Piracy Risk and Measure Analysis

***A. Albers, L. Marxen, J. Oerding, M. Meboldt,* Thomas Schäffer**
IPEK Institute of Product Development Karlsruhe
Kaiserstr. 10, 76131 Karlsruhe
+49 721 / 608-2371, +49 721 / 608-6051
info@ipek.uni-karlsruhe.de

Summary

Product Piracy has become a more and more serious threat over the past years, especially for small and medium businesses, whose competitiveness strongly depends on their ability to come up with new, innovative solutions. Generally, those businesses have proven to be successfully matching that primary challenge. Protecting products from counterfeit is a secondary challenge, that smaller businesses have difficulty coping with, due to a lack of practice and information.

Therefore, intensified research is necessary to strengthen the businesses in need of solutions. This paper will suggest a new approach, analysing and minimizing potential risks of piracy in the early stages of the development process rather than only curing the results of piracy after it occurred and already caused damage. The suggested approach is a PRMA (Piracy Risk and Measure Analysis). It is based on the logic of FMEA (Failure Mode and Effect Analysis), predetermining the risk and severity of a product being copied as well as the effectiveness of available countermeasures. Using methods that have already been established (i.e. in the field of quality management) is promising in general. Therefore, an outlook on prospective other methods, whose logic can be adapted to piracy risk determination is given in the end of this paper.

Keywords

product piracy, product counterfeiting, FMEA, PRMA

1 Introduction

Markets are rapidly expanding, using worldwide resources to support manufacturers' supply chains. Therefore, the phenomenon of product piracy is no longer only a matter of large enterprises. Small and medium businesses in the field of mechanical engineering are suffering more and more from intellectual property theft and counterfeiting of their products. In this new, globalised setting, product protection is becoming a more and more important key to success. Individual businesses with their own products need individual solutions. General strategies against product piracy are limited mostly to legal measures, acting curatively. Therefore, there is a need to develop preventive strategies and methods, to protect businesses from counterfeiting of their products.

The choice of possible strategies to minimize piracy risks has become large. Speeding up life- and development cycles, fast changing product generations, secrecy of knowledge-driven processes, integrated constructive protective measures to integration of high-tech micro electronic devices such as RFID tags only represent part of the available options. This large variety is hard to oversee for most companies, so it is difficult to know which option is the best for which product.

1.1 Product development

Product development and business economics have become strongly integrated. Design theories of the eighties have developed into strategic business processes driven not only by the engineers, but also by the companies' upper management. Especially Cooper has turned strictly design based product development into business oriented processes through his stage gate model [CO02]. The risks and cost of piracy can mainly be analysed from an economical point of view, whereas countermeasures against those risks can mainly be taken on the design side. There are already well established methods of which the logical approach can also be used in this field. Quality management is widely using FMEA (failure mode and effect analysis) to reveal potential weaknesses of products in their very early stages of development. Adapting that method to reveal weak spots in the context of product piracy seems very promising [PFE96].

1.2 Product piracy

Talking about piracy, one has to consider that there is a certain variety of types of piracy. Most important to distinguish are brand piracy and product piracy, not only because legally, those are different offenses.

Types of piracy

According to [BF07], brand Piracy is the illegal use of signs, names, logos and business labels, used by the original equipment manufacturer to distinguish their products in trade. Product piracy on the other hand is defined as the forbidden reengineering and reproducing of goods of which the legal producers are in possession of intellectual property rights.

Appearance

According to statistics by the European Commission, 87% of confiscated goods at European borders are cases of brand piracy [EC06]. However, the numbers of reengineered products and cases of product piracy are rising. Also, the estimated number of unreported cases of product piracy as compared to brand piracy is potentially higher, since there is a larger amount of small and medium businesses. Brand pirates mostly focus on large companies with valuable brand names. Those companies can afford to pursue the pirates, whereas small businesses might not have the time and money, to actually go to court.

Consequences

Both brand and product piracy damage not only OEMs but also customers buying counterfeit products and the economy of countries producing counterfeit products [WI+06].

OEMs' primarily suffer from loss of sales. This is caused both by customers knowingly buying illegal copies as well as those unknowingly buying piracy material. Apart from that, loss of reputation and resulting depreciation of the brand name are indirect consequences. Customers, dissatisfied with a counterfeit product might still relate the inferior quality to the OEM. Finally, warranty claims from customers that have unknowingly been using an illegal copy causes a serious problem for some companies, since they have to prove that the product claimed is not theirs.

Customers that buy an illegal copy of a product without knowing about it usually purchase an article with inferior quality.

1.3 Product Piracy Countermeasures

Countermeasures against product piracy can generally be divided into two groups: technologies and strategies. Strategic measures vary from applying intellectual property rights, to high confidentiality of crucial data. Within the European Union, governments are trying to support businesses through new laws, to strengthen their economy. Since 2004, i.e. owners of European-registered trademarks can apply for customs confiscation of illegal copies of their products throughout the EU at no charge. Before, costs varied from a few thousand to over a hundred thousand Euros, per country [KATZ04].

There is also a growing amount of technologies available that can be added to a product or its wrapping, to secure it from being copied. However, it is important to be aware, that the problem is not a lack of methods and technologies or strategies available. The real problem is, that most businesses affected or potentially affected by piracy, do not know how to choose the right protection for their product.

The following paragraphs will give a short overview over some of the available technologies today.

Radio Frequency Identification (RFID)

RFID tags also known as *Smartlabels, electronic imprints* and *electronic tags,* can be categorized into passive and active transponders. Passive transponders are smaller, but can only be read from short distances. Active transponders have an integrated power supply and send their signals over a distance of more than a hundred meters. *RFID* is still one of the most expensive technologies and therefore not yet widespread. However, experts predict strong growth and with that, a strong reduction in prices, so it is likely that in future, a large number of businesses will try and protect their products through identification and tracing of its products using this technology.

Barcode and Matrix Code Nano Codes

A cheap alternative to RFID tags are Barcodes. The stripes represent a number that contains information about a product's serial number, its manufacturer, country of origin, batch number, and so on [LE03]. Barcodes can be used to identify a product. To achieve security against counterfeiting, the parts and products must be identified many times along the supply chain. The information about the time and place of the product can be added to a database. Missing barcodes or inconsistencies about a products history can indicate that it is a fake.

Matrix codes work the same way as barcodes. They are two dimensional and can carry more information or more safely decoded information, if the same size as a barcode. Vice versa, if only little information is needed, matrix codes are much smaller than barcodes, which makes it easier to integrate them into the product design.

Image 1: RFID-tag (left), Barcode (middle) and Matrix Code (right)

Three-dimensional barcodes can be realized through shaping a small cube, attached to the products surface, through nano technology. They are even smaller than matrix codes and harder to copy but also more expensive, not only in manufacturing, but also reading them is cost intensive, as this can only be done with the help of a electronic microscope. It's use is only interesting for luxury products such as diamonds [HA05].

Hologram

Holograms are nowadays widespread. They are openly visible and are supposed to help the customer or sales professional to recognize the authenticity of the product. They are an eye-catcher and have a positive influence on the customer's perception of the product's quality [WE+07].

However, there is a large scope in quality of the holograms. Simple versions are cheap to produce but can be easily copied. The fact that the majority of the producers of holograms are based in countries known for a high rate of product piracy should be taken as a warning, to be very careful when choosing a supplier [SO06]. Holograms cost between 8 and 24 eurocents, so they are not applicable for any type of product [FU06].

Digital Watermarks

Regular watermarks are a translucent signature added to an objects appearance, well known from banknotes. The digital version also adds information to an object that is not clearly visible to the human eye and cannot be completely copied. To read a digital watermark one can for example use a digital camera and an analyzing software able to decode and translate the hidden information. The printing of digital watermarks can be integrated in existing printing processes and is therefore very cost efficient [MA05].

Laser Surface Authentication (LSA)

LSA is based on the fact that each individual product reflects a laser beam in a distinguished manner. With a special laser, a defiened area of a product's surface can be analyzed, so that an individual "fingerprint" can be taken. Comparing the fingerprint with a database, one can detect whether a product is the original or has been exchanged with a fake. This way of recognizing a product's authenticity is copy-proof, but necessary hardware is expensive [BR+07].

Micro Color Particles

This technology available from several suppliers, uses extremely small particles made of plastics, that are invisible to the human eye. They consist of several different coloured layers, each only a few nanometres in thickness. The order of the different colours is a code distinguishing one product from another. A special hand held reader can magnify and analyze the particles on a product. The particles can be added to ink, transparent varnish or even polyester fibres. The cost for this technology is less than one cent per article [FU06].

Special Printing Techniques

There are different techniques of printing, to distinguish a products wrapping. They make it harder for pirates to copy the product, but are not a hundred percent safe against counterfeiting.

Microtext includes microscopic patterns such as pictures or text in the macroscopic appearance [WE+07]. Similar to *Microtext*, *Guilloche Patterns* are very small patterns integrated into a design. They are cheap to produce, therefore easy to reproduce. However, simple copying is not that easy.

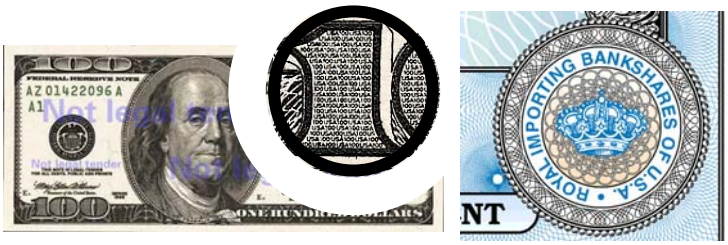

Image 2: Microtext on a US banknote (left) and guiloche pattern (right)

Special Ink

Apart from specialized printing techniques, the use of adapted ink that cannot easily be copied by product pirates is a possible countermeasure. Especially since it is not openly visible, that the ink has been manipulated, product pirates are not aware of the countermeasure and might get caught. The variety of special ink systems is large, so only a limited choice can be presented in this paper. To name a few, there is *Optically Variable Inks*, that change colour depending on the angle from which one looks at the print.

Thermochrome Ink changes its colour when the temperature reaches a certain level.

Infrared Inks are only visible under infrared lamps. Prints cannot be copied with a graphic scanner.

Fluorescent Colours are only visible under UV-lamps and work similar to infrared ink

Seals

Several companies offer a broad variety of seals, equipped with a combination of holograms, special inks and printing techniques that make it very hard to copy those seals. Applying them to the wrapping of a product ensures that any manipulation of the package can be easily detected. This way, pirates can be deterred from copying a product.

2 Anti Product Piracy Methodology

Small and medium businesses suffer the most from counterfeiting. However, there are no methods to assist businesses when choosing countermeasures. This barrier can lead to scepticism and wrong choice. The goal is to support businesses with a practicable set of methods, independent from specific products, to analyze, identify, and evaluate piracy risks and potential countermeasures. The approach is to built a database containing available technologies, and to use the logic of the FMEA to evaluate piracy risks.

2.1 Anti Piracy Database

Currently, there is no available practicable overview over the permanently changing and growing set of strategies and technologies to prevent piracy but also changing risks of piracy. Therefore, the first step towards a general anti piracy methodology must be to collect analyze and describe all known piracy risks and countermeasures along with their advantages, disadvantages and potential usage. The results will be documented in an anti piracy database. One of the most severe difficulties when choosing countermeasures is the offset in time between the necessary protection and the piracy risk it is supposed to minimize. For this reason the risks and countermeasures not only have to be documented, but the relation between them needs to be clear.

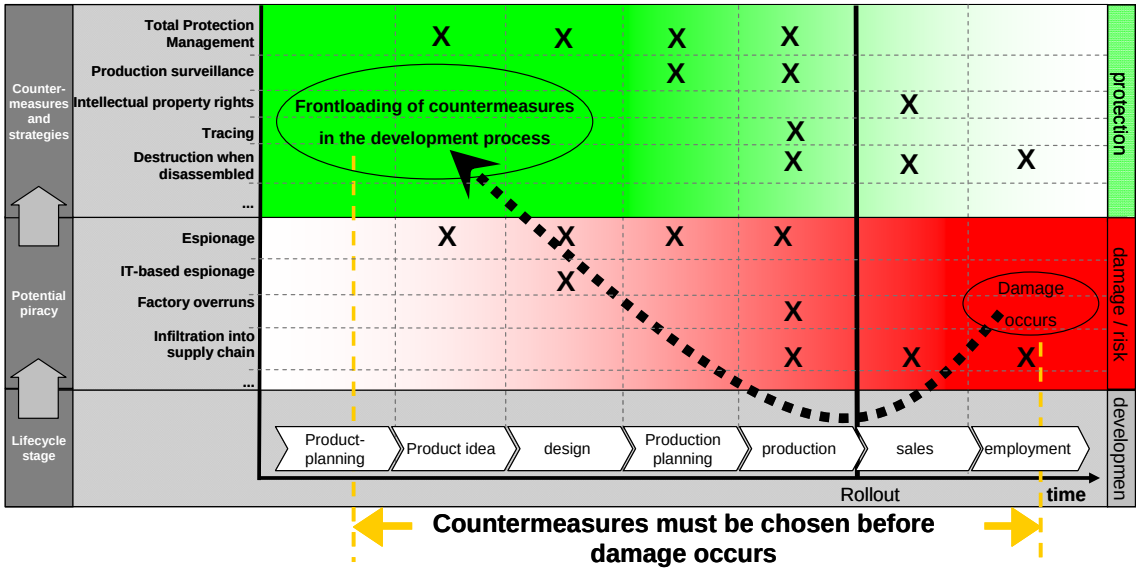

Image 3: frontloading of countermeasures

When the product profile is being defined the type of good should be clear. Brand name products with a valuable brand image i.e. are more likely to be consciously bought as counterfeit products. Protective measures must be adapted to such influences. For aftermarket products such as. spare parts, the situation is completely different. Often, customers are not willing to accept safety risks by purchasing fake parts. However, copies can have an identical appearance, so it is difficult to recognize the counterfeit. When the part fails, the damage can be rather big. Especially problematic are cases, where personal damage has been done. In that case, a different class of protective measures is available. The original parts have to be made recognizable i.e. through product DNA, watermarks, RFID or ohters. These examples are supposed to emphasize, that the best protection depends on the product, its market and its customers. Therefore it is important that product developers have tools and methods at hand, to evaluate those factors in early development stages

2.2 Piracy Risk Analysis

To protect individual products one needs individual solutions. In order to choose and adapt countermeasures from the anti piracy database, it will be necessary to identify the right ones. Therefore, a method to analyze potential risks in early stages of development is needed. In this paper, the general logic of the FMEA is adapted so that it suits the strategic choosing of countermeasures.

FMEA

The general FMEA compares concepts and solutions in early product development by calculating the **r**isk **p**riority **n**umber (*RPN*). It consists of three multipliers: severity (*S*), occurrence (*O*) and detection (*D*). Each of the factors is given a value between 1 and 10, so that the *RPN* will be evaluated between 1 and 1000.

S describes the **severity** of the consequences, if a failure occurs, i.e. failure of a car's brake-system would be more severe than the failure of its navigation system. The **occurrence *O*** quantifies the likelihood of the failure. A car's navigation system is more likely to fail, than a redundant brake system, for example. The **detection *D*** describes how easy the failure is to be detected prior to its consequences? If the satellite receiver of the navigation system is broken, electronics will notice when starting the car, that there is no signal, therefore it would get a low value. A weak brake tube on the other hand can hardly be detected prior to its failure, so the detection value would be very high.

Piracy Risk Analysis

The piracy risk analysis is used to evaluate piracy risks, depending on trade, technology and market. In accordance to the FMEA described above, the piracy risk analysis provides the PRN, the **p**iracy **r**isk **n**umber, consisting of the three factors as well.

$$PRN = S_P \times O_P \times D_P$$

In accordance to a general FMEA, for each factor a value between 1 and 10 is determined. This results in a PRN between 1 and 1000.

The **Severity S_P** indicates what kind of damage can be done to the company and in general, if the product is counterfeit. Loss of sales, lawsuits and rising warranty costs damage the company directly. Other damage that must be taken into account are consequences for man and nature. Fake medication can severely damage a person's health. Fake parts in industrial engineering could lead to environmental damage. All that needs to be taken into account. Furthermore, the **occurrence O_P** quantifies how likely a pirate will try to reengineer the product or parts of it. How attractive is it for a potential pirate? The growing awareness of product piracy leading to more statics should allow quantifying the likelihood in the future. Also helpful factors to determine O_P are:

Distribution channels - selling a fake watch on eBay is easier than selling fake spare parts in aviation.

Spread - a product that is cheap to manufacture is more likely to be reengineered than cost intensive products, as the pirate's potential benefit is higher, accompanied by low necessary investments.

Customer awareness - investment goods a lot of times are being purchased by employed purchasing personnel, so it can be harder for a pirate to sell his fake product.

Customer demand - Depending on the product, customers consciously buy fake products. Prominent examples are luxury watches and clothing. In those the market is very attractive for pirates.

The **detection D_P** evaluates how easy the fake product can be recognized as such? Whole product's copies are mostly easy to detect. Fake parts, that are hidden within the product are not easy to detect and often are only discovered, after they have led to early failure of the product.

Piracy Risk and Measure Analysis (PRMA)

The PRMA can be used to benchmark product ideas, concepts and products. It uses a fourth factor, the preventability *P*. This factor takes into account that some products are easier to protect against piracy than others. It ranges from 1 to 10, so PRN_{ext} scopes between 1 and 100 and indicates a product's robustness against piracy.

$$PRN_{ext} = \frac{S_P \times O_P \times D_P}{P}$$

The **preventability P** shows how effective countermeasures are that can be used with a specific product?

Table 1: Adapted Piracy-FMEA

FMEA		**PRA**		**PRMA**	
$RPN = S \times O \times D$		$PRN = S_P \times O_P \times D_P$		$PRN_{ext} = \frac{S_P \times O_P \times D_P}{P}$	
Risk **P**riority **N**umber		**P**iracy **R**isk **N**umber		**Extended P**iracy **R**isk **N**umber	
Severity	How bad is the potential failure?	Severity	How severe are the consequences if product is counterfeit?	Severity	How severe are the consequences if product is counterfeit?
Occurrence	How likely is the failure?	Occurrence	How likely is the product to be counterfeit	Occurrence	How likely is the product to be counterfeit
Detection	How easily can the failure be detected before it does any damage is done?	Detection	How easily can the fake be discovered before it generates company losses?	Detection	How easily can the fake be discovered before it generates company losses?
				Preventability	How effectively can the Piracy be prevented?

3 Summary

The growing threat of companies' losses caused by product piracy has to be minimized by new methods. This paper has shown how piracy risks can be systematically analysed through an adapted FMEA. Protective action can then be taken. An anti piracy database will support businesses to take the most sensible actions. For specific products and concepts, the extended piracy FMEA helps to benchmark between different solutions, determining the products' robustness against counterfeiting.

In the future, further methods should be adapted to the specifics of product piracy. Scenario management and QFD are both methods, suitable for this cause. Furthermore, there is a need to develop instruments and tools to help integrate those methods into the product development process.

Another difficulty protecting products against potential piracy is that it will usually make the product more expensive. However, customers will hardly be willing to pay more for a copy-proof product, as there is no direct benefit for them. Since it is very difficult to evaluate the cost-value ratio for piracy countermeasures, there is a lot of research that needs to be done, in order to enable businesses to protect their innovations against piracy not only effectively but also in a cost-efficient way.

Literature

[BF07] BUNDESFINANZMINISTERIUM: *„Gewerblicher Rechtsschutz Jahresbericht 2006“*
Berlin, 2007

[BR+07] BRÜLL, L.; FRIEDRICH, M.*: Laser-Streulichtmessungen zur Verpackungsidentifizierung und -verfolgung - Einsatzmöglichkeiten in der Prozessindustrie*
Bayer Technology Services GmbH, Leverkusen 2007

[CO02] COOPER R. J.: *Top oder Flop in der Produktentwicklung*
Wily, Weinheim 2002.

[EC06] EURPEAN COMISSION: *Summary of Community Customs Activities on Counterfeit and Piracy – Results at the European Border 2006*

[FU06] FUCHS, H.-J.: *Piraten, Fälscher und Kopierer*
Gabler, Wiesbaden, 2006

[HA05] HAMER, M.: *3D barcodes to identify stolen valuables* - New Scientist, issue 2510
Reed Business Information Ltd UK 2005

[KATZ04] KATZENSTEINER, T.*: Überraschung Ost* - in Wirtschaftswoche Nr.6 2004, Verlagsgruppe Handelsblatt GmbH, Düsseldorf 2004

[LE03] LENK, B.: *Handbuch der automatischen Identifikation*
Band 1, 2. Auflage, Lenk Monika Fachbuchverlag, Kirchheim, 2003

[MA+05] MALIK, H.; SCHINDLER, S.: FÄLSCHUNGSSICHERE VERPACKUNGEN
Malik (editor), 2005

[PFE96] PFEIFER, T.: *Qualitätsmanagement: Strategien, Methoden, Techniken*
Hanser, München, Wien: 2006

[SO06] SOKIANOS N.P.: *Produkt- und Konzeptpiraterie*
Gabler, Wiesbaden, 2006

[WE+07] WELSER, M. V.; GONZÁLES, A: *Marken- und Produktpiraterie*
Wiley, Weinheim, 2007

[WI+06] WILDEMANN ET AL.: *Plagiatschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie*
TCW, München, 2006

Authors

Prof. Dr.-Ing. Dr. h. c. Albert Albers

IPEK – Institut of Product Development, University of Karlsruhe (TH)

76128 Karlsruhe, Germany

e-mail: sekreteriat@ipek.uni-karlsruhe.de, phone: +49-(0)721-608/2371

Dipl.-Ing. Leif Marxen

IPEK – Institut of Product Development, University of Karlsruhe (TH)

76128 Karlsruhe, Germany

e-mail: marxen@ipek.uni-karlsruhe.de, phone: +49-(0)721-608/3953

Dipl.-Ing. Mirko Meboldt

IPEK – Institut of Product Development, University of Karlsruhe (TH)

76128 Karlsruhe, Germany

e-mail: meboldt@ipek.uni-karlsruhe.de, phone: +49-(0)721-608/8062

Dipl.-Ing. Jochen Oerding

IPEK – Institut of Product Development, University of Karlsruhe (TH)

76128 Karlsruhe, Germany

e-mail: oerding@ipek.uni-karlsruhe.de, phone: +49-(0)721-608/8061

cand. wi.-ing. Thomas Schäffer

Vorholzstrasse 14

76137 Karlsruhe, Germany

e-mail: th.schaeffer@gmx.de; phone: +49-(0)174 / 6590085