Jurnal
Teknologi

Full Paper

APPROACH FOR IDENTIFYING COMPONENTS WORTHY OF PROTECTION OF CYBER-PHYSICAL SYSTEMS (CPS) BASED ON A SYSTEM MODEL

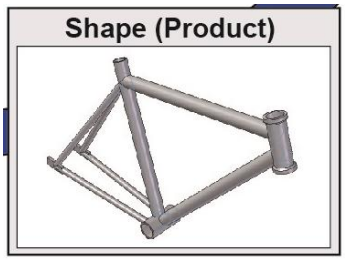
Daniel Kliewe[a*], Lydia Kaiser[a], Roman Dumitrescu[a], Jürgen Gausemeier[b]

[a]Fraunhofer Institute for Production Technology IPT, Project Group Mechatronic Systems DesignZukunftsmeile 1, 33102 Paderborn, Germany
[b]Heinz Nixdorf Institute, University of Paderborn, Fuerstenallee 11, 33102 Paderborn, Germany

Article history
Received
14 January 2015
Received in revised form
25 March 2015
Accepted
29 June 2015

*Corresponding author
daniel.kliewe@ipt.fraunhofer.de

Graphical abstract



Abstract

This paper will improve the system protection for Cyber-Physical Systems (CPS) by the use of the specification technique CONSENS. Therefore an approach is demonstrated and validated. The possibilities how the system protection can be integrated in Model-Based Systems Engineering (MBSE) and especially in CONSENS are shown and discussed. First results how the different views on the system can be used to identify components worth protecting of CPS are presented. The identified components are of crucial importance in order to ensure the protection of CPS.

Keywords: Model-based systems engineering, systems engineering, anti-counterfeiting, intelligent technical systems, cyber physical systems, system security, system protection

1.0 INTRODUCTION

The research presented in this paper deals with the improvement of the protection of cyber-physical systems against all kinds of threads like counterfeiting, manipulation, espionage and know-how loss. To ensure the protection of CPS an approach for the identification of components worthy of protection is demonstrated. This identification is based on a system model and is essential in the holistic protection of intelligent, networked systems such as CPS.

The research in this paper is structured as follows: Todays challenges in protecting CPS are described and requirements for the demonstrated approach identified in chapter two. Chapter three reveals the state of the art and compares the requirements to existing methods. In chapter four the approach for the identification of components worthy of protection of CPS is shown and a validation carried out. At the end of the paper a short summery is given.

2.0 CHALLENGES IN THE PROTECTION OF CPS

2.1 Cyber-Physical Systems (CPS)

CPS differ from mechanical and mechatronic systems because of their inherent intelligence as well as their networking abilities. They are characterized by four core properties in particular: adaptive, robust, predictive and user-friendly [1]. The route to intelligent systems is determined by three general trends in technology: miniaturization of electronics [2], software technology as driver of innovations [3], [4] and networking of information systems [5]

The push towards greater multichannel integration, for example integration of functions or inherent intelligence leads to a greater experience for the customer. However, it also leads to new challenges for an approach in protecting CPS. The increasing amount of integrated functions and interfaces has to

be considered right at the beginning and during the development of CPS.

2.2 Model-Based Systems Engineering

The design of CPS 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. This leads to an increase of complexity and various discipline specific views and different understandings of the system. To meet these challenges a holistic MBSE is required [1].

CPS are promising a great market potential and have the potential for a cross-industry innovation leap, an early understanding and considering of protection measures is therefore inevitable. Hence components worth protecting have to be identified in the early stages of the development.

2.3 Anti-Counterfeiting

In 2013, 71% of all German companies in machine and plant construction were affected by product piracy. The damage caused is 8 billion euros per year since 2011 [6].

Know-how loss, manipulation and product piracy is a worldwide issue. International cyberattacks cause intellectual property loss as described in a joint study by McKinsey and the World Economic Forum in 2014 [7]. 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.

This leads to the challenge that new ways of protecting CPS must be developed and the known protection measures must be adapted. An example to adapt measures is to combine them with the core properties of CPS. Existing protective measures can be improved a lot by connecting them to the characteristics of CPS and using these properties to create an inherent system protection. For example, if a sensor for monitoring activity is combined with the information of many sensors of the CPS, big data analysis are able to find patterns and detect anomaly. If anomaly is found, the adaption can be used to adjust the settings of the CPS so that no manipulation can be done.

To protect CPS and secure the investments from the original manufactures in R&D the found challenges on the protection of CPS must be fulfilled:

- Consider the increasing amount of integrated functions, sensors and interfaces in the beginning and during the development.
- Identify components worthy of protecting in the early stages of the development of CPS.
- Develop new ways of protecting CPS and adapt the known protection measures.

3.0 STATE OF THE ART

3.1 Model-Based Systems Engineering

The creation of CPS includes beside the discipline specific work also ensuring a uniform understanding of the system. The communication and cooperation across the boundaries of individual disciplines is imperative, current methods cannot handle this complexity [8].

According to INCOSE, Model-Based Systems Engineering (MBSE) is the future paradigm of product engineering to meet this challenge [9]. It describes the idea of a holistic description and analysis of the system based on models from earlier phases of the product development over the complete course of the life cycle of the product. The reduction of the real systems to an initially abstract model supports the creation of a holistic understanding of the system [10].

To describe the system model, a modeling method and language are required. The engineering method CONSENS includes a modeling language and a procedure for creating a system model.

CONSENS (CONceptual design Specification technique for the Engineering of complex Systems) is developed at the Heinz Nixdorf Institute within the Collaborative Research Centre (CRC) 614 [11]. It includes a modeling language and focuses on the conceptual design phase of the product development. CONSENS is divided into aspects (so called partial models), which need to be taken into account: requirements, environment, application scenarios, functions, active structure, behavior and shape. In the demonstrated approach the partial models functions and active structure are in the focus of the research. Therefore they are described in detail.

The partial model functions must be divided between the functional hierarchy and the functional structure. To create the hierarchy a decomposition of a complex function is performed in more simply sub function [12]. Each sub function is shown graphically in a hierarchy [13]. The modeling of a solution-neutral functional hierarchy succeeds based on the request list [14].

The central partial model in CONSENS is the active structure. It shows the interactions between the elements of the system. The interaction of the elements is described with flows [11]. We distinguish between material, energy and information flow. System elements represent physical elements as components as well as non-physical elements like software components. Each system element can be refined by other system elements. The result is a hierarchical structure of the system which shows functional nature. This structure is used in the method developed.

The shown components of MBSE help to handle the increasing amount of integrated functions and sensors in CPS. However, MBSE is not designed to consider the aspects of the CPS-protection

3.2 System Protection

Preventive system protection must cover the entire product life cycle starting as early as in the strategic product planning. A sustainable protection can only be achieved through a holistic coordinated set of protection measures, so-called protection concepts. As in [15], 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 80. These have a high potential for the fight against piracy [15]. However, these measures are not designed for the protection of intelligent and communicating systems and therefore have to be renewed or replaced.

There are numerous approaches to the creation of protective measures and protection concepts, for example the procedure of Kokoschka, this procedure was conceived in order to develop imitation-protected products and production systems [16. Or the counterfeiting process according to FUCHS *et al.* [17], the methodology for the protection against product imitation according to Neemann [18], the development of an anti-piracy strategy according to Jacobs *et al.* [19] or the BMBF research initiative "Innovation against product piracy", which conceived the "product protection needs analysis" in the transfer project "ConImit - Contra Imitatio" [15].

Some of the methods consider the protection in the early stages of the development. However, none of the above-mentioned procedures, methods and projects takes the integration of new functions, sensors and interfaces into account. The existing measures and methods do not consider the 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.

4.0 SYSTEM PROTECTION OF CPS BY CONSENS

The specification technique CONSENS is used to describe products and related production systems. It supports the development through the fundamental and interdisciplinary understanding, which is generated by the method. However, CONSENS does not consider the protection of the system to be developed. The demonstrated approach (see Figure 1) is based on the partial models functions and active structure. All three identified challenges (see chapter 1) are fulfilled by this approach. The extended functions model for example considers the integrated functions in the early stages of the development process and initiates new ways of CPS-protection. The extended active structure model contributes to an early understanding of the system and consideration of protection measures. Overall, components worthy of protection are identified.

So that components can be classified worth protecting, they must meet the following properties: They have a high number of connections to other components, are manufactured by the company itself, are characterized by a high level of inherent know-how and they contribute significantly to the fulfillment of the functions of the CPS. These properties can be found examining the partial models.

Some of the partial models are already used by known approaches. For example uses Kokoschka the functional hierarchy, which is a part of the partial model functions [16]. Eckelt *et al*. uses single partial models like the environment or the active structure for a preventive approach for product protection [20]. However, the approach demonstrated in this research focuses not only on using the partial models but on extending them.

Through the extension the models are adapted to fulfil the challenges given in the protection of CPS. By integrating aspects for protection of CPS into the models of CONSENS no additional resources are needed to consider the system protection right in the early stages of the development.

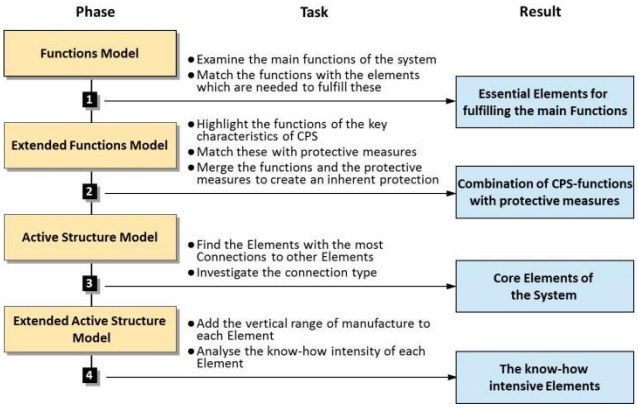


Figure 1 Procedure model for identifying components worthy of protection with CONSENS

The developed approach is applied and validated by an example of the extended active structure model (Figure 2). The example relates to the third and fourth phases of the approach. The first two phases are not considered in this validation. For the identification of components worth protecting for securing CPS the active structure is particularly suitable. Through the active structure the internal interactions between the elements are described

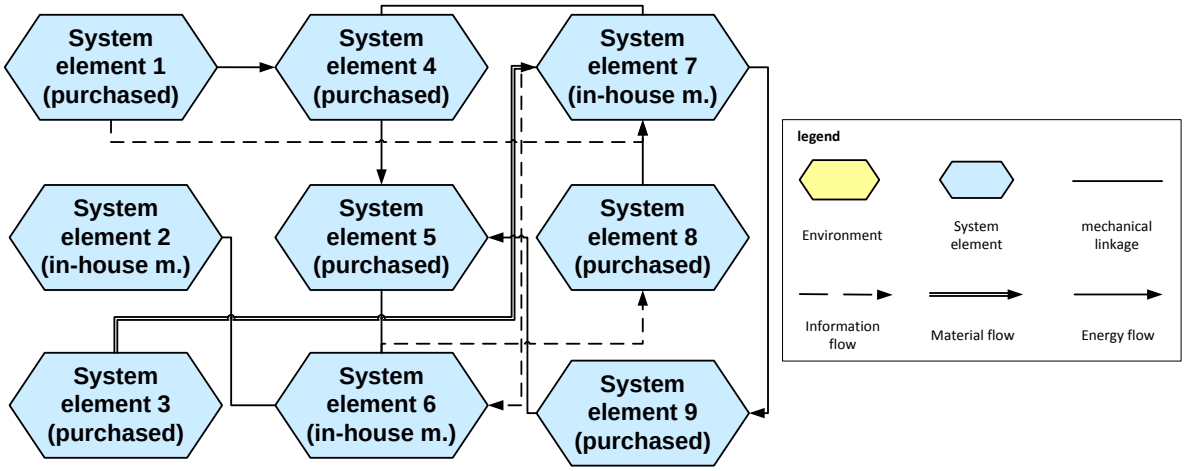


Figure 2 Example for an extended active structure model

The first step in identifying an important element is to count the number of connections at each system element. The element System element 7 has six connections and therefore the most in the shown system; the System element 6 has four connections and should also be taken into account.

The next step is to investigate the connection-type. The System element 7 has different connection and has to be important for different tasks. This element should be further examined.

The System element 6 has also different connection-types. In this case, further information is necessary to see if this element is a core element of the system. One way to do a more detailed analysis is to extend the active structure with the vertical range of manufacture. This helps to find out the know-how intensity of the elements. The elements which are manufactured by the company itself have a high intensity of the company's know-how therefore the protection is of crucial importance. These elements can be found in the extended active structure (see Figure 2).

Three elements are "in-house manufactured", for these elements the know-how intensity needs to be examined in detail. A workshop with employees from the company could be an appropriate way. The elements 6 and 7 were already discussed due to their high numbers of connections; these elements need to be considered to protect the system and are classified worth protecting.

4.0 SUMMARY

The contribution gives insight into new possibilities in the field of system protection that arise when aspects of product protection are integrated in SE. An approach to identify core components which are worth protecting is developed and validated. As a result of this method components worth protecting of CPS can be detected within the process of product development. In further research all partial models of CONSENS have to be examined and adapted to consider the protection of CPS.

References

[1] Gausemeier, J., Tschirner, C., and Dumitrescu, R. 2013. Der Weg zu Intelligenten Technischen Systemen. *Industrie Management*. GITO Verlag.

[2] Herzog, O. and Schildhauer, T. 2009. *(Hrsg.): acatech DISKUTIERT. Intelligente Objekte: Technische Gestaltung – Wirtschaftliche Verwertung–Gesellschaftliche Wirkung*. Springer Verlag, Berlin.

[3] Damm, W., Achatz, R., Beetz, K., Broy, M., Grimm, K. andLiggesmeyer, P. 2010. Nationale Roadmap Embedded Systems. In: Broy, M. (Hrsg.): Cyber-Physical Systems–Innovation Durch Softwareintensive Eingebettete Systeme. *acatech DISKUTIERT*. Springer Verlag, Berlin.

[4] Schäfer, W. and Wehrheim, H. 2007. The Challenges of Building Advanced Mechatronic Systems. *In FOSE ´07: 2007 Future of Software Engineering. IEEE Computer Society*. 72-84.

[5] Broy, M. 2010. (Hrsg.): Cyber-Physical Systems–Innovation Durch Software Intensive Eingebettete Systeme. *acatech DISKUTIERT*. Springer Verlag, Berlin.

[6] Verband Deutscher Maschinen-und Anlagenbau e.V. 2014.(VDMA): Studie Produktpiraterie.

[7] World Intellectual Property Organization (WIPO); Understanding Industrial Property. 2008. WIPO Publication No. 895(E). Geneva.

[8] Gausemeier, J., Czaja, A., Wiederkehr, O., Dumitrescu, R.,Tschriner, C.and Steffen, D. 2013. Systems Engineering in der Industriellen Praxis. In: Gausemeier, J., Dumitrescu, R., Rammig, F. J., Schäfer, W. andTrächtler, A. *(Hrsg.): 9. Paderborner Workshop Entwurf Mechatronischer Systeme, HNI Verlagsschriftenreihe*, Band 310, 18-19. April, Paderborn.

[9] 2007. International Council on Systems Engineering (INCOSE). *Systems Engineering Vision 2020*, INCOSE, San Diego.

[10] Ropohl, G. 2009. *Allgemeine Technologie–Eine Systemtheorie der Technik*. Third Edition. Universitaetsverlag Karlsruhe, Karlsruhe.

[11] Friedenthal, S., Moore, A. and Steiner, R. 2012. A Practical Guide to SysML. *The Systems Modeling Language*. Second Edition. Morgan Kaufmann, Waltham.

[12] Pahl, G. and Beitz, W. 2003. *Konstruktionslehre–Grundlagen Erfolgreicher Produktentwicklung. 5. Auflage*, ISBN 3-540-00319-3. Springer Verlag.

[13] Gausemeier, J., Lanza, G. and Lindemann, U. 2012. *Produkte und Produktionssysteme Integrativ Konzipieren–Modellbildung und Analyse in der frühen Phase der Produktentstehung, München*. Hanser Verlag.
[14] Gausemeier, J., Dumitrescu, R., Tschirner, C. and Stille, K. 2011. Modellbasierte Konzipierung eines hybriden Energie-Speichersystems für ein autonomes Schienenfahrzeug. *Tag des Systems Engineerings 2011 (TdSE)*.
[15] Gausemeier, J., Glatz, R., and Lindemann, U. 2012. (Hrsg): *Präventiver Produktschutz–Leitfaden und Anwendungsbeispiele*. Carl Hanser Verlag, München.
[16] Kokoschka, M. 2013. Verfahren zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme. Dissertation Universität Paderborn, Paderborn.
[17] Fuchs, H. J. 2006. (HRSG.): Piraten, Fälscher und Kopierer–Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China. Betriebswirtschaftlicher Verlag Dr. Th. Gabler, Wiesbaden.
[18] Neemann, C. W. 2007. Methodik zum Schutz gegen Produktimitationen. *Dissertation Fraunhofer Institut für Produktionstechnologie IPT*. Aachen, Shaker Verlag, Band 13/2007, Aachen.
[19] Jacobs, L., Samli, A. C. andJedlik, T. 2001. The Nightmareof International Product Piracy–Exploring Defensive Strategies. In: Industrial Marketing Management 30, S. 499-509, North-Holland Publishing.
[20] Eckelt, D., Altemeier, K. andKliewe, D. 2014. Präventiver Produktschutz-Ein ganzheitlicher Ansatz für die Bedrohungsanalyse. *Industrie Management 1/2014*: S. 55-58, Feb. 2014.