OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Ensuring Know-how Protection in Production

Günther Schuh[1], Matthias Kreimeier[2]
[1]*Department of Technology Management, Fraunhofer Institute for Production Technology, Aachen, Germany*
[2]*Department of Technology Management, Fraunhofer Institute for Production Technology, Aachen, Germany*

Aabstract: *While many different product protection measures have been developed and established in recent years, there is still a great risk posed by the leakage of knowledge in production. These risks are often downplayed by companies, although they directly relate to their own production and engineering know-how. The various company-specific protection measures in production span a wide range, and they can be applied both to production relocation (e.g. to China) and to existing facilities. A systematic approach for identifying critical damage scenarios, and the methodically supported development and selection of individual protection measures are required for effective protection of critical company know-how in production.*

Keywords: *know-how protection measures, outsourcing, product piracy, production processes, risk assessment.*

I. Motivation and Challenges

The damage to the Gkerman mechanical engineering sector caused by product piracy has been growing steadily in recent years, and reached approximately 7.9 billion Euros in 2013[[1]]. According to a study by the VDMA (association of the German mechanical engineering industry) conducted with companies in Germany, more than 71 percent of the participants are affected by product and/ or brand piracy. Nowadays, not only designs, but also components and entire machinesare being plagiarized. The majority of plagiarism originates from the People's Republic of China (72%), followed by Germany (23%), Turkey (20%), and India (19%). Overall, the percentage of plagiarism from other countries has also been increasing [[1]].

Despite these developments and the high number of plagiarism cases from countries such as India and China, the trend to outsource production to these countries continues to develop [[2]]. Although the "outsourcing hype" has decreased in recent years, the absolute number of outsourced production continues to rise further. The main motive behind this remains the reduction in personnel costs. Therefore, the companies that seek “price leadership” are primarily those who outsource their production. Additionally, companies are increasingly tending to outsource their non-core production in order to focus on core products and components. Of course, the rapid growth of the market in China, and the requirement of having local production also play a crucial role. In addition to the electrical and textile industry, companies in the automotive and mechanical engineering industries continue to outsource their production capacities [[2]]. Technological and organizational measures can be taken to protect know-how while establishing the production and onsite throughout the production process itself. Effective protection is particularly necessary and important in cases where specific technological knowledge is necessary for production.

Many protective measures against product piracy have been developed in the past, and have already become standard (e.g. special product labelling). Similarly, methods have already been developed for the evaluation and selection of protective measures. The Product Piracy Conflict (PPC) matrix is an example [[3]]. However, the protection of a company’s own production know-how has not receivedsufficient attention yet. With a systematic approach to assess possible damage scenarios and to identify and develop effective protection measures, the risk of a leakage of knowledge can be sustainably minimized [[4], [5], [6]].

II. Methodology For Establishing Knowledge-Protected Production

The procedure for developing effective knowledge protection in production includes three essential elements. After the identification of critical damage scenarios, appropriate safeguards should be researched and/ or developed. A reassessment of damage scenarios while taking the developed protective measures into consideration then forms the basis for establishing a plan of action and the development of further protective measures. The implementation and periodic review of the effectiveness of protective measures can then be carried out. Figure 1shows the entire procedure with further sub-steps in accordance with the process proposed

by Marxen et al. forconducting a piracy risk and measures analysis (PRMA) to systematically identify potential hazards caused by product piracy [[7]].

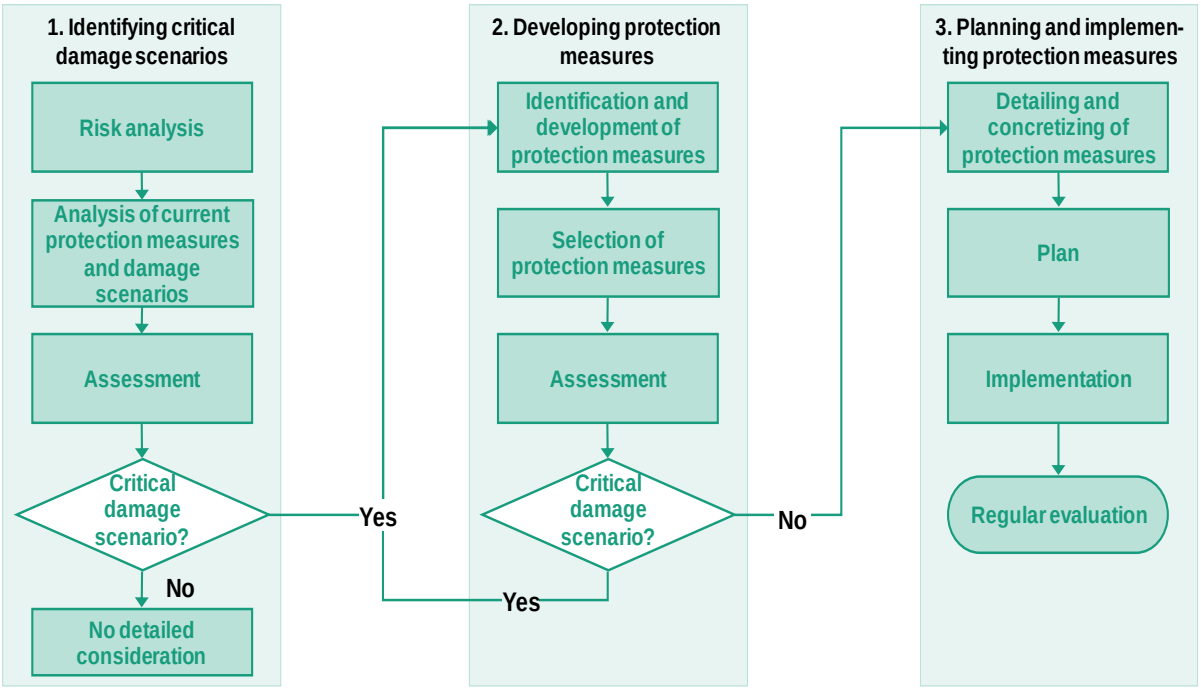

Figure 1: Methodology for developing a know-how protection concept in production

III. Identifying Critical Damage Scenarios

A risk analysis of the entire product production process serves as the starting point for identifying possible critical damage scenarios. To this extent, the individual process steps must be identified, starting with the procurement of required production goods such as raw materials. Existing process documentation can be of help here. It is important to record internal and external information flows, as well as dependencies and interactions between individual stages. Similarly, the machinery, equipment, and tools required for production should also be considered. All relevant holders know-howsuch as employees, documents, and software such as machine programs must be identified.

Based on the production process, critical aspects which are relevant to product and knowledge protection can be identified in the next step along with their corresponding risk areas. Then, damage scenarios which could potentially lead to a know-how leakage are sought within each area, andthe possible causes and reasons for the loss of knowledge should be identified. The aim of this analysis is to collect all potential and hypothetical damage scenarios, also the unlikely ones.

In order to cover damage scenarios that are not directly obvious or known, the method of "Six Thinking Hats" [[8]] can be applied. This creative technique is used as an instrument to take different positions and viewpoints on an issue and therefore the simulation of various approaches. In this case, the method can be used to switch one's own point of view. It is possible to gain several points of view for detecting damage scenarios through targeted questioning techniques (e.g. "Imagine that you supplyto plant xy. Which information do you receive about your customers and their products?"). Similarly, the know-how protection measures and activities which are currently implemented should alsobe identified and assigned to the risk categories and damage scenarios.

Subsequently, the identified loss scenarios must be evaluated. The probability that a damage scenario occurs is assessed on a points scale (refer to [[7]]). Also, the significance of the risk must be evaluated on a similar scale (e.g. 1 point = no expected consequences, whereas 5 points = very serious consequences expected). The probability of occurrence is then multiplied by the risk significance, as done by Marxen et al., to generate a risk ratio which serves as an indicator of the know-how leakage risk [[7]]. To evaluate whether appropriate measures should be developed for a particular damage scenario, it is necessary to establish critical values for the probability of occurrence, the risk significance, and the risk ratio. Plotting this evaluation in a portfolio reveals the scenarios for which protection measures must be developed (Figure 2, shaded area).

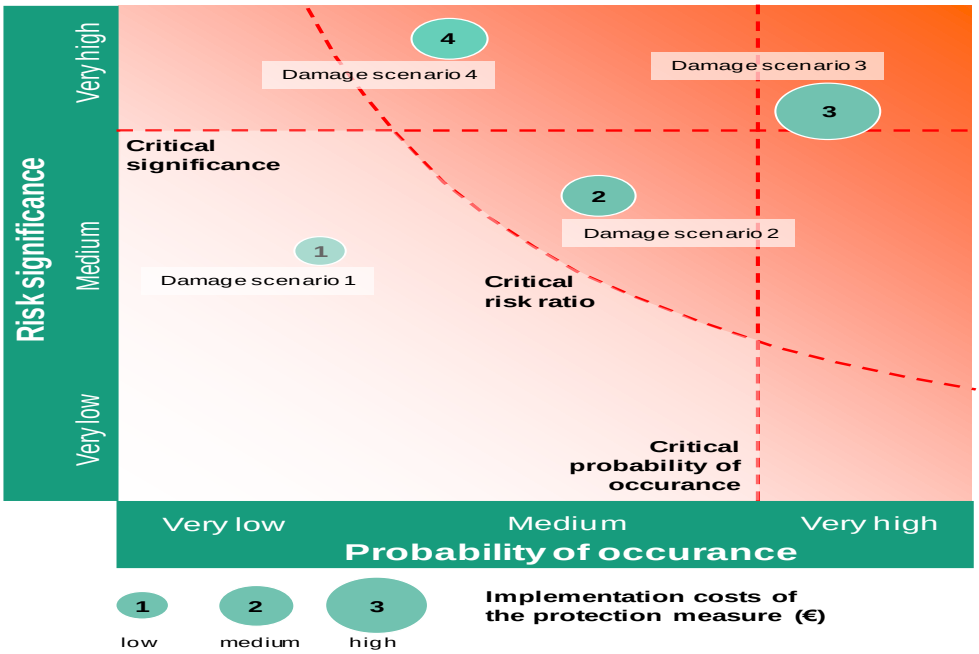

Figure 2: Identification and evaluation of critical damage scenarios

IV. Developing Protection Measures

Individual measures should be identified for each critical damage scenario in order to develop a comprehensive approach for securing production knowledge. Measures which are principally possible to implement in specific cases and scenarios are selected from a catalog of already known measures. Furthermore, it must be checked whether the development of new safety measures for each damage scenario makes sense.

In order to identify appropriate prevention measures, the applicability of established standard measures will be examined as a first step. Additionally, an evaluation of the possible effectiveness of the measures for the specific company will be performed. The measures' applicability is to be evaluated either as "meaningful", "possibly meaningful" or "not meaningful".An overview of all meaningful measures will therefore be available for the company. For example, a wide range of standard protection measures involves the encryption or securing of data related to machine control systems [[9], [10]]. However, small- and medium-sized companies often have older machines with no Windows-based machine control, rendering this measure ineffective.

Creative techniques, such as the TRIZ method [[11]], used throughout facilitated workshops with interdisciplinary participants from a company have been deemed to be effective for the development of new protective measures or the modification of existing ones. Further support for the development of individual protection measures poses the following central questions:

- Which protective measures come first to mind?
  - Raising awareness
  - Making plagiarized products unattractive
  - Complicating marketing
  - Managing human resources
  - Making access to production processes less transparent
  - Limiting access to critical company know-how
- Which conditions must be met?
- With which mechanisms/ other measures can the idea be combined?
- Which challenges are associated with the idea? Which consequences would the protection measure have (e.g. effects on material properties or the overall process)?
- What are the advantages and disadvantages of the measure?

After this step, a variety of potentially applicable measures can be developed. This is followed by a second step which involves a systematic selection of measures which have the highest benefit for the company in question.The protection potential, implementation costs, and the impact on existing production processes will be evaluated. This supports a need-based selection and prioritization of the individual protective measures based on the company's restrictions.

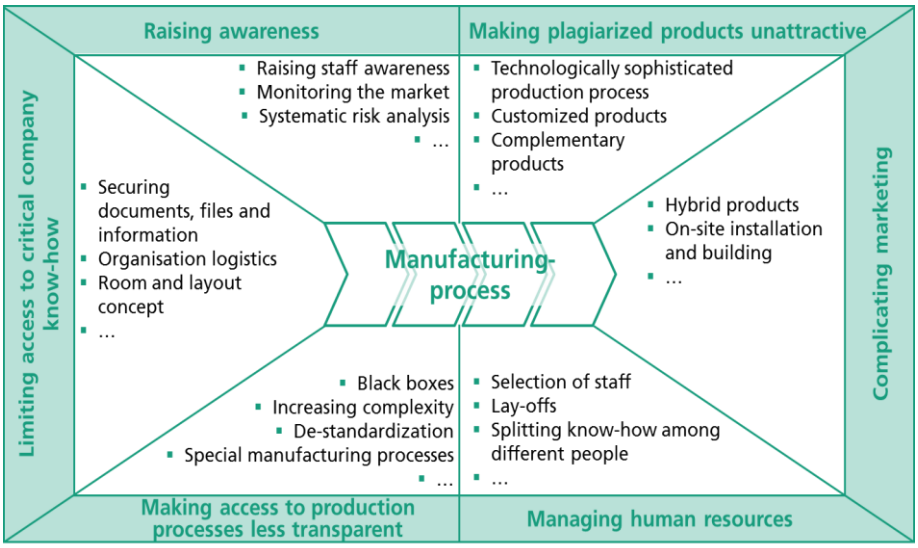

Figure 3: Know-how protection concept with six basic factors

The critical damage scenarios are subsequently evaluated based on the selected protection measures once again with regard to risk significance and probability of occurrence. This should be done through a detailed discussion of the individual damage scenarios in a workshop with participants from different departments and hierarchical levels of the company. Can the selected measures reduce the risk and significance of the damage scenario so that it is no longer in the critical region of the portfolio (seeFigure 2), or are additional measures needed? This question should be answered at the workshop. The protection potential and the effect of the selected measuresare therefore defined for the respective critical damage scenario.

If the selected measures ensure sufficient protection for all critical potential damage scenarios, the planning and implementation of the measures can be done in the next phase. If the reevaluation reveals further critical damage scenarios, another iteration of the second phase "developing protection measures" (seeFigure 1) is necessary.

A sustainable concept for knowledge protection in production consists of a systematic combination of different individual measures [[12]]. To maximize the protection potential, measures with different protection functions should be implemented. An overview of the six components of a protection concept and exemplary protective measures are shown inFigure 3.

The particularly critical categories for know-how protection in production form the following three areas:

- Limiting access to critical company know-how
- Making access to production processes less transparent
- Managing human resources

The first category includes individual protection measures which limit the access to critical company know-how. An example of such a measure is an adapted room concept. The development of a special room concept for production allows the separation of sensitive process steps or keeping specific process parameters hidden from the machine operators. One possible form of implementation is the encapsulation of machine components, which can only be accessed by authorized employees.

For the second category, measures that decrease transparency or the use of de-standardized components serve to decrease the risk of leaking critical production information. The actions associated with an increase in process complexity include, for example, the integration of unneeded components/ supplies in various production processes, or the performance of unnecessary process steps. The use of de-standardized components in production leads to significantlyimpeding unauthorized replica. For a large part of the potential plagiarists, the de-standardization of components is not obvious at first glance. A replica of the products with standard components inevitably leads to a significant reduction in functionality or the lifetime of the product. The complicated procurement of de-standardized components discourages a lot of potential plagiarists [[12]].

The third category of know-how protection relates to human resources management. The aim is to scrutinize employees deployed in critical areas of production. If it is found that an employee has connections to competitors, or an above average tendency to change jobs, then particular attention needs to be paid while selecting the tasks to be assigned to this employee, and his/ her setting. In addition, access to critical areas of production should only be granted to employees with long years of service.

V. Planning and Implementing Protection Measures

After selecting all measures for the development of a comprehensive protection concept, the third phase consists of supporting the planning and implementation of the measures. The first step is to detail and concretize the selected protection measures. This includes appointing responsible employees, identifying development costs, and coordinating with potential suppliers. Asensible and responsibledealing with suppliers is of particular importance in the implementation of protection measures.

It must be ensured that business partners will not transmit any critical documents or information [[13], [14]]. Communication rules for disclosingcompany information to third parties form an important part of the protection strategy. These rules should be set and agreed upon in advance with all departments. The unintentional transmission of sensitive information to external business partners can therefore prevented. Additionally, the procurement of components and modules which should be protected should not be done through a systems supplier, but rather through several independent suppliers.The knowledge of the individual components of the protected product is therefore divided, and no single vendor has all of the information concerning the product.

If the measures are worked out in detail, and the necessary implementation efforts are approved, each activity can be converted into an action plan. In addition to assigning the responsible employees, a time planning of the different activities should be carried out. Once this planning step is completed, the implementation of the protective measures should be started.

It is very important to periodically review of the protection concept including all its components. Companies currently operate in a highly dynamic competitive environment, and are confronted with ever-changing factors. A static protection concept therefore cannot guarantee long-term protection. Continuously updating the risk analysis and reviewing the identified damage scenarios are therefore a prerequisite for ensuring sustainable know-how protection [[12]].

VI. Conclusion

Sustainable know-how protection in production is especially important if the uniqueness of the product depends on manufacturing skills and unique features [[15]]. A systematic approach is essential to identify critical damage scenarios. Technological and organizational protection measures can be developed through a creative, methodically supported process. Effective protection is provided by measures individually developed for each damage scenario, where already existing standard measures forpiracy protection can be used, as well their further development to suit the individual needs of the company.

REFERENCES

[1] VDMA workinggroup “Produkt- und Know-how-Schutz“: VDMA Studie Produktpiraterie, 2014

[2] Kinkei, S.; Maloca, S.: Produktionsverlagerung und Rückverlagerung in Zeiten der Krise. Modernisierung der Produktion, Mitteilungen aus der ISI-Erhebung Nr. 52. Fraunhofer ISI, Karlsruhe 2009, p. 12

[3] Schuh, G.; Haag, C.: How to Prevent Product Piracy Using a New TRIZ-Based Methodology - TRIZ Future Conference 2008. Procedia Engineering (2011) 9, p. 391-401

[4] Abele, E.; Kuske, P.; Lang, H.: Schutz vor Produktpiraterie. Springer-Verlag, Berlin, Heidelberg 2011

[5] Wildemann, H.: Produktpiraterie. TCW-Verlag, München 2010

[6] Abele, E.; Kuske, P.; Lauer, B.: Know-how Schutzstrategien im Maschinenbau implementieren. ZWF 106 (2011) 6, p. 444-448

[7] Marxen, L.; Geiger, R.; Meyer-Schwickerath, B.: Systematische Risiko- und Maßnahmenidentifikationund strategische Verankerung im Unternehmen. In: Abele, E.; Albers, A.; Aurich, J.C.; Günther, WA. (Hrsg.): Wirksamer Schutz gegen Produktpiraterie im Unternehmen. Piraterierisiken erkennen und Schutzmaßnahmen umsetzen. VDMA-Verlag, Frankfurt am Main 2010, p. 25 -63

[8] De Bono, Edward. Six thinking hats. Penguin, 1999.

[9] Birkhold, M.; Verl, A.: Post-Stuxnet: Sicherheitslücken bedrohen weiterhin Produktionsanlagen. ZWF 106 (2011) 4, p. 237 - 240

[10] Jessenberger, S.: Detaillierte Lösungskonzepte für mehr IT-Sicherheit in industriellen Netzwerken. ZWF 104 (2009) 2, p.94-97

[11] Al□tshuller, GenrikhSaulovich. The innovation algorithm: TRIZ, systematic innovation and technical creativity. Technical Innovation Center, Inc., 1999.

[12] Neemann, Chr. W: Methodik zum Schutz gegen Produktimitationen. Dissertation, RWTH Aachen, 2007. Berichte aus der Produktionstechnik 2007, Nr. 13, Shaker Verlag, Aachen 2007

[13] Meier, H.; Siebei, C.; Nahr, M.: Auswahlstrategie von Kooperationspartnern im Kontext der Produktpiraterie. ZWF 104 (2009) 12, p. 1093 -1096

[14] Kafitz, W: Sicherheit und Plagiatschutz beim automatisierten Datenaustausch. ZWF 104 (2009) 6, p. 513-517

[15] Gausemeier, J.: Produktpiraterie – Bedrohung für Innovationskraft und Wettbewerbsfähigkeit. ZWF 105 (2010) 5, p. 403-404.