International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:9, No:5, 2015

Challenges in Anti-Counterfeiting of Cyber-Physical Systems

Daniel Kliewe, Arno Kühn, Roman Dumitrescu, Jürgen Gausemeier

***Abstract*—**This paper examines the system protection for cyber-physical systems (CPS). CPS are particularly characterized by their networking system components. This means they are able to adapt to the needs of their users and its environment. With this ability, CPS have new, specific requirements on the protection against anti-counterfeiting, know-how loss and manipulation. They increase the requirements on system protection because piracy attacks can be more diverse, for example because of an increasing number of interfaces or through the networking abilities. The new requirements were identified and in a next step matched with existing protective measures. Due to the found gap the development of new protection measures has to be forced to close this gap. Moreover a comparison of the effectiveness between selected measures was realized and the first results are presented in this paper.

***Keywords*—**Anti-counterfeiting, cyber physical systems, Intellectual property (IP) and knowledge management, system protection.

I. Introduction

THE research presented in this paper deals with the new challenges that arise in the field of anti-counterfeiting for intelligent, networked systems. These innovative, complex systems are characterized by a growing interconnection with their environment, better communication skills, and an inherent partial intelligence. Modern automobiles today are an example of such systems. They contain highly networked, mechatronic systems and communicate with the infrastructure and other vehicles, creating superior cyber-physical systems (CPS).

The innovation leap from mechatronics to CPS results in new fields of action in the protection of these systems. The aim of this research is to help understanding and meeting these challenges. Therefore the new requirements of CPS must be identified and considered.

The research in this paper is structured as follows: In chapter II the challenges in anti-counterfeiting of CPS are identified. These are compared to existing approaches for anti-counterfeiting in chapter III. Chapter IV demonstrates the identification of the requirements of CPS in system protection. Furthermore, all found requirements are matched with the existing protection measures. Thus, it can be determined to what extent research is necessary in the development of protection measures. Beyond, new measures are searched to improve the protection of CPS and first solution possibilities are demonstrated based on examples given. Chapter V gives a short summery and guidance about the further development of protection measures for CPS.

D. Kliewe, A. Kühn and R. Dumitrescu are with the Fraunhofer Institute for Production Technology IPT, Project Group Mechatronic Systems Design Zukunftsmeile 1, 33102 Paderborn, Germany (phone: +4952515465269; fax: +4952515465102; e-mail: [daniel.kliewe; arno.kuehn; roman.dumitrescu]@ipt.fraunhofer.de).

J. Gausemeier is with Heinz Nixdorf Institute University of Paderborn, Fürstenallee 11, 33102 Paderborn, Germany (e-mail: juergen.gausemeier@hni.upb.de).

II. Challenges in Anti-Counterfeiting of CPS

A. Intellectual Property (IP) and Knowledge Management

Intellectual property (IP) and knowledge management are often neglected in companies. Most companies lack both, willingness and a systematic approach to deal with IP management [1]. IP is usually divided into two branches, industrial property and copyright [2]. Mittelstaedt extends this understanding and adds more aspects to the definition of IP, among other things, the fields of secrets, know-how, licenses and domains [1]. The research demonstrated in this paper aims on the protection of the unprotected knowledge which is available within the products of a company as illustrated in Fig. 1.

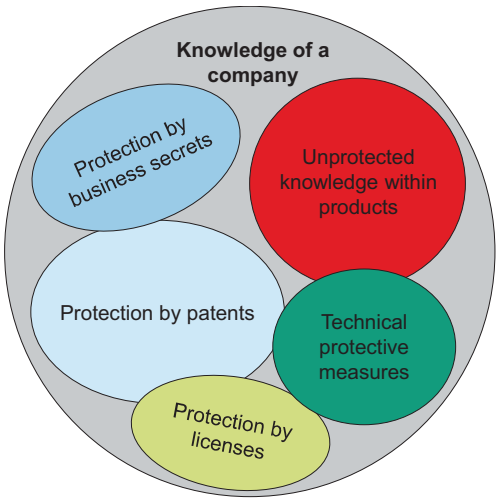


Fig. 1 Different forms of knowledge of a company

The knowledge within a product can be extracted for example by analyzing the product. It is of great interest for manipulators, counterfeiters and other companies.

There are different protective measures existing for the protection of the company's knowledge (see Fig. 1). Some knowledge is protected by secrets kept in the company, other by legal measures such as patents and some knowledge is licensed. However, even the technical protective measures are

not able to protect the complete knowledge within products. By performing a detailed analysis of a product, lots of details about the company, the manufacturing process and the product itself can be identified.

The research shown in this paper focuses on the protection of the knowledge within products and especially within CPS. Especially for these networked, intelligent and adaptive systems, new challenges in protecting these systems have to be considered.

B. Cyber-Physical Systems (CPS)

The mechanical engineering industry and related industries are undergoing a massive shift from classic mechanic-centered products to mechatronics. The technical systems of tomorrow will go beyond current mechatronics by incorporating inherent intelligence. Information technology and non-technical disciplines such as cognitive science, neurobiology and linguistics are developing a variety of methods, technologies and procedures that integrate sensory, actuatory and cognitive functions into technical systems. We call such systems cyber-physical systems (CPS). The route to these systems is determined by three general trends in technology:

1) Miniaturization of the electronics [3]
2) Software technology as driver of innovations [4], [5]
3) Networking of information systems [6]

Primarily - but not exclusively - the way of information processing is implementing the change from mechatronical to CPS. The design of such systems is an interdisciplinary and complex task. Therefore, effective and continuous cooperation and communication between developers from different domains during the whole development process are required. CPS differ from classical mechanical and mechatronic systems in their inherent intelligence as well as their internal and external networking. They are characterized by four core properties in particular: they are **adaptive, robust, predictive and user-friendly** [7].

The technology concept of an intelligent, networked system is shown in Fig. 2 and describes what is understood by the term **cyber-physical systems (CPS)**. The technology concept structures a CPS into a total of four units: basic system, sensors, actuators, and information processing. The basic configuration of the four listed units is known as a partial system. In this system, information processing has a central role. With the help of a communication system, it intervenes between the sensor and the actuator systems. The sensors record the necessary information during the interplay between actuators and base system [7].

At this point, it already becomes clear that the change to intelligent systems is characterized in particular by data processing. This leads to new challenges for an approach in protecting CPS. The increasing amount of software in CPS must be considered and the software-components must be protected. Furthermore it is essential that the data processing based on the networking abilities are protected against outside influences.

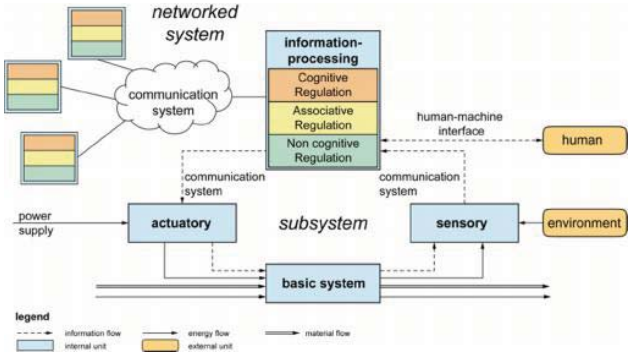


Fig. 2 Technology concept - by intelligent subsystems to the networked, cyber-physical systems according to [7]

The integration of new technologies, multiple sensors and inherent intelligence adds significantly to the customer experience but introduces many new interfaces that intruders such as product pirates or hackers can exploit. As a result the protection of CPS has to consider established topics like anti-counterfeiting, product piracy, intellectual property or knowledge management and beyond that also has to consider aspects of security engineering.

C. The Danger of Product Piracy and Security Engineering

The latest study of the VDMA "StudyProduct Piracy 2014" has shown that the damage caused by **product piracy** is a serious issue in Germany. In 2013, 71 % of all German companies in machine and plant construction were affected by product piracy. The revenue loss is 7.9 billion euros [8]. The development of the revenue loss and the damage is shown in Fig. 3.

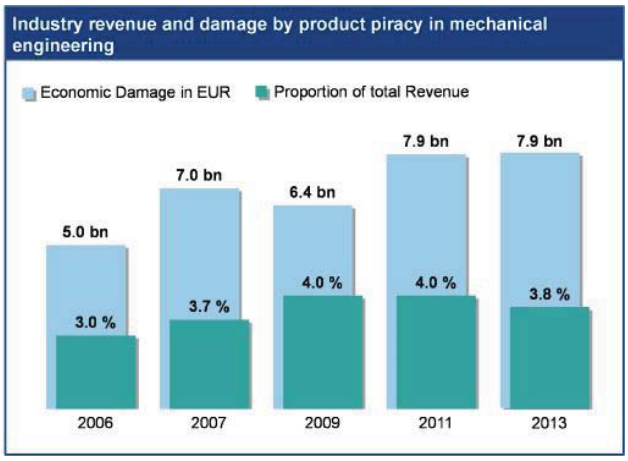


Fig. 3 Damage and loss in revenue due to product piracy [8]

The amount of the damage is almost 8 billion euros since 2011. This means an equivalent of a loss of 40,000 jobs per year [8]. Moreover, the percentage of total sales has been stable for years and has only slightly decreased in 2013. This is due to the increase of the revenue of the industry.

According to the survey, 82% of the German companies try to protect themselves from imitations with legal measures,

such as patents, utility models and industrial designs. These measures present an important prerequisite in the fight against piracy, but they are reactive, i.e. they attack only if the damage has already occurred. In addition, less than half of the businesses take action against plagiarism, once property rights have been violated [8]. For these reasons it is especially important to use preventive protection measures.

Also worldwide cyber-attacks are a big issue in **security engineering** and cause intellectual property loss as described in a joint study by McKinsey and the World Economic Forum in 2014 [9]. 65% of the interviewed industry leaders believe that malicious attacks from external or internal sources are the most likely risk to have a negative impact on their business. More than half of the industry leaders think that the risk of cyber-attack will be a significant issue over the next five years. Furthermore the study shows that the pace of attackers will increase more quickly than the development of new protection measures [9]. This leads to the challenge that new measures for the protection of CPS must be considered. These measures have to make sure that the networking abilities are secure and consider possible malicious attacks.

Future technical products like CPS will significantly differ from the familiar mechatronic products. They have the potential for a cross-industry innovation leap; an early understanding on specific protection measures is of crucial importance. This is the only way the competitive advantage for the companies investing in innovation and research can be preserved and jobs can be secured. For these original manufacturers, it is essential to protect these systems right from the start.

To do so, the found **challenges** on the protection of CPS must be considered:

- consider the requirements for the system protection of CPS
- consider and protect the increasing amount of software in CPS
- protect new interfaces like the networking abilities against outside influences such as cyberattacks
- consider new measures for the protection of CPS

In the next chapter, these challenges are compared to protective methods which provide the state of the art.

III. State of the Art

Preventive system protection for CPS has to fulfill the identified challenges from chapter II, consider the entire product life cycle, and during strategic product planning. This protection can only be reached holistically through a coordinated bundle of protection measures, so-called protection concepts. As in [10], the protection measures against product piracy are divided into seven categories: strategic, product - and process-related, marking, IT based, legal and communicative measures. In this context, the number of known measures is very high with over 90. An exemplary strategic protection measure is the limitation of important know-how on selected individual employees. Another example is the use of an RFID-chip. The chip can be used for marking measures to track and trace the system and proof its originality. All these measures as a whole have a high potential for the fight against piracy [10]. However the measures mentioned do not fulfill the challenges for the protection of CPS.

As in [11], a procedure was conceived in order to develop imitation-protected products and production systems. First, the risk situation will be analyzed. This step identifies targets for knowledge flows and product piracy. Then, the sensitive technologies of the company will be identified. After that, protection measures will be examined and a protection strategy will be developed. In the end, requests will be put up to establish the foundations for the remaining phases where protected products and production systems will be designed [11]. This procedure does not consider the challenges for the protection of CPS.

In addition, there are numerous approaches to the creation of protective measures and protection concepts, for example the counterfeiting process according to [12], the methodology for the protection against product imitation according to [13], the development of an anti-piracy strategy according to [14] or the BMBF research initiative "Innovation against product piracy", which conceived the "product protection needs analysis" in the transfer project "ConImit - Contra Imitatio [10].

None of the above-mentioned procedures, methods and projects takes into account the special challenges of CPS in the field of system protection. The existing measures and methods are not designed for intelligent, networked systems and therefore not applicable without adjustment.

The situation analysis and the state of the art have revealed that existing protection measures must be examined with regard to their effectiveness in CPS. For being able to examine and adjust the measures and methods one has to know the requirements CPS demand on their protection. These new requirements are identified and matched with the existing measures for system protection in the next chapter.

IV. System Protection of Cyber-Physical Systems

A. Approach to Gathering the Requirements:

CPS have become increasingly important due to the current development of technological innovation. In order to find the appropriate measures to protect CPS from original manufactures, one has to know about the requirements of CPS and of the companies for system protection. The procedure for gathering these requirements is shown in Fig. 4.

In the course of requirement gathering, a direct survey was carried out with 16 companies of the leading-edge cluster “Intelligent Technical Systems Ost Westfalen Lippe - it’s OWL”, to obtain the necessary information first-hand. For this purpose, a questionnaire was created. Firstly, matching questions had to be sought and formulated for the preparation of the questionnaire.

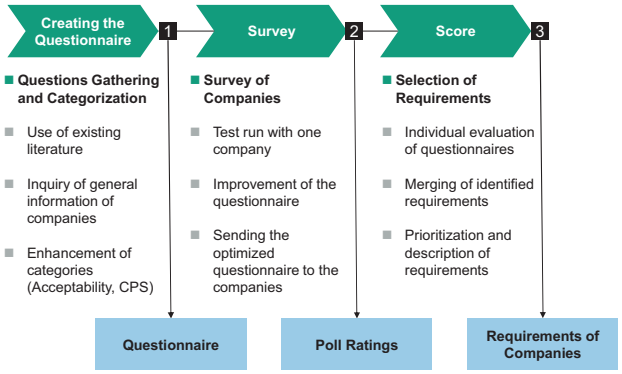


Fig. 4 Process for gathering the requirements

1) Creating the Questionnaire:

First, new questions had to be developed and existing questions collected for the creation of the questionnaire. The questions were formulated in a way that the company's requirements could be derived from the answers. Therefore, different types of questions have been provided: closed questions to identify the relevance of a topic and open questions to absorb the know-how of the company.

The questions can be divided in three main areas:

- General questions about the company
- Questions concerning system protection in general
- Questions concerning the protection of CPS

General questions about the company: General questions concerning the company, e.g. regarding the size or the extent of being affected by piracy where included in the questionnaire.

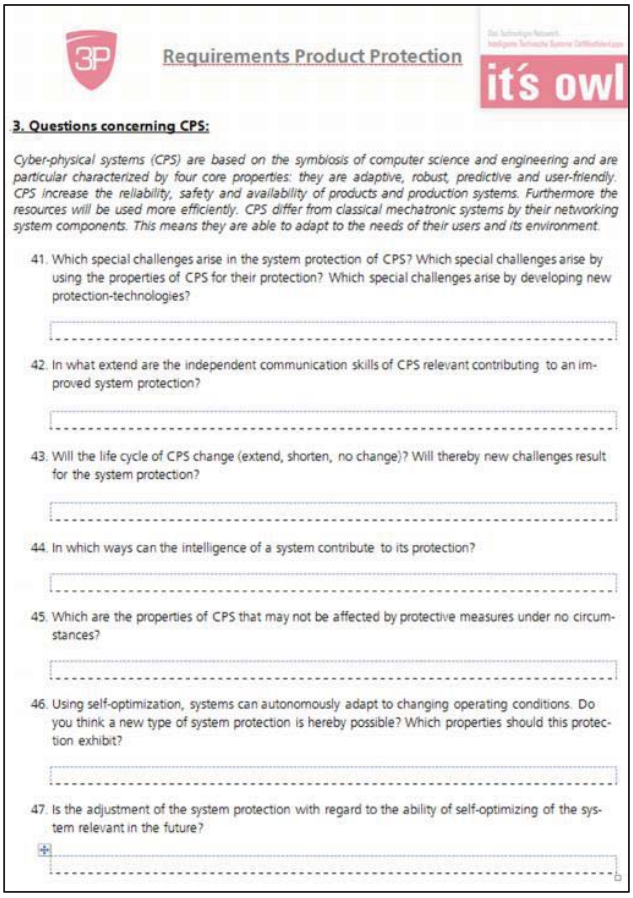
Questions concerning the system protection in general: These questions aim for gathering the companies' requirements for the system protection. The questions are divided into categories of protection measures. Moreover, to get an overview of the previous use of system protection measures, there were also questions regarding the use of protection measures within the company.

The subcategories for questions concerning system protection in general are based on the seven categories of protection measures [11]. These were adopted and extended by the categories of "acceptance" and "company-specific".

The questions in the **category "acceptance"** are to determine a company's requirements in the general acceptance of technologies and protective measures. This involves both the acceptance of employees who will apply the measures and the acceptance of the customers who buy the systems. In this category, questions were developed to indicate the specific requirements. These requirements with regard to the acceptance of technologies and measures are relevant as system protection measures lead to new technologies or processes for a company. These technologies or processes must be integrated into the company. It is only possible to integrate these if the acceptance of the company is fully given and there are no restrictions caused by the new modifications. The questions concerning acceptance were discussed and optimized with business psychologists.

In addition to the general questions, company-specific requirements were determined. The questions in the category **"company-specific"** should identify the requirements on system and know-how protection which are individually given by each of the companies surveyed. This information is especially important for the individualization and customization of protection measures with regard to the needs of each company.

The questions concerning the protection of CPS have been grouped in a separate main area and are demonstrated in Fig. 5.


Requirements Product Protection

it's owl

3. Questions concerning CPS:

Cyber-physical systems (CPS) are based on the symbiosis of computer science and engineering and are particular characterized by four core properties: they are adaptive, robust, predictive and user-friendly. CPS increase the reliability, safety and availability of products and production systems. Furthermore the resources will be used more efficiently. CPS differ from classical mechatronic systems by their networking system components. This means they are able to adapt to the needs of their users and its environment.

41. Which special challenges arise in the system protection of CPS? Which special challenges arise by using the properties of CPS for their protection? Which special challenges arise by developing new protection-technologies?

42. In what extend are the independent communication skills of CPS relevant contributing to an improved system protection?

43. Will the life cycle of CPS change (extend, shorten, no change)? Will thereby new challenges result for the system protection?

44. In which ways can the intelligence of a system contribute to its protection?

45. Which are the properties of CPS that may not be affected by protective measures under no circumstances?

46. Using self-optimization, systems can autonomously adapt to changing operating conditions. Do you think a new type of system protection is hereby possible? Which properties should this protection exhibit?

47. Is the adjustment of the system protection with regard to the ability of self-optimizing of the system relevant in the future?

Fig. 5 Excerpt from the questionnaire for gathering the requirements on system protection of CPS

These questions are the focus of the survey because based on these questions the requirements on system protection of CPS will be identified. A later comparison of existing protective measures with the requirements gathered (see chapter IV) examines which protective measures are most suitable for the protection of CPS. It is crucial to know the requirements on system protection in order to develop protective measures and to ensure the profits of R&D - investments.

2) Survey:

Before sending the questionnaire to the companies, a test

run was conducted with one of the companies. This questionnaire was discussed together with employees of the company to find out if there is any potential for improvement in the design of the questionnaire.

The companies were supposed to send the presented questionnaire to the employees in charge who deal with the issue of system protection (if available in the company). Most of the answers came from the legal department. Only few surveys were answered from the head of the R&D – department or the manager for corporate technology. Interestingly, their answers were significantly different from the answers given of the legal department. Typical requirements from the legal department where for example: the improvement of a holistic management of the patents, new methods for a selective search for counterfeits and raising the awareness of the issue. The requirements from the technology departments where more aimed on solutions beyond legal measures. For example controllability of a measure, costs, design and performance of the system may not be affected and the usability of a measure has to be considered.

3) Evaluation:

After the companies had answered the questionnaire and sent back, it was first individually evaluated for the respective companies. A summary of the replies to the questionnaire was created for each company individually. The requirements for the specified categories were filtered out of the summary. After the individual evaluations of the questionnaires, it was necessary to merge the identified requirements of the individual companies. This merge was realized in a table which summarized the determined requirements by each category. All the requirements are included in the created table. In addition, it is noted which companies have pointed out these requirements.

The frequency of the nomination by the companies helped to prioritize the requirements. The more a requirement was mentioned by the companies, the more important this requirement is for system protection. For the most stated of these requirements, it is particularly important to have appropriate protective measures or newly develop these.

The most quoted requirements are:

- Raising the awareness of the issue (12 quotes out of 16 questionnaires)
- Inform the customer when he uses an original system or spare part (12 quotes)
- Security in data management (12 quotes)
- Effectiveness of a protect measure (11 quotes)
- The “internationality” of a protection measure (meaning the measure has to worldwide usable) (10 quotes)
- simple and cost-effective implementation (10 quotes)

A total of **36 requirements** were recorded by the survey and the subsequent evaluation. **Six of these requirements are in the CPS category**. These are:

- Security in data management (12 quotes)
- In the event of a sabotage, manipulation or know-how loss, automatic transfer of information to the company and warning of other systems (9 quotes)
- Support and use of the characteristics of CPS for their inherent protection (7 quotes)
- Security in networking (6 quotes)
- Protection of software components (2 quotes)
- Use of self-optimization to learn from attacks (1 quotes)

These requirements are fundamentally new and prove the existing difference between the system protection for mechatronics and CPS. The newly identified requirements refer to the use and support of CPS-specific properties, such as the ability to self-optimization. The networking and communication skills of CPS offer new possibilities of system protection, but at the same time new targets for counterfeiters appear. Thus, the new requirements show that above all networking and data exchange security are of a high priority.

B. Matching the Requirements with Existing Measures

When the recording and evaluation of requirements was complete, we had to find out to what extent the existing system protection measures fulfil the 36 identified ones. For this purpose, the identified requirements had to be matched with the existing protective measures.

The general framework conditions have been set prior to evaluation. These conditions define the general requirements for a protective measure (such as the effectiveness or the reliability of a protective measure). In addition, to achieve a better traceability, the perspective from which the match had been done was described. Existing measures in relation to the requirements will be evaluated. Following this outlined base, the overall requirements were matched with the known measures.

The **comparison detects the areas which need to be improved** with regard to protective measures. Consequently, the need for development is pointed out to implement an adequate system protection. For the matching, the protection measures are directly compared to the found requirements.

For this matching process, a table was created which shows the requirements in the first line and the protective measures in the first column (Fig. 6).

Like this, each requirement can be matched with any protection measure. Due to the division of the requirements as well as the measures into identical categories, the categories themselves can be compared. This way, strategic requirements can be matched with strategic measures. Product-related requirements can be compared to product-related measures, and so on (Fig. 6).

This makes sense because for instance the IT-based requirements such as the "protection of know-how in data transmission" are so specific that they can only be met by information technology measures such as encryption, reduction of information or secure communication links.

Measures*\Requirements	International effectiveness	Simple and cost-effective Implementation	Monitorability	Adaption and Optimizability in the Product Life-Cycle
Strategic Measures				
Strengthen Employee Loyalty	met	met	met	
Implementation of Knowledge Management	met	partially met	met	
Restriction of valuable know-how to selected employees	met	met	partially met	met
Sensitization of Employees for Social Engineering	met	met	partially met	
Cooperation in the Field of Product Protection across departments	met	met	met	partially met
Optimization of Innovation Processes	partially met		met	met
Target Costing	met	partially met	partially met	met
Cooperation with external Suppliers	partially met	partially met	partially met	
Integration of external Suppliers	partially met	partially met	partially met	

Fig. 6 Excerpt of the comparison in the category "strategic actions"

There are three levels of satisfaction when matching the existing protection measures with the requirements. For a better overview, the three satisfaction levels are marked in different colors (see Fig. 6). The definition of the fields (levels) is defined as follows:

1) White boxes: There is no connection between the requirement and the measure. So the requirement cannot be fulfilled with this measure.
2) Yellow fields: The measure can contribute to the fulfilment of the requirement; the evaluation is specified as "partially met". A partial fulfillment of the requirement exists if the requirement cannot be fulfilled by the measure completely, but it can partially contribute to.
3) Green fields: The requirement is fully met by the measure and requires no combination of several measures to meet the requirement. The evaluation is defined as "met".

Measures*\Requirements	Secure Data management	Automatic Transfer of Information	Support of the CPS-characteristics	Security in networking
IT Measures				
Biometric Assisted Access Control				
Role-based Access Control				
Encryption of Documents	partially met		partially met	partially met
Removal of Information from CAD-Models	partially met			partially met
Secure communication connections (Secure Information Flow)	met		partially met	met
Mutual Authetication of Components		partially met	partially met	
Product Activation				
Outsourcing of safety-relevant Computing Operations		partially met		partially met
Protection of embedded Software	met		met	

Fig. 7 Excerpt of the CPS-comparison in the category "strategic actions"

A special case in this evaluation is **matching the requirements of the CPS** (Fig. 7). Because so far no measures have been developed in this specific area, the requirements by CPS are matched with the existing system protection measures in all categories. This way, it is possible to check if there are already potential measures for the protection of CPS. Thus, the need for development in this area can be estimated. **The numerous "white spots" point out the gaps which exist between the requirements and the protection measures**. New technologies and protection measures are needed to close these gaps.

The match reveals that in most categories all requirements can be fulfilled by combining individual measures (Fig. 6). Only with regard to the requirements of the CPS, white spots are largely visible (Fig. 7). Here, the existing measures can only occasionally meet the requirements. A complete fulfillment is only possible with a combination of numerous measures in different categories.

C. External Measures for the System Protection of CPS:

The investigation shows that the companies' requirements for system protection are well fulfilled by the existing protection measures. In addition, it became clear that **CPS has created new requirements on system protection**. These six new requirements can only be fulfilled in an insufficient manner by the existing protective measures (see Fig. 7). Existing protection mechanisms are not designed for CPS system protection because CPS integrate a variety of new features. Up to now, there is no protection approach which sufficiently takes into account the challenges and requirements for the protection of CPS. There is an acute need for action to develop system and know-how protection measures as well as new technologies for the protection of CPS.

It becomes clear that one main area in CPS is the field of information technologies. The fulfillment of the requirements is the best in the field of IT-based protection measures.

The gathered requirements point out the gap between the requirements of CPS and the existing protection measures. Hence, the measures have to be adapted and extended. Also external protection measures (meaning not considered in the research so far) have to be searched and new ones developed to close the gap. Based on that, external technologies and methods for the protection of complex, intelligent systems were analyzed and compared to the existing ones.

The identification of new technologies and external measures for system protection of CPS could be promoted through cooperation with the Fraunhofer Institute for Applied and Integrated Security – AISEC. Due to this cooperation external protective measures were identified, some of these are shown in Fig. 8. An example for a measure is the protective foil "protecting electronic products – PEP". It protects the critical areas of an embedded system, seals the housings tamper-proof and disables the functionality of a system in case of an attack [15].

A comparison of the effectiveness between the known IT-based protection measures and the AISEC-measures was carried out and is shown in Fig. 8.

The known IT-based protection measures are shown above, the new measures below. The effectiveness indicates the level of fulfillment of the requirements. The green bars show the amount of total fulfillment of the requirements. The orange bars indicate the amount of the partially fulfillment. And the red bars demonstrate the amount of the requirements which were not fulfilled.

The protective foil is the first of the new protective measures in Fig. 8. It has a fulfillment of all the identified requirements of 39% and a partial fulfillment of 28%. Combined 67% of all requirements are at least partially

fulfilled. In comparison to the known IT measures it is remarkable, that 67% of at least partial fulfillment is only the second best value. The protective measure "secure communication" has a better value with more than 70%.

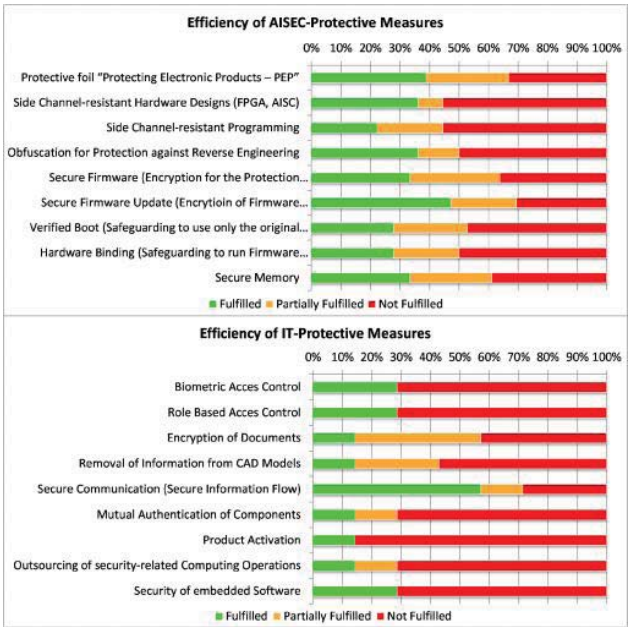


Fig. 8 Comparison of the efficiency of protection measures

The average of the new protective measures efficiency is higher compared to the one of the IT measures. The comparison showed that the new protective measures have a better fulfillment of the requirements. But there are still "white spots" in the comparison to the requirements of CPS. Therefore the development, extension and adaption of protective measures have to be continued.

One way to improve the protection of CPS is to arrange several single protective measures to a coordinated protection concept. This way the protection impact can be raised, because the single protective measures support each other. Furthermore the new measures can be arranged with the known measures as well. Hence the efficiency of a protection measure concept is better compared to single measures.

Some of the protective measures, like the protective foil, are still at the experimental stage. So roadmaps have to be worked out to give a better overview on the protection concepts and their timelines. A first example of a roadmap is shown in Fig. 9.

On the left side of the roadmap some of the protective measures are listed. Above are the new measures and below the known ones. The horizontal line above is the timeline.

The protection concept A (orange line) consists of three single measures, one new and two known ones. As demonstrated in the roadmap, the concept can be implemented in the middle of the year 2015. The concept B, which consists of two new and one known measure can be implemented in the middle of the year 2017, because the new measures are not available on the market until then.

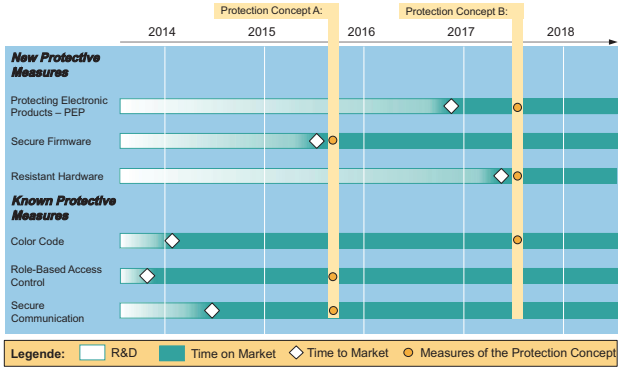


Fig. 9 Example for a protective measures roadmap

With the help of these first roadmaps, protective measures and the resulting protection concepts are highlighted to demonstrate the further development.

V. Summary and Outlook

The paper gives insights into the challenges that exist with system protection by innovative, intelligent systems. By identifying new requirements and matching requirements with existing protective measures, the current lack of protection can be displayed. New protective measures are demonstrated. With the help of roadmaps, new measures and the resulting protection concepts are highlighted with a focus on authentically illustrating the course of time.

Nevertheless the found requirements of CPS cannot be completely fulfilled by the new protective measures. So there is still need for research in developing new protective measures and in the development of new technologies, which potentially increase system protection for CPS. Especially the integration of the characteristics of CPS like adaption, self-optimization or inherence intelligence has to be more in the center of the research and development of new protective measures.

Acknowledgment

This research is funded by the German Federal Ministry of Education and Research (BMBF) within the Leading-Edge Cluster "Intelligent Technical Systems OstWestfalenLippe" (it's OWL) and managed by the Project Management Agency Karlsruhe (PTKA). The cluster management is supported by the Ministry of Economic Affairs, Energy and Industry of the German State North Rhine-Westphalia and by the Ministry of Innovation, Science and Research of the German State of North Rhine-Westphalia. The authors are responsible for the contents of this publication.

References

[1] Mittelstaedt, A.; Strategisches IP-Management - mehr als nur Patente. Gabler Verlag, Wiesbaden, 2009
[2] World Intellectual Property Organization (WIPO); Understanding industrial property. WIPO publication no. 895(E), Geneva, 2008
[3] Herzog, O.; Schildhauer, T. (Hrsg.): acatech DISKUTIERT. Intelligente Objekte: Technische Gestaltung – Wirtschaftliche Verwertung – Gesellschaftliche Wirkung. Springer Verlag, Berlin, 2009

[4] Damm, W.; Achatz, R.; Beetz, K.; Broy, M.; Grimm, K.; Liggesmeyer, P.: Nationale Roadmap Embedded Systems. In: Broy, M. (Hrsg.): Cyber-Physical Systems – Innovation durch softwareintensive eingebettete Systeme. acatech DISKUTIERT, Springer Verlag, Berlin, 2010
[5] Schäfer, W.; Wehrheim, H.: The Challenges of Building Advanced Mechatronic Systems. In FOSE ´07: 2007 Future of Software Engineering, pp. 72-84, IEEE Computer Society, 2007
[6] Broy, M. (Hrsg.): Cyber-Physical Systems – Innovation durch softwareintensive eingebettete Systeme. acatech DISKUTIERT, Springer Verlag, Berlin, 2010
[7] Gausemeier, J.; Tschirner, C.; Dumitrescu, R.: Der Weg zu Intelligenten Technischen Systemen. Industrie Management, GITO Verlag, 1/2013.
[8] Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA): Studie Produktpiraterie 2014
[9] World Economic Forum; McKinsey & Company: Risk and Responsibility in a Hyperconnected World – Insight Report, 2014
[10] Gausemeier, J.; Glatz, R.; Lindemann, U. (Hrsg): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012
[11] Kokoschka, M.: Verfahren zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme. Dissertation, Universität Paderborn, Paderborn, 2013
[12] Fuchs, H.J. (HRSG.): Piraten, Fälscher und Kopierer – Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China, Betriebswirtschaftlicher Verlag Dr. Th. Gabler, Wiesbaden, 2006
[13] Neemann, C. W.: Methodik zum Schutz gegen Produktimitationen, Dissertation Fraun-hofer Institut für Produktionstechnologie IPT, Aachen, Shaker Verlag, Band 13/2007, Aachen, 2007
[14] Jacobs, L.; Samli, A. C.; Jedlik, T.: The Nightmare of International Product Piracy – Exploring Defensive Strategies. In: Industrial Marketing Management 30, S. 499-509, North-Holland Publishing, 2001
[15] Fraunhofer Institute for Applied and Integrated Security; http://www.aisec.fraunhofer.de/de/fields-of-expertise/product-protection/pep-protecting-electronic-products.html, March 2015