allows the theft of documents, components, and finished products; this also applies to the uncontrolled disposal of rejected products.
Sales	Products can be lost in obscure sales channels, e.g. by bribing sales personnel or legitimate sales agents supporting counterfeiters in the distribution of their products.
Trade Exhibitions	Product innovations can be inspected by potential counterfeiters; personal discussions can reveal further technical details.
Licensing	License holders gain comprehensive product insight and can draw further conclusions about proprietary information.
Patents	The information disclosed in patent filings can be sourced by competitors.
Business Partnerships	The Chinese authorities require joint ventures as preconditions for entering the Chinese markets in certain industries, e.g. in the automotive or rail transport sector. Tenders often require local production of up to 80%; such a degree of local production is often impossible with subsidiaries, and partnerships with domestic Chinese businesses are required.

Loss of know-how, Source: Meiwald[18]

The potential reasons for such betrayal by employees are personal financial issues, greed, revenge, or self-glorification[19]. Often, the lost information is not disseminated by people, but rather on unprotected documents. Such documents most commonly include technical product information, such as:

- Requirements and specifications;
- Designs and technical drawings;
- Software source code;
- Wiring diagrams or work plans;
- Spare parts documents;
- Operating instructions;
- Bills of material[20].

[18] MEIWALD 2011, p. 41

[19] PÜTZ et al. (2006, pp. 56ff) and LIMAN (1999, pp. 239ff)

[20] Cf. HELBIG 2006, pp. 150ff

Loss of Know-how in Projects

Apart from the intentional betrayal of secrets, there is the risk of leaks of document-based information in IT-based development environments or during the strategic planning process. Such development activities are often globally distributed.

Development processes are being pushed and optimized in response to the immense rationalization pressure. Complex development jobs (design of components, integration of design and calculation, validation, process chain integration) are highly automated with methods and tools of knowledge-based engineering resulting in major time savings and efficiencies[21].

At the same time, manufacturers employ external suppliers and production services across the globe. This makes it necessary for CAD models and drawings to leave the original company's premises in many business processes – often without any means of control or protection. Frequently, flexible communication networks are established on an ad-hoc basis for this purpose, integrating new partners and changing their make-up dynamically depending on the development cycle. Today's partner can be a direct competitor in tomorrow's project. The highly complex data exchange processes make the unauthorized access by third parties to proprietary know-how very likely. When there are no know-how protection means in place, e.g. no secure data exchange platforms, no specially prepared data is sent, or even different security technologies are used, the doors are open to counterfeiters.

This shows that the potential threat is not limited only to outright industrial espionage, but also concerns the risks of routine product development processes.

These conditions increase the risks of unintentional loss of know-how. Access to CAD models means direct access to product know-how if the data owner has not applied any targeted security measures. This product know-how usually takes the form of configuration, design, or calculation data – the HOW of product development and production[22]. Losing such know-how to counterfeiters should be considered particularly serious. It gives access to knowledge that cannot be reconstructed by other means. With such knowledge, a criminal competitor has the ability to produce identical or similar products at much lower costs for the world market without the need for any development effort. Suitable countermeasures[23] [24] [25] need to be taken to prevent sensitive production knowledge from becoming public through loss, unintentional disclosure, or outright theft of technical data.

Counterfeiters are making more and more use of methodical approaches, such as competitive intelligence, to source systematic information about the intentions, strengths and weaknesses, tactics, risks and opportunities, products and services, sales channels and sales performance, new designs, registered proprietary rights, or technologies of the companies they try to emulate.[26]

[21] LIESE et al. 2004

[22] WENDENBURG 2010

[23] LIESE 2012

[24] BUGOW 2007

[25] STJEPANDIC et al. 2008

3.2 Counterfeiters' Self-Preservation Measures

To protect their business model, counterfeiters who intentionally infringe proprietary rights use specific self-preservation measures. These include minor changes to the product design to make enforcing design rights more difficult, or filing patents for counterfeited products. For this purpose, patent documents and drawings are copied from the websites of U.S., European, or Japanese patent offices, modified in details, and filed for registration in a patent office in China or other countries.[27]

There have also been cases in which brand or product pirates have taken the original manufacturers to court for infringing Chinese patent rights acquired in this manner – and indeed won[28].

Other tactics are used to deceive the end customer. Since extremely low prices would cause attention, the pricing difference to the original product is often kept to a minimum. A ten or twenty-percent discount reduces the risk of unusually low prices attracting the attention of the judiciary or the original rights owner[29].

In some instances, the production sites and stores of counterfeiters are protected by local police or military units[30]. Protectionism is also a motive behind the sale of counterfeit products in China. In particular in the case of consumer goods, these products are sold to wholesalers that often are important pillars of the province's business. The markets are built by the local offices of the "Administration of Industry and Commerce "(AIC) to promote and regulate local commercial activities. This creates networks between the local authorities and the brand and product pirates. The local AICs have invested in establishing these markets and are in charge of its management. Income is generated in the form of monthly administration fees and leases. The same officials are responsible for protecting proprietary rights, which creates a typical conflict of interests between domestic and local law and justice, which in turn does not create much impetus for prosecuting product pirates.[31]

If the sales are not limited to the domestic market, product pirates often hide originals in counterfeit shipments to complicate investigations. Copying is not limited to products or packaging; shipping and customs papers are also regularly forged. When counterfeit products are shipped with forged documents along the same routes as the original products, counterfeiters substantially reduce the risk of customs identifying their deeds. Another countermeasure to avoid prosecution is the import of so-called blanks, that is, plagiarized products that are only given their counterfeit branding immediately before sale in the target market. This prevents larger shipments of counterfeit products from being picked up at the

[26] FUCHS 2007, p. 394

[27] WINKLER et al. 2007, p. 62

[28] Cf. WINKLER et al. 2007, p. 63

[29] Cf. WINKLER et al. 2007, pp. 69ff

[30] Cf. STÖCKEL 2006, p. 269; BLUME 2006, p. 218; WINKLER et al. 2007, pp. 69f

[31] WINKLER et al. 2007, p. 48

perpetrator, since the brand infringement has not happened at that point. The supply line remains unbroken – even when major shipments are stopped.

Counterfeiters “permanently develop new ‘breaking bulk’ strategies that enable the illegal goods to be transported from the place of origin to their destination, or from the port of destination to the point of sale, without being caught by investigators”.[32] Counterfeiters are constantly changing their modus operandi to avoid discovery.

The self-preservation tactics of counterfeiters also include not sending product samples to potential buyers abroad. They only accept wholesale buyers who buy in bulk. This makes inspections more expensive and makes it difficult for people to establish whether a product is a forgery.

[32] WINKLER et al. 2007, p. 72

3.3 Producing Counterfeit Products

The manufacturing of counterfeit product takes many forms, from technologically complex large-scale production at large, legal companies[33] to generally illegal "underground factories" in which products are made without much sophisticated equipment in modest circumstances[34]. These primitive production sites need minimal investments and can be relocated at a moment's notice, e.g. to avoid discovery by competitors or official authorities.

To avoid legal risks, many counterfeiters do not produce their goods themselves, but rather pass orders on to sub-contractors[35].

Another typical phenomenon is the proverbial "fourth shift". In this case, the same production facilities are used that are employed in the production of the original branded goods.

A related occurrence is the establishment of parallel plants, which copy specific know-how from the legal production operations of the original producer[36].

3.4 Distributing Counterfeit Products

The global distribution of counterfeit products is driven mostly by the internet. The web allows information to be shared and products to be marketed anywhere in the world. When counterfeit products are concerned, www.alibaba.com, www.china.alibaba.com, and www.made-in-china.com are common sights.

Improved transport, travel, and communication processes mean that counterfeit products are often already on sale in markets that the original manufacturer has yet to enter.

3.5 Impact of Product Piracy

Product piracy affects consumers, commercial buyers, original equipment manufacturers, and the entire economy. The impact on consumers lies mostly in the poor product quality of counterfeits, which can create danger to personal safety and can have financial consequences[37].

For commercial buyers of counterfeit products that infringe proprietary rights, there are potential financial damages, since they cannot legally sell products

[33] Cf. BLUME 2006, p. 47; RUPPEL 2007, p. 93; WINKLER et al. 2007, pp. 69f

[34] Cf. RUPPEL 2007, p. 94; AVERY et al. 2008, p. 318

[35] Cf. WINKLER et al. 2007, p. 70

[36] Cf. HOPKINS et al. 2003, p. 9; BLUME 2006, p. 47; STÖCKEL 2006, p. 267; STAAKE 2007, p. 22; WINKLER et al. 2007, p. 65; SCHAAF 2009, pp. 74ff

[37] Cf. BRAUN 1993, pp. 34f; HOPKINS et al. 2003, pp. 155ff; SCHIWEK 2004, p. 26; FUCHS et al. 2006, pp. 50ff; STÖCKEL 2006, p. 268; RUPPEL 2007, pp. 94f; WINKLER et al. 2007, pp. 31f; AVERY et al. 2008, pp. 134f and 262f

covered by other proprietary rights. They might also be liable for cease-and-desist orders or claims for destruction of the products. In turn, they can be held liable by end customers if they sell lower-quality products[38].

The impact on the general economy has many forms, above all the loss of jobs, lost social security contributions, and lost tax revenue in the target countries[39]. The countries of origin experience both negative and positive effects. Taxes are paid and jobs are created, which improves the gross domestic product. However, foreign investors might be reticent about investing in countries that promote or tacitly accept counterfeiting. This can damage the natural advantages of the country and limits its domestic innovation capacities[40].

For the makers of the original products, the damage lies in the loss of market share and profit, the impact on their reputation, the undermining of the brand, and the additional costs for combating product piracy[41].

For these manufacturers, commercial success might therefore also depend on their ability to protect sensitive data and electronic communication from theft and misuse.

Overview of Potential Damages

The following table offers a brief overview of the potential impact of product piracy and the loss of know-how:

Immediate Impact	Medium-Term Impact	Long-Term Impact
Lost revenue	Damage to image	Lost procedural competence
Lost core competences	Pressure on prices / profit margins	Poorer location advantages
Lost innovation leadership	Loss of financial control	Official regulations
Lost time-to-market advantages	Chaotic controlling	Damage claims
Brand abuse (piracy)	Loss of market share	Cost of litigation
Unwarranted liability claims	Injuries	Recalls
	Cancelled orders	
	Customer boycotts	

[38] Cf. BRAUN 1993, p. 34; HOPKINS et al. 2003, pp. 164f; RUPPEL 2007, p. 95

[39] Cf. BRAUN 1993, p. 35; FUCHS et al. 2006, pp. 44 and pp. 53ff; WINKLER et al. 2007, p. 32; AVERY et al. 2008, pp. 134f and 307f

[40] RUPPEL 2007, p. 96f; also cf. HOPKINS et al. 2003, pp. 158ff and p. 182; WINKLER et al. 2007 p. 32

[41] AVERY et al. 2008, p. 307

4 Project Approach

Whenever a company begins to consider the introduction of product or know-how protection, the complexity of the topic demands an organized, focused approach. The introduction should ideally be set up as a project at the company.

Whenever possible, the project team should include stakeholders from all stages in the value chain for the products in question. This can include personnel from:

- Development,
- Design,
- Automation,
- Procurement,
- Production / Assembly,
- Corporate Security / IT,
- Logistics,
- Sales, and
- Marketing.

It should be noted that the involvement of external partners should be limited as far as possible in view of the sensitivity of the issue.

Complex questions, however, can require external support, e.g. from specialist consultants. They can add the necessary experience with assessing and evaluating threats and contribute expertise in developing effective countermeasures.

The required project budget can be based on the assumed or expected damages caused by counterfeiting. The effort needs to be commercially viable, which often requires a complex calculation. For the first step, we recommend using a simple payback calculation.

In the following model, we will outline a generic project for introducing protective measures.

Generic Model

This generic approach is meant as a frame of reference that companies can apply if they want to protect themselves against counterfeiters or the loss of know-how. The approach is equally suitable for protecting products and know-how. It allows the definition of a protection strategy for products just as much as a concept for defining and implementing know-how protection for processes.

1. Defining the Objectives for the Protection System

The first step consists in understanding and defining the targets that need to be protected, now and in the future. It needs to be defined what the future concept is meant to do.

What do I want to protect (PIMP)?

- Products
- Information
- Machines
- Processes

The targets need to be qualitative first and later supported with a quantitative basis. This will be essential for validating the chosen protection strategy in line with the performance criteria of the second step. Quantifying the often rather “soft” criteria is not an easy task; such soft targets should be translated into measurable indicators.

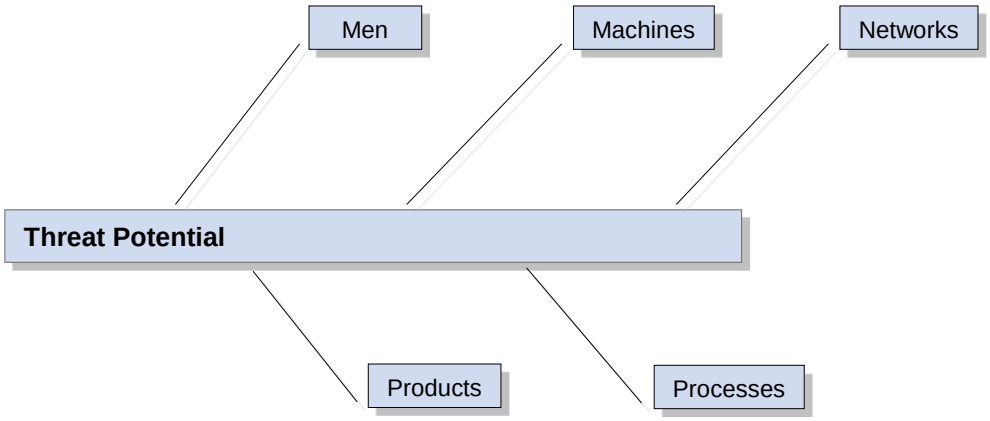
This step also needs to define which conditions need to be in place, resulting in a **specifications list** with targets and applicable conditions documented.

The project as a whole should be launched officially at this point and the people involved in it chosen, the necessary resources allocated, and the work started in a kick-off event.

2. Threat Analysis

The company's situation is reviewed in terms of the threats it is facing and the measures or protection systems that are already in place. The analysis should consider the strengths and weaknesses from the point of view of product and know-how protection.

The threat potential should be considered from various points of view (PIMP model):



The following methods have proven helpful for this purpose:

- Interviews with representatives from R&D, production, procurement, customer service, sales, logistics, service, or IT.
  The aim is to get a first overview concerning the status quo. Special checklists can help for this purpose.
- Analyzing the flow of information and products in the scope of the project, e.g. by checking available documents or using reverse engineering.
  Assumption: By emulating the point of view of potential counterfeiters or other perpetrators, it becomes possible to see the critical processes, components, and aspects at-risk.

The threats should be classified in the next two steps:

1. **Determining the risk factors**
   based on an analysis of the product or know-how-related aspects and the potential financial damage for the company.

   Sensitive know-how can take many forms, such as:

   - Proprietary design know-how

- Proprietary production or process know-how
- Strategies, indicators

2. **Determining the level of threat**
   by analyzing the threats and weak spots

   Current threats include:

- The theft of drawings (CAD)
- Loss of know-how to or by suppliers
- Reverse engineering of mechanical components
- Reverse engineering of electronic layout
- Reverse engineering of (embedded) software
- Copying of production processes, brands, or patent infringements.

It helps to visualize these risks. Risks in the process can be display along the value chain or the process itself with a traffic light system.

3. Defining Selection Criteria

This step covers the selection and definition of measures that can be included in the planned protection strategy.

The target protection level is defined first by considering the identified risk situation. It is calculated by weighing the current level of threat (low, abstract, clear and present) and its financial impact.

There are many different measures that can be taken. A systematic selection process is required, e.g. following the PIMP model (Process, Information, Machine, Product):

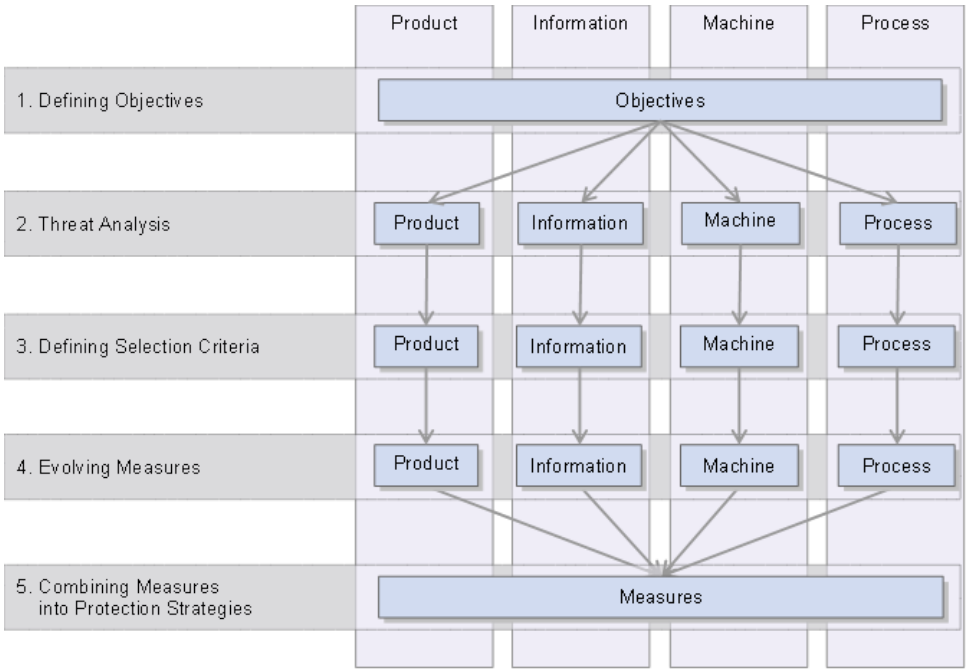


Chart: A systematic approach for selecting protection measures (PIMP model)

The measures are selected with a view to addressing the chosen targets and conditions.
Not all measures are necessary or, indeed, helpful. The chosen measures must eliminate a present or latent threat. Each measure can address one or more risks; at the same time, a single threat might need multiple countermeasures in response.

Ideally, the measures build on the inherent strengths of the company in question.

4. Evolving the Measures

When the available measures are applied to the given situation of the company, it is often necessary to adjust and develop them further in certain aspects.

It can also be required to continue evolving the available measures. Specialty areas of concern can be addressed in cooperation with external partners, such as vendors of IT solutions.

5. Combining Measures into Protection Strategies

The measures defined and fine-tuned in the last step are now combined into a suitable protection strategy, with due consideration for their mutual interaction and interdependency. Some measures tend to reinforce each other's effect; others cancel each other out. There are also measures that operate completely independently from one another.

It helps to compile the various possible interactions between the chosen measures in a so-called design structure matrix (cf. the following table) in order to develop effective protection strategies. Each concept includes a unique selection of fully or partially established measures with new measures.

	Measure 1	Measure 2	Measure 3
Measure 1	-	Reinforces	No interaction
Measure 2	Reinforces	-	Weakens
Measure 3	No interaction	Weakens	-

Table: Design Structure Matrix

6. Evaluating the Protection Strategies

The finished protection strategies need to be evaluated in terms of their effectiveness and efficiency for reducing the identified risks. This means understanding the costs and benefits of each protection strategy.

This is often a complex task as a result of the limited and incomplete information that is typically available. Applying the scenario technique, i.e. developing and testing alternative prospective scenarios has proven a helpful means for this purpose.

7. Selecting the Protection Strategy and Preparing Its Implementation

The most effective protection strategy should be chosen for implementation from the various options.

Implementing the protection scheme for products or know-how follows the usual implementation process used in projects of a similar nature.

Deadlines and responsibilities need to be defined for all specific tasks included in the protection strategy. A project budget is defined and approved. A project schedule is created and control mechanisms are put in place to track progress.

More complex projects benefit from the consolidation of the protection strategy with its set of defined measures in a specification.

8. Implementing the Protection Strategy

The measures that need to be implemented partially or completely to enable the protection strategy are executed by the assigned people.

Longer-term projects can benefit by being aware of the constantly changing circumstances in the markets. All measures should be able to fulfill their original function at the time of their actual launch.

The same applies to problems that occur during implementation. If the deviations from the plans are severe, it might be wise to rethink and revise the original protection strategy.

9. Validating the Protection Strategy

After the protection strategy has been put in place and first experiences with it have been gained, its effectiveness should be measured and evaluated. The key question is whether the goals that were identified have been achieved. An additional cost-benefit calculation is also recommended at this point.

Adjustments may be required if the strategy fails to achieve its objectives. This can mean revisions to individual components or the introduction of additional measures. The practicality of measures that have no visible effect should be critically reviewed if their application requires any costs or significant effort.

5 Solutions

5.1 Background Situation

The following solutions illustrate how the individual threats and responses relate to each other. For this purpose, the PIMP concept is applied to the fictional EDA Company.

Scenario: About “Elektronik Deutschland AG”

The EDA AG is a joint stock company based in Frankfurt am Main, Germany. Employing over 8,000 people, the EDA produces complex electronic components for clients in the automotive, mechanical engineering, aerospace, and defense sectors worldwide. The company is a global leader in its market and operates a broad distribution network, with production facilities in Brazil, Russia, and China. Its products are used in almost all vehicles and machines around the world. Its most critical products are specialist components for tanks, cruise missiles, and satellites, requiring exceptional know-how and offering a substantial ROI. The EDA uses machines and production equipment from a range of producers to stay flexible at all times. It invests more than 10% of its turnover into the development of new technologies, materials, and products, with over 2,000 patents in Germany alone, as evidence of its innovative capabilities. Products with lower production runs are produced in-house; the necessary production data and information is made available through a supplier-side extranet. Products for specialist markets, such as the Russian or the Brazilian market, are made and sold on site.

5.2 Problem Analysis with the PIMP Concept

Alexandra Schulz, Benno Scholze

Introduction Recently, the EDA has had to respond more frequently to the counterfeiting of its products. The copies have begun to resemble its products ever more closely in form and function. Retailers and customers are finding it increasingly difficult to determine whether they are buying an OEM part from the EDA in open retail. This development and the pressure on prices exerted by new producers from Brazil and Russia have led to a massive double-digit drop in revenue.

The loss of Intellectual Property seems to originate from inside the company, as the product copies are becoming increasingly sophisticated. The evidence points to leaks at suppliers and the company’s own international branches.

1. Objectives The board of the EDA has decided to introduce a sweeping anti-piracy strategy to combat the obvious know-how leaks. A combination of several measures is required for the purpose.

2. Threat Analysis

Applying the concept introduced in chp. 3, the threat analysis should cover the criteria:

- Products
- Information
- Machines
- Processes.

Since the threats faced by the EDA are many, all areas of the business should be reviewed.

For this purpose, interviews are conducted with the relevant personnel in R&D, production, procurement, sales, service, logistics, and IT, using comprehensive interview checklists to ascertain the nature of the threat.

Next, the flow of information and products is analyzed by reviewing the available documents, e.g. the quality manuals, production data, or sales and market information. The focus lies on understanding the perspective of potential counterfeiters, considering the critical processes, components, and market information as the threatened Intellectual Property.

The threats faced by the EDA are categorized in a two-step process:

1. Determining the risk factors:

The EDA identifies the following as particularly threatened know-how:

- Design information and related patents;
- New production technologies;
- Information about prices, customers, and markets.

2. Determining the threat situation:

Weak spots exist in terms of:

- The cooperation with external suppliers;
- Design drawings stored on a supplier extranet;
- The publication of patent records;
- International cooperation for special markets in Russia and Brazil.

The EDA visualizes these threats in swim lane models with suitable software, such as VISIO or ARIS, representing and organizing the threats with different colors (traffic light system).

The identified threats are then evaluated with the following formula:[42]

$$\texttt{PotentialDamage} = p_S \cdot \texttt{Amount}$$

with Ps signifying the likelihood of the damage occurring.

The EDA calculates the potential amount of damage in terms of the contribution margin lost as a result of products not sold, higher stock inventories / losses, and lower utilization of production capacities. The calculation also considers potential liability issues in terms of warranty costs and the cost of litigation.

[42] GEIGER 2009

3. Selection Criteria

The EDA is pursuing a high degree of protection, since the threats are seen as very clear and present, with financial damages already estimated at double digit figures in terms of lost revenue. In this respect, the current risk for the EDA can be considered severe.

The following measures are reviewed in the next step to check to what extent they fulfill the goals and can be introduced immediately given the current circumstances.

	Product	Information	Machines	Processes
Access and Usage Rights Concept	Making prototypes available only to certified customers and partners	Roles and access rights for CAD data	Controlling and limiting access to production plants and facilities	Four-eyes principle for controlling access
Communication Concept	Selective communication before launching innovations	Creating awareness in the workforce	Restrictive configuration of teleservices	Encrypted communication for data and language
Procurement Concept	Promoting cooperation with trustworthy partners	Reducing design data in procurement to the required minimum	In-house developments	Reviewing the extent of vertical integration

4. Evolving the Measures

These measures are developed further, adjusted, and integrated to create an effective protection strategy for the EDA (chp. 5.7).

Chapters 5.3 to 5.6 outline the measures and recommendations that prove relevant and effective for the situation faced by the EDA.

5.3 Procedural Solutions

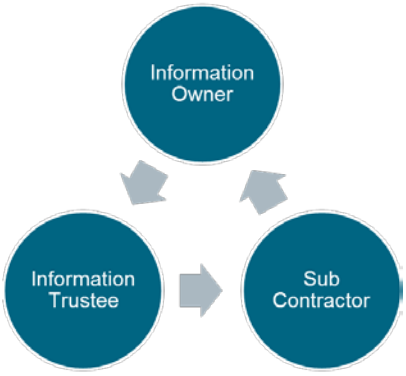
Peter Mnich, Benno Scholze

Procedural Solutions

Procedural solutions refer to mechanisms for protecting know-how and products in the information and business processes and throughout the product lifecycle.

The targets and actions can reach levels of complexity that call for treating them as a distinct management system.

Managing know-how protection requires identification of all relevant people, responsibilities, and processes and putting in place suitable processes for protecting sensitive information from access by unauthorized or other third parties. It also reduces the likelihood of misuse by authorized parties.



As a result of this process, the company gains a better understanding of the flow of sensitive information and its potential threats, and is therefore in a position to address the identified weak spots in the process chains.

Employees are enabled and empowered to recognize when information is sensitive and learn to use know-how protection measures. Creating general awareness makes it more likely that attacks will not go unnoticed.

Protecting information in all types of business transactions relies on well-planned strategy, with IT tools run by competent staff supporting the necessary processes in all project phases.

The essential process steps in the virtual scenario of the EDA are:

- A first joint consultation of all personnel involved in the process (information custodians) with the commissioning client, usually an internal client or functional unit (information owner) covering the plans in question (production, development, sales, projects).
- Identifying sensitive information and determining the degree of protection in terms of threats and potential implications.
- Allocating local branches or organizational departments to the people handling the information.
- Documenting the start and end of custodianship.
- Defining the involved personnel's authorization to access information.
- Selecting and defining individual know-how protection measures for the relevant information to match the identified threats.
- Defining and documenting the chosen and implemented know-how protection measures for the planned activities.
- Responding to and documenting any changes in the given circumstances (changed locations, involvement of additional parties, e.g. suppliers, etc.).
- Keeping project logs with a chronological record of all relevant project incidents.
- Defining indicators for project controlling and assuring the quality of the protection measures.

At the EDA, procedural solutions in the sense of a holistic know-how protection management system include:

- Analyzing and evaluating the required international standards:

  The EDA develops and produces components for the armaments industry. This means that the EDA is supported by the Federal Ministry of Economics and Technology in aspects of security; the security manual defines the organizational and procedural framework for a variety of personnel and material security measures.

  A distinction needs to be made between (official) security and internal know-how and product protection.

  The applicable legal requirements, standards, norms, and customer specifications also need to be verified.

  Integration with risk management is required to comply with the stipulations of the Act on Control and Transparency in Enterprises (early warning system).

- Developing a know-how / product protection manual that describes the management system. This covers e.g. the know-how protection strategy, responsibilities, and processes. It includes the regulations that act as the basis for all active steps.

- Developing and enforcing know-how protection standards in the form of methods, rules, activities, and indicators.

- Developing and implementing measures in the sense of an integral strategy; organizing know-how / product protection.

  For this purpose, the EDA has to organize comprehensive and globally applicable protection processes, including audits and improvements to existing processes and activities, the development methods and measures, incident management, and compliance standards (e.g. identification of noncompliance).

Protecting the EDA's processes means working in various areas:

- Secure cooperation with business partners

  This includes regulations, more awareness, and the behavior of all involved personnel in the handling and use of products, devices, information, and data through their entire lifecycles.

  Secure solutions for communication, such as shared data spaces and secure conference solutions also need to be used. IP-based encryption technology offers a holistic solution for protecting against the interception of verbal communication, conferences, or data spaces in a highly secure cloud solution. This allows keeping international communication secure in all sensitive processes.

  Contracts should be reviewed with a view to aspects of confidentiality and means of redress in the case of a breach of confidentiality.

  Suppliers should be evaluated and monitored on a permanent basis.

- Secure organization and use of central IT tools (cf. information-based solutions)

- Secure organization and use of relevant locations and venues

  This includes the entire physical security, safe access processes with defined roles and authorizations, trustworthy conference venues, secure development labs, safe mailing processes, trusted cleaning and waste disposal, controls, and incident management.

- Secure HR processes

  The EDA has to harmonize and implement the following processes across the organization:

  Recruitment with consideration for know-how protection criteria; HR and security clearances; HR development; redundancy / resignation processes.

- Security-conscious work processes

Since the EDA operates production facilities in Russia, Brazil, and China, its people need to be trained and made aware of the best practices for handling sensitive information with due consideration for the given circumstances, possible threats, and cultural aspects. The mandatory use of encrypted communication can help in everyday operations.

5.4 Information-Based Solutions

Dr. Harald Liese

Information-Based Solutions:

The IT-based protection of design and product data and of descriptive documents, that are related to the product, covers a number of areas: [43]

- **Protecting sensitive data with encryption technology**
- **Reduction of know-how in the product data (e.g. CAD data)**
- **Using simplified 3D models to protect intellectual property**

Protecting sensitive product data with encryption technology is particularly important when data is transmitted to other partners in the value chain. By means of a suitable solution the exchange of data via the internet is made secure and stable, transparent, and comfortable at the same time. To achieve this, a multi-level, highly secure encryption strategy needs to be in place. The encryption of all communication connections and of the data, the use of signatures and verification as well as data receipt confirmation processes must be enabled. The automated and secure exchange of mass data with high frequency of data flows can be ensured by a dedicated data exchange platform. Such a platform can be used for exchanging a variety of product data and information securely, e.g. even in the form of a sourcing platform for technical procurement. These processes can be controlled by an existing PDM solution. This makes it easy to implement the complete documentation of all data exchanged, the application of suitable encryption technology, and the automation of many processes. Another means to improve secure data exchange is the use of Enterprise Rights Management (ERM).

Reduction of know-how in the product data (e.g. CAD data) is another powerful protection measure. The contents of CAD models are a particularly easy means for accessing proprietary intellectual property when the models are shared with other partners in the value chain. Using special software modules, sensitive data can be removed automatically from the CAD data while complying with the demanding requirements of the data recipient regarding the scope of delivery and quality of the CAD data. Content removed before data exchange cannot be misused by the recipient at a later point. Therefore product know-how is removed from the CAD models or CAD drawings in a tailored way. Such data filtering can even be integrated in every day's data exchange by reliable processes.

Using **simplified 3D models** for Intellectual Property protection purposes can, for instance, be realized by means of 3D PDF. 3D data can be transmitted by embedding the 3D models in PDF documents that can be visualized via Adobe Reader. At the same time, this greatly improves the level of protection as the original CAD model is converted into the PDF format. The user can decide during that conversion with which level of precision and detail the model is to be embedded into the 3D PDF file. The system also allows the precise definition of what the recipient is authorized to do with the 3D PDF document. Conversion processes of this type can be automatically integrated into the company

[43] LIESE 2012

processes. Additionally the information stored in the 3D PDFs can be protected with Enterprise Rights Management (ERM), e.g. limiting access to the documents to specific users. Access rights can even be limited for specific periods of time, changed at a later date, or withdrawn altogether.

In case of the EDA AG the practical use of these protection means can be illustrated, because it is facing the following threats:

- Product data (including CAD data) is exchanged globally between many global development and production sites of the EDA and their suppliers and clients. In a number of cases, competitors have been producing counterfeit products before the actual original was available in the market. This points to a leak of design data at an early stage.
- When distributing tender documents and business proposals to suppliers, the EDA often discloses more information than would be required. The suppliers need information about 3D models for the tendering process, but usually not in the level of detail of the original CAD models, whose disclosure constitutes a threat for the EDA.
- In many cases, the EDA shares confidential digital data with partners by unsecured means. There is no coherent IT solution at the EDA that allows the encrypted exchange and sharing of digital data within the company or with external partners.

Working with a provider for PLM integration, there have been developed a number of solutions for EDA to enable the secure exchange of product data and its integration into the company's development areas and overall processes:

- Every kind of data transfer for all relevant departments is being automated with a web-based, highly secure encrypted data exchange platform. This platform is operated as a "Managed File Transfer" solution that integrates relevant suppliers by a portal. The scalable security of the solution is ensured by allowing encrypted connections and system-side as well as personal encryption of stored data. High-frequency data transfer of large data sets is also made possible in a secure way. Moreover the EDA is introducing the secure data exchange platform as a sourcing platform for technical procurement. Powerful and comfortable clients and extensive integration with the established IT systems (e.g. mail system, PDM system) achieve great acceptance among the users of the solution. The EDA has achieved the complete documentation of all data exchange transactions (tamper-proof record of all transfers) and the automation of many processes.
- Communication in the various business processes now makes far more use of 3D PDFs, e.g. for calling in proposals, in approval and revision processes, or even in drawingless production and the electronic distribution of sales and service documents. The PDF documents bring together 3D models and other product data from different sources into one structured document. The PDF document is created in an automated, replicable and procedurally reliable way and contains extensive security functions. 3D CAD models are, for instance, converted into PDF format to protect the Intellectual Property contained in them. Selected documents are additionally protected with Enterprise Rights Management.

- In cases in which the original CAD files need to be shared, certain product knowledge that the recipient does not need to complete his job is removed on a case-by-case basis from the CAD file. This is done by means of a dedicated software solution, which allows manual filtering where needed, but generally uses automated filters in response to queries from the data exchange platform. Even the selection of filters can be automated depending on the chosen recipient. The high CAD data quality required by the recipient is guaranteed thereby.

5.5 Machine-Based Solutions

Oliver Winzenried

Machine-Based Solutions: Protecting Machines with Preventative Technical Measures

Like many areas of business, machines and technical facilities are becoming more and more reliant on software functionalities; this typically takes the form of PLC software or so-called embedded software. Effective protection of this software makes its reproduction a much more challenging endeavor. The following mechanisms can act as protection against different attacks:

1. Protecting against reproduction
    - Complete machines are being copied by reproducing mechanical components or replacing standard components with similar parts. The software is simply copied to a new PLC. In such instances, encrypting the control or embedded software can prevent it from working with other controllers. Another option is to bind the software with the original machine's controller, e.g. by a form of serial number or another non-reproducible trait, a type of 'immobilizer' for the machine.
    - Especially effective procedures and algorithms are being reverse-engineered by counterfeiters for use in their machines. This saves the time and effort of in-house development. Again, encrypting the machine software prevents its disassembly or decompiling.
    - Service documents needed for repairs and maintenance often includes valuable Intellectual Property. Encrypting these documents can help make copies worthless and allows even authorized service technicians to only access and use the documents at the point of need.
2. Protecting against tampering and unauthorized changes
    - Another important object of protection is the machine's integrity to ensure that it is functioning correctly and fight the increasingly prevalent threat of industry computer viruses, such as Stuxnet, Duqu, or Flame.
    - There are many norms and standards governing specific mechanisms and processes for operational safety purposes ("safety"), i.e. averting dangers to human beings or the environment. Standards governing "Security", i.e. protecting against changes, are slowly being developed, such as the so-called Security Assurance

Level, SAL, in ISA 99 or IEC 61508. “Safety” can only be guaranteed if the correct functioning of its mechanisms is protected with “security”.

- The mutual authentication of control and embedded systems ensures the reliable operation of machines connected in automated production facilities. This also applies to so-called cyber-physical systems, i.e. embedded systems in critical infrastructures like smart grids, traffic controls, logistics, or building services as well as in Industry 4.0 systems.

3. Additional benefits of machine protection systems

   - Access limitation for service functions or settings. Functions that are included in the machine control system, but only meant for use by authorized service personnel, are stored in encrypted form. Service personnel can use these functions with authentication tokens.
   - New opportunities for the after-sales business are opened up when additional functionality can be sold or made available to the user by later software activation. This creates new business models like “Feature-On-Demand” or “Pay-Per-Use” models.
   - Production data processed by production machinery can be protected by encryption, and the number of products limited for each production run. Such systems are being used in the clothing industry to avoid factories from producing grey market goods in “fourth shifts” by simply continuing to use proprietary designs.

4. Solutions

   - Mechanical engineering firms tend to develop apparently secure solutions in house. This is a costly effort and often does not have the intended effect, which makes it more reasonable to apply standard solutions that the market offers.

Sample solutions for “Elektronik Deutschland AG”

As a large multinational corporation, Elektronik Deutschland AG works with masses of employees, numerous locations, and many suppliers around the world. Embedded security solutions and technical preventative measures help it produce the right responses to the following challenges:

- Protecting Intellectual Property by preventing the unauthorized access of electronic documents and the reverse engineering of particularly valuable proprietary processes and algorithms in the EDA’s control and embedded software.
- Protecting the control software of machines from different manufacturers with different automation concepts against reproduction, reverse engineering, and tampering.
- Using different signatures (“electronic signatures”) for different applications at various locations, such as code and document signatures, encryption, and verification processes.
- Secure sharing of know-how and documents in extranets by encrypting the documents and requiring authentication before any access by authorized parties.

The EDA's responds to these challenges with the following solutions:

1. Document protection:

   Encryption technology is used to protect documents against unauthorized access, i.e. reading. An optional electronic signature system is also available to ensure that documents are not tampered with. User rights are recorded in highly secure USB tokens. The management of these users rights can be accomplished by a fully automated and elegant corporate IT solution, such as an SAP ERP system. The rights are defined in intricate detail: validity from a certain date to a certain date or for a certain period; frequency of access; printing rights, etc.. The permission-based USB token can be secured additionally with passwords to protect against accidental loss.

2. Authentication
   a. USB tokens are used to access the extranet. By contrast to simple passwords that can be disclosed intentionally or unintentionally, these tokens are secure and can be protected further with passwords for a true two-factor authentication (knowledge and ownership). They can also be given a limited period of validity.
   b. Developers at various locations are also given USB tokens to access encrypted source code. They have the option to sign their code as a precondition for its use in machine control systems.

3. Software Protection

   Replace normal SD or CF memory cards in a PLC system or industry PC with special memory cards with integrated smart-card security component, adds the following protection layers to control and embedded systems:

   a. Protecting software against copying by encrypting it and allowing its use only with a matching smart card.
   b. Protecting software against tampering. Code signing with digital signatures means that the control systems can only use software from authorized developers. This helps identify unauthorized changes.
   c. Activating certain functions for service purposes.
   d. Mutual authentication of control components.

4. Flexible management of different markets:
   a. In different geographies or functional markets, certain machine functionalities can be protected or licensed in different forms, e.g. with time restrictions.
   b. Production data used in the machines can be protected with encryption and its use recorded and limited for different criteria, e.g. usage period or production volume.

5.6 Product-Based Solutions

Dr. Thomas Meiwald

Product-Based Solutions

The physical protection of the product in terms of the threat scenarios discussed above falls into four distinct categories:

1. Identification of original and counterfeit products
2. Protection against and proof of tampering
3. Identification of grey market trading
4. Prevention of hidden surplus production.

Identifying **original vs. counterfeit products** is accomplished by plain-sight, hidden, or digital markers. Consumers and end customers are served best by visible markers like holograms, color shifts, or other markers that they can verify manually, e.g. by mobile phone. The links in the supply chain are aided most effectively with visible and semi-visible markers (microtext on holograms etc.). The specialists of the brand owner can use hidden markers to distinguish original products from fakes. Hidden markers of this type are therefore a second line of defense that is particularly hard to see for the uninitiated. Digital means are particularly effective for actors in the supply chain who wish to automate their authentication processes. What any effective and coherent counterfeit protection system depends on is the application of the marker on the product or packaging at the end of each production flow. This keeps the costs and efforts for establishing and operating a safe zone manageable.

To protect against and prove cases of **tampering**, companies can apply various sealing technologies that cover a versatile range of functions. Creating reliable proof of the original opening, allowing re-sealing of the product, proving instances of tampering (with cutting markers, tearing of the packaging material, or intentional self-destruction of the label).

To uncover **grey market trading,** track and trace solutions offer means of tracing every single item by applying serialized authentication markers. Track & trace solutions integrated in this manner are a reliable means of identifying misappropriated, re-imported, or exchanged goods or documents and optimizing logistics processes down to the satisfied customer's doorstep. Specialist technology is available that allows producers to track which products are in circulation in which markets by following their users' authentication of marker codes. For such purposes, 15-figure alphanumerical codes or similar markers are attached that can be verified via the web or a dedicated call center. The product can therefore be authenticated at every step in the distribution chain.

The problem of **hidden surplus production** – the proverbial 'fourth shift' – can be addressed by similar means. Combined with a tamper-proof authentication marker, suppliers are thus prevented from marking surplus products unlawfully as originals.

These means of protection can be seen in action at the EDA AG, which is facing the following threat types:

- Deception of customers with lower-quality counterfeit products that are superficially almost indistinguishable from the original.
- Unauthorized opening of original shipments; removal of original products and inclusion of lower-quality counterfeits in the shipments.
- Suppliers not complying with their production batches and distributing both surplus and rejected products illegally.
- Wholesalers selling to regions for which they have not been authorized.

The situation was reviewed with the support of an expert provider of manipulation and counterfeiting protection solutions and a tailor-made protection strategy was developed. It is built around the following key elements:

- Marking of particularly sensitive components with direct laser application of a digital copy protection marker by the provider; this stops counterfeit products from entering the goods stream unnoticed.
- Sealing the transport containers with a unique logistics seal with security marker, including the following features:
    - Optimized gluing or attachment of security markers to prevent the non-destructive or unnoticed removal of markers.
    - Customer-specific multilayer holograms with plain-sight and hidden security markers.
    - Phone-readable combination of data matrix codes and digital copy protection that links product authentication with online customer communication. The customer can be informed e.g. about other traits of visible markers, such as holograms to avoid deception on the customer's side. The authentication queries also provide the EDA with data about where its products are in circulation and might uncover any potential leaks in the retail network. Serial production combined with the use of authentication markers stops suppliers from distributing more marker seals than required; surplus markers could not be authenticated in this manner.
    - Hidden security marker as back-up protection in the case of counterfeit logistics seals.

5.7 Protection Strategies

The newly developed and recommended measures and the measures that are already in place are combined into fields for action in a holistic protection strategy that mitigates or even removes the risk factors or concrete threats caused by the identified weak spots.

When combining individual measures in this way, the overall concept needs to take their mutual interdependency and effects on each other into account. A design structure matrix as outlined in chp. 4 makes it easier to take the step into a full-grown protection strategy.

At the EDA, the fields for action and protection strategy takes the following form:

Threat or Weak Spot	International cooperation to cover special markets Work with external suppliers Design drawings stored in a supplier extranet Publication of patent records

Protection Strategy	Access and Usage Rights Concept
Product	• Application of a digital copy protection marker • Use of specially adjusted logistics seals • Track & trace
Information	• Roles and access rights for product data • Reduction of know-how in the CAD data • Encryption / Enterprise Rights Management
Machines	• Document protection • Authentication • Software protection
Processes	• Global guidelines for classifying information • Reporting and monitoring • 4-eyes principle

Protection Strategy	Communication Concept
Product	• Selective communication before launching innovations
Information	• Use of dedicated platforms for the automated and secure data exchange
Machines	• Roles and access rights for documents with permission-based USB tokens
Processes	• Communication concept with defined roles, information handlers, and authorized parties for the entire information process • IT organization, Encrypted communication

Protection Strategy	Procurement Concept
Product	• Manipulation-proof application of unique plain-sight and hidden security markets
Information	• Case-by-case encryption for procurement purposes • Reduction of design data to the required minimum • Use of simplified 3D models
Machines	• Integrated software protection • Mutual authentication
Processes	• Regular review and checks of the trustworthiness of business partners with audits, trial purchases and penetration tests

6 Conclusions and a Look Ahead

Protecting products and know-how has become an indispensable part of life for the many reasons explained here. These guidelines show the various strategies, processes, and technologies recognized by the Working Group on Product and Know-How Protection that companies can already apply effectively to combat the threat of piracy.

These guidelines have introduced an overview of potential threats that should not be considered final or complete. However, understanding the methods and aims of the potential perpetrators and the specific damage they can cause for the property of your business can help you anticipate the risks for your business processes. The proposed and proven project approaches are designed to give you a starting point for finding and establishing the right protection measures to mitigate these risks.

The solutions described as part of the PIMP concept offer a selection of concrete preventative measures for protecting the products and intellectual property of many businesses across the economy.

Developing new and innovative tools for product and know-how protection will remain a necessary job, responding to the potentially predatory interests of state actors or competitors. The consumer's needs are also becoming ever more relevant, as the market demands and deserves simple-to-use means to authenticate the purchases. The call for ways to prove the authenticity and origin is particularly significant in more sensitive product areas, such as pharmaceutical or food products.

The VDMA has committed itself to working with and supporting users, producers, developers and consultants in mastering this challenge.

VDMA German Engineering Federation
Working Group Product and Know How Protection

Lyoner Strasse 18
60528 Frankfurt am Main
Germany

www.protect-ing.de

pks.vdma.org

7 Index

Appendix A: Glossary

Application Engineering	Development of components and systems
Breaking Bulk Strategy	Splitting mass production into smaller batches, including packaging, outer packaging, filling etc.
CAD models	Models produced with CAD systems, e.g. 3D volume models, surface models, or drawings. 3D CAD models are often parametric models with design history. They are an increasingly relevant record of Intellectual Property, stored as files and/or in PDM systems.
Design Structure Matrix	Matrix presentation of the dependencies between elements.
Embedded Security Solutions	Embedded systems are processing units with defined functionality that are integrated in a larger technical system, where they cover a range of tasks, usually without the user's knowledge. ***Embedded security*** deals with the IT security of the embedded systems by applying measures against unauthorized tampering in the procurement, transfer, processing, or storage of information. The use of encryption technology is a basic precondition for these solutions (cf. Dejan Lazich, IKS am KIT: http://www.iks.kit.edu/index.php?id=es-ss10&L=2)
ERM	Enterprise Rights Management (ERM) is a technical solution (based on cryptography) for securing the Intellectual Property of a company in distributed product development scenarios. ERM permits access to particular parts of a data record and to selected operations, …, generally achieved by encapsulating the data record in a protected envelope.[44]
Fourth Shift	The terms "fourth shift", "(factory) overruns", or "night-time production" refers to suppliers or manufacturing plants in general who have been approved by the brand owner to produce a certain volume of original products, but eventually produce more than that number. The surplus products are fully identical with the normal production run originals in terms of quality, function, branding etc. (cf. Hopkins et al. 2003, p. 9; Blume 2006, p. 47; Stöckel 2006, p. 267; Staake 2007, p. 22; Winkler et al. 2007, p. 65; Schaaf, Christian 2009, pp. 74ff)
Feature on demand	"Feature on demand" refers to the option to enable certain features at the point of need. Such features can be released – and their usage tracked – in devices or machines on a pay-per-use basis. This creates new business models for additional after-sales business in mechanical engineering.
First-to-market	A strategy aimed at being the first actor in a market as a means of gaining a competitive head-start.
Follow-the-leader	A strategy that relies on following the globalization strategy of a competitor, e.g. the market leader.
Intellectual Property	Intellectual property refers to intangible assets in the form of expertise, patents, innovations, symbols or similar assets that are essential for the

[44] ProSTEP iViP Association 2012 (I)

	workings of the business and are protected by exclusive proprietary rights. Trade secrets or other operational knowledge may or may not enjoy similar legal protections depending on the applicable jurisdiction.
Know-how	The know-how of a company refers to certain expertise or abilities that enable the business to produce its commercial performance (cf. Liman 1999, p. 116). These include both legally protected Intellectual Property (see above) and other intangible assets worthy of protection.
PDM	Product data management concerns product-related information management over the entire product life cycle in an enterprise. It also comprises a holistic approach to the planning, control, and review of processes required to generate and manage related data, documents, and resources.[45]
Product Counterfeiting	A counterfeit product means a combination of the unlawful use of another company's brand with a product designed to deceive the customers to trick them into mistaking the product for the original.
Product Piracy	Product piracy means referring to constellations with an OEM producer and a counterfeiter who is trying to poach market share or make a profit by copying the ideas of the original manufacturer.
Product Plagiarism	Product plagiarism refers to copying a product without trying to emulate its branding. (cf. Hopkins et al. 2003, p. 9)
Reverse Engineering	Reverse Engineering refers to the process of extracting the construction components of a given finished system or typically mass-produced product by exploring its structures, states, and operations. The finished product is turned into a construction plan again that becomes the starting point for counterfeiting. (cf. Blume 2006, p. 35; Winkler et al. 2007, p. 114)
Track & Trace	In logistics, tracking & tracing allows an insight into where goods are at a given point in time (track) and how they got there (trace). For this purpose, shipments are marked with machine-readable labels (barcode, data matrix code, RFID), also to allow tracing via GSM (Global System for Mobile Communications).
Underground Factories	Companies that operate in the underground, usually illegally.

[45] ProSTEP iViP Association 2012 (II)

Appendix B: Bibliography

AVERY et al. 2008

Avery, P.; Cerri, F.; Haie-Fayle, L.; Olsen, K. B.; Scorpecci, D.; Tryazowski, P. (ed.): The Economic Impact of Counterfeiting and Piracy. OECD, Paris (2008).

BLUME 2006

Blume, A.: Produkt- und Markenpiraterie in der VR China - eine politisch-ökonomische Analyse (Product and brand piracy in the PRC - a political-economic analysis), University of Trier, Trier (2006).

BRAUN 1993

Braun, E.: Produktpiraterie - Rechtsschutz durch Zivil-, Straf- und Verwaltungsrecht sowie ausgewählte Probleme der Rechtsverletzung (Legal protection against product piracy through through civil, criminal, and administrative legislation including selected problems of infringements), Cologne: Carl Heymanns Verlag KG 1993. ISBN: 3-452-22658-1. (IUS Informationis - Europäische Schriftenreihe zum Informationsrecht).

BREMICKER 2006

Bremicker, M.: In: Sokianos, N. P. (Hrsg.): Produkt- und Konzeptpiraterie - erkennen, vorbeugen, abwehren, nutzen, dulden (Product and concept piracy – recognize, prevent, repel, use, tolerate), 1st ed. Wiesbaden: Gabler 2006, p. 13. ISBN: 978-8349-0100-2.

BUGOW 2007

Bugow, R.: Mehr IT-Sicherheit beim Datenverkehr (More IT security in data traffic), CAD/CAM Report, Dressler, Heidelberg, 2007, p.12.

DELOITTE CHINESE SERVICES GROUP 2009

Deloitte Chinese Services Group: 2010 - Engaging China's five-year planning cycle. New York: Deloitte Development LLC 2009. (November - December 2009).

FUCHS 2007

Fuchs, H. J.: Die China AG - Zielmärkte und Strategien chinesischer Markenunternehmen in Deutschland und Europa (The China AG - target markets and brand strategies of Chinese companies in Germany and Europe), 1st ed. Munich: FinanzBuch Verlag GmbH 2007. ISBN: 978-3-89879-347-6.

FUCHS et al. 2006

Fuchs, H. J.; Kammerer, J.; Ma, X.; Rehn, I.: Piraten, Fälscher und Kopierer (Pirates, counterfeiters, and forgers), Wiesbaden: Gabler 2006. ISBN: 3-8349-0159-8.

GEIGER 2009

Geiger, R.: Wirtschaftlichkeitsanalyse von Schutzmaßnahmen gegen Produktpiraterie im Maschinenbau (Economic analysis of protective measures against piracy in mechanical engineering), IPRI Research Paper No. 24 2009, ISSN 1860-840X

HARTE-BAVENDAMM 2000

Harte-Bavendamm, H.: Handbuch der Markenpiraterie in Europa (Handbook of piracy in Europe), Munich: C. H. Beck'sche Verlagsbuchhandlung Oscar Beck, oHG 2000. ISBN: 3-406-45244-2.

HAUSCHILDT 1998

Hauschildt, J.: Promotoren - Antriebskräfte der Innovation (Promoters - drivers of innovation), Klagenfurt: 1998. ISBN: 3-85496-501-X. (Series "BWL aktuell").

HOPKINS et al. 2003

Hopkins, D.; Kontnik, L.; Turnage, M.: Counterfeiting Exposed - Protecting Your Brand and Customers. Hoboken, New Jersey, USA: John Wiley & Sons 2003. ISBN: 0-471-26990-5.

IMPULS FOUNDATION 007

Impuls Foundation (Eds.): China's strategies to become an innovative juggernaut. Stiftung für den Maschinenbau, den Anlagenbau und die Informationstechnik, Frankfurt (2007).

JONHANSSON 2006

Jonhansson, J. K.: Global Marketing - Foreign Entry, Local Marketing, & Global Management. 4th ed. New York: McGraw-Hill/Irwin 2006. ISBN: 007-124454-9.

LIESE et al. 2004

Liese, H., Stjepandic, J.: Konstruktionsmethodik: Wissensbasierende 3D-CAD-Modellierung (Design methodology: Knowledge-based 3D CAD modeling), CAD/CAM Report, Dressler Verlag, Heidelberg, 2004, p. 10.

LIESE 2012

Liese, H.: Schutz von Konstruktionsdaten, MEHRWERT DURCH SOFTWARE (Protection of construction data, ADDING VALUE WITH SOFTWARE), 12th ed. 2012, Fachverband Software im Verband Deutscher Maschinen und Anlagenbau e.V. (VDMA), VDMA Verlag GmbH.

LIMAN 1999

Liman, B.: Bewertung des irregulären Verlustes von Know-how - Schäden durch Wirtschaftsspionage und Fluktuation (Review of the irregular loss of Know-how - damage caused by industrial espionage and fluctuation), Cologne: Wirtschaftsverlag Bachem 1999. ISBN: 3-89172-416-0. (Series "Unternehmensführung und Personalwirtschaft" (Management and Human Resources)).

MEIWALD 2011

Meiwald, T.: Konzepte zum Schutz vor Produktpiraterie und unerwünschtem Know-how-Abfluss (Concepts for protection against piracy and unwanted Know-how drain), Dr. Hut Verlag, Munich 2011, ISBN 978-3-8439-0167-3

ProSTEP iViP Association 2012 (I)

ProSTEP iViP Association. Application Project "Enterprise Rights Management (ERM.Open)". http://www.prostep.org/de/projects/enterprise-rights-management-ermopen.html

ProSTEP iViP Association 2012 (II)

ProSTEP iViP Association. Glossary. http://www.prostep.org/en/footer/glossary.html

RUPPEL 2007

Ruppel, N.: Deutsche Unternehmen in China: Chancen und Risiken unter Berücksichtigung der Produkt- und Markenpiraterie (German companies in China: Opportunities and risks taking into account product and brand piracy). Hamburg: Diplomica GmbH 2007. ISBN: 978-3-8324-9361-5. (China Series).

SCHAAF 2009

Schaaf, C.: Industriespionage - Der große Angriff auf den Mittelstand (Industrial espionage - The great assault on the middle class), Stuttgart: Richard Boorberg Verlag GmbH & Co. KG 2009. ISBN: 978-3-415-04308-4.

SCHEWE 1992

Schewe, G.: Imitationsmanagement - Nachahmung als Option des Technologiemanagements (Management imitation - imitation as an option of technology management), Stuttgart:

Schäffer-Poeschel 1992. ISBN: 3-7910-0618-5. (Management von Forschung, Entwicklung und Innovation (Management of research, development, and innovation)).

SCHIWEK 2004

Schiwek, F.: Die Strafbarkeit der Markenpiraterie. Frankfurt am Main: Peter Lang GmbH 2004. ISBN: 3-631-52194-4. (Series “Rechtswissenschaften II” (Legal Sciences II)).

SEIDENSCHWARZ et al. 2008

Seidenschwarz, W.; Veit, D.: China is awakened - and some companies are disillusioned. Business Forum China 2/08 (2008) p. 4.

STAAKE 2007

Staake, R.: Counterfeit Trade - Economics and Countermeasures. Bamberg: Difo-Druck GmbH 2007.

STJEPANDIC et al. 2008

Stjepandic, J., Liese, H.: Methodischer Know-how-Schutz in der Automobilindustrie (Methodological Know-how protection in the automotive industry); lecture given at the VDI conference „CAD-Daten top secret“ (Top secret CAD data) in Munich, 2/3 December 2008, http://www.prostep.com/fileadmin/user_upload/prostep/Medienberichte/SD_2008/PROSTEP_Methodischer_Know-how-Schutz.pdf.

STÖCKEL 2006

Stöckel, M.: Handbook „Marken- und Designrecht“ (Trademark and design legislation), 2nd ed. Berlin: Erich Schmidt Verlag 2006. ISBN: 3-503-09039-8.

WENDENBURG 2010

Wendenburg, M.: Kein Patentrezept für den Schutzschild (No panacea for protection shields), DIGITAL ENGINEERING MAGAZIN, 3/2010, WIN-Verlag GmbH & Co.KG.

WILDEMANN et al. 2007

Wildemann, H.; Ann, C.; Broy, M.; Günthner, W.; Lindemann, U.: Plagiatschutz - Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie (Piracy protection – open options for manufacturers against piracy), Munich: TCW Transfer-Centrum 2007. ISBN: 978-3-937236-63-5.

WINKLER et al. 2007

Winkler, I.; Wang, X.: Made in China - Marken und Produktpiraterie - Strategien der Fälscher & Abwehrstrategien für Unternehmen (Made in China - Brand and product piracy - strategies of counterfeiters and defensive strategies for businesses), Frankfurt am Main: IKO - Verlag für interkulturelle Kommunikation 2007. ISBN: 978-3-88939-893-6.

Further Reading:

BITKOM:

- Eingebettete Systeme – Anwendungsbeispiele, Zahlen und Trends (Embedded systems - examples, figures and trends), February 2010, http://www.bitkom.org/60376.aspx?url=EingebetteteSysteme_web.pdf&mode=0&b=Themen
- Nationale Roadmap Embedded Systems (National roadmap for embedded systems), December 2009, http://www.bitkom.org/files/documents/NRMES_2009_einseitig.pdf

Federal Office for Information Security, BSI

- Die Lage der IT-Sicherheit in Deutschland 2011 (The situation of IT security in Germany 2011), May 2011, https://www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html
- Industrial Control System Security - Top 10 Threats, 12 April 2012, https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Analysen/Statistiken/BSIa004.html

Trusted Computing Group

- Trusted Platform Module Specification, http://www.trustedcomputinggroup.org/developers/trusted_platform_module

VDMA

- Survey on Product and Brand Piracy, 9 April 2010 and 23 April 2012
- Piraterierobuste Gestaltung von Produkten Prozessen (Robust product design processes against piracy), volume 1 of the series „Innovation gegen Produktpiraterie“ (Innovation against product piracy), VDMA Verlag, ISBN 978-3-8163-0601-6 October 2010
- Study "Status Quo des Know-how-Schutzes im Maschinen- und Anlagenbau" (Status Quo of the protection Know-how for machine and plant construction), 8 April 2013

Acatech

- CYBER-PHYSICAL SYSTEMS, Manfred Broy (Hrsg.), Springer, ISBN 978-3-642-14498-1

Appendix C: Authors and Contributors

The following list covers all persons who actively contributed to the development of these guidelines.

	Company	Internet	Contact
	3S Simons Security Systems GmbH	www.secutag.com	Rolf Simons
	Fraunhofer AISEC	aisec.fraunhofer.de	Bartol Filipovic
	Icon-X GmbH	www.icon-x.de	Alexandra Schulz
	Navayo Technologies	www.navayo.net	Benno Scholze
	PROSTEP AG	www.prostep.com	Dr Harald Liese
	Schreiner Group	www.schreiner-group.com	Dr Thomas Meiwald
	VICCON GmbH	www.viccon.de	Peter Mnich
	WIBU-SYSTEMS AG	www.wibu.com	Oliver Winzenried