Combined Secure Process and Data Model for IT-Security in Industrie 4.0

Yübo Wang, Riham Fakhry, Sebastian Rohr and Reiner Anderl

***Abstract*—The majority of enterprises identifies the potential and the benefits of Industrie 4.0. However, many companies consider Industrie 4.0 more as a security challenge than an opportunity to optimize their processes or an enabler for new business models. Therefore effective security methods to protect the Industrie 4.0 systems and its associated values and assets are needed. Based on the connectivity infrastructure in the shopfloor, the diversity in the corporate landscape of the global mechanical and plant engineering ultimately causes that every enterprise has to develop its own way of production IT security management.**

The purpose of this paper is to analyze the challenges of IT security in Industrie 4.0 and to identify and combine the requirements from manufacturing automation, mechanical engineering, process engineering and the properties of cyber-physical systems with well-established core elements of IT security descriptions. Having taken all these factors into account a process model, which consists of a data model and an algorithm as its core element is developed to consider the challenges and to cope with the requirements. As a prototypical implementation security measures and their properties are presented in a technological *Industrie 4.0 Toolbox IT-Security*, as the result of the whole process and data model.

***Index Terms*—IT security in Industrie 4.0, Defense in Depth, Security by Design**

I. Introduction

THE fourth industrial revolution (Industrie 4.0) is distinguished by a growing network and intelligence of machines, products, services and data. The property is reflected in the creation of value-added networks across enterprise boundaries [1]. In addition, the traditional way of engineering and its production system goes through a change. The change manifests in digital enterprises, wherein the vision of Industrie 4.0 establishes, on the one hand, the collaborative product development and virtual engineering, on the other hand, it sets up an integrated and intelligent production planning and controlling [2, 13]. Furthermore, the digital network is an opportunity to improve collaboration, coordination and transparency across all business sectors of an enterprise [3].

Holistic technical and organizational changes accompany the horizontal and vertical integration of Industrie 4.0. These circumstances create new security requirements and implications for the product development and enterprise processes, incurred data, production plants and resources [4]. The successful creation of a security culture is one of the important key prerequisites for Industrie 4.0. Only a holistic view for an Industrie 4.0 security culture leads to trustworthy, resilient and socially accepted Industrie 4.0 systems and processes. Such a culture includes both safety and security, where security is divided into office IT security and production IT security [5]. This paper focuses on the environment of the production IT-Security.

The challenges for the production IT security possess diverse characteristics. The diversity, on the one hand, stems from the increasing use of internet technologies in the production area and the trend that in Industrie 4.0 cyber-physical systems (CPS) and cyber-physical production systems (CPPS) merge with Internet of Things, Internet of Services and Internet of Data [6, 17]. Whenever CPS and internet technologies are adopted into machines, the increasing threat of vulnerable IT systems is automatically transferred to the industrial plant. Regrettably there is no way to build an absolutely secure system, however, there can only be different degrees of protection [7].

On the other hand, the networked production resources, cross-organizational collaboration, coordination and transparency across all business sectors of an enterprise and cross-enterprise networks forms a chain of security measures, that - like any chain - is only as strong as its weakest link. Currently used systems have not been designed for the connected mode of operation they are deployed in, hence they usually do not provide security functionality of even security related information like modern IT components does. The IT sub-systems that have so far been used in production environments are not adequately aligned to current security requirements, never mind under the complex networked circumstances of Industrie 4.0 [5].

Consequently, any Industrie 4.0 initiatives need to be designed IT security as one of the key design criteria. An additional challenge is to address on the technology level the

Manuscript received January 07, 2017; revised February 02, 2017. This work was supported in part by the Federal Ministry of Education and Research of Germany (BMBF) in the National Reference Project for IT security in Industrie 4.0 (IUNO). The IUNO research project, identifies threats and risks for the intelligent factory, develops protective measures, and implements them in four use cases. The aim is to develop as general-purpose solutions as possible to meet the challenges of IT security in the industrial application field. The tested and transferable IT security solutions are combined into a toolbox.

Yübo Wang is with the Department of Computer Integrated Design of the Technical University Darmstadt, 64287 Darmstadt, Germany (phone: +49 (0)6151-16-21845; fax: +49 (0)6151-16-21793; email: y.wang@dik.tu-darmstadt.de)

Riham Fakhry is Security Engineer at accessec GmbH, Marktstraße 47-49, 64401 Groß-Bieberau, Germany. (phone: +49 (0)6162 800420 email: fakhry@accessec.com)

Sebastian Rohr is CTO and Managing Director of accessec GmbH (phone: +49 (0)6162 800420 email: rohr@accessec.com)

Reiner Anderl is Head of the Department of Computer Integrated Design of the Technical University Darmstadt, 64287 Darmstadt, (email: anderl@dik.tu-darmstadt.de)

topics of secure networks, secure processes, secure services, and secure data – depending on the requirements each system and process has. Resilient and trusted cyber-physical machines have to be designed and build at the system level. Only based on this foundation, Industrie 4.0 applications will be able to unfold the full potential of its possibilities and benefits.

II. Approaches to IT-Security Strategy and Design in Industrie 4.0

Constantly, new vulnerabilities in IT and CP systems are detected and, consequently, new attack methods are developed to exploit these vulnerabilities. With this insight in mind, it is easy to understand why it is impossible to design a perfectly secure system or to maintain a high-security level over time with no additional effort. IT security is not a goal that is achieved once – it is rather a continuous process based on behavioral change [8].

Security solutions for Industrial Control Systems (ICS) so far have been based only on adding to the complexity of the architecture. This strategy, known as Security by Obscurity, has however only worked well for environments without external communication connections [9]. This single protective measure is bound to create problems on the usability side and primarily does not meet the requirements derived from Industrie 4.0 scenarios, wherein the ICS is not only connected to the internal network but is also extensively connected with external networks and networked nodes under the control of third parties. Therefore, the Defense in Depth strategy has been defined as a model to meet the security requirements for ICS. This layered approach means that in order to secure the entire environment, the use of several protective measures at different points and levels of the system is required [10]. A prerequisite for the Defense in Depth strategy is the division of the system into several separate areas. This separation may be logical and/or physical, e.g. by separating assets, values or different domains [3].

Another important approach is to establish Security by Design as a core design principle. This approach is particularly relevant for the development of future systems. It requires an early assessment of possible threats and the consideration of necessary protective measures in the first phases of product development and in the construction of infrastructures [3]. The result of such an approach is, that only systems with technologies that meet the defined security requirements are allowed to be used [11]. It has to pass the threat analysis and risk assessment for individual components over systems to entire industries [1]. Due to this approach, security is transformed from a subordinate, retrospective issue to an integrated topic in the development process [3].

III. Challenges of IT-Security in Industrie 4.0 in the German industrial landscape

In order to cope with the complexity in Industrie 4.0, several organizations have created guidance for different stakeholders. While the leading institution for promoting German Industrie 4.0 activities, the Platform Industrie 4.0, has announced 17 technology development areas and an implementation roadmap for describing the vision of Industrie 4.0 [12], the Mechanical Engineering Industry Association (VDMA), who represents over 3000 mostly medium-sized companies, published the “Guideline Industrie 4.0” to set up the “Guiding principles for the implementation of Industrie 4.0 in small and medium-sized businesses”. The core method for this is the *Industrie 4.0 Toolbox Product* and *Industrie 4.0 Toolbox Production* [16].

In addition, the “Generic Procedure Model to introduce Industrie 4.0 in Small and Medium-sized Enterprises” (GPMI4.0) performs in four different project formats. First, a holistic company-specific project format over one year with a focus on developing specific solutions and to subsequently implement these solutions successfully in a real production environment [14]. Second, a workshop concept to support the enterprise in generating their own framework to implement Industrie 4.0 [16]. Third, regular competence-building events focusing on knowledge transformation from research projects to industrial approach with respect to Industrie 4.0. Fourth, coaching event for trainers, which imparts the methods and procedures to develop a corporate Industrie 4.0 workshop. Accordingly, there is huge supply and demand in the German market.

Since 2011, when Industrie 4.0 was officially presented during the 2011 Hannover Messe Industrie (HMI) fair, both global players and small and medium-sized enterprises (SME) recognize and identify the potential of Industrie 4.0 applications and its possibilities and benefits with the support and assistance by public or private offers. Enterprises always build specific implementation roadmaps after consuming these initial support and assistance offers. Furthermore, their present production systems or subsystems are analyzed, existing system processes are modeled and ideas to optimize them resiliently or upgrade mechanic systems over mechatronic systems over adaptronic systems to cyber-physical systems are generated. However, IT security issues have been discussed, but have not yet been detailed in secure networks, secure processes, secure services, and secure data.

In the context of Industrie 4.0, an integrated concept is needed, which combines the requirements from manufacturing automation, mechanical engineering, process engineering and the properties of cyber-physical systems with well-established core elements of IT security descriptions. These results in:

A. Diversity of systems and processes (R1)

Industrie 4.0 includes a large number of different, networked systems with many actors and components. These are all involved in several processes throughout the entire product lifecycle [1]. An approach to creating an *Industrie 4.0 Toolbox IT-Security* is designed to meet these requirements.

B. Defense in Depth strategy (R2)

The Defense in Depth strategy is based on the idea of achieving an acceptable level of security for industrial systems not only with a single protective measure but with several adjunct and layered measures. The tendency is to

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

achieve the targeted security level by the combined use of several protective measures of a considered system or component, so that the attack becomes more complicated to execute, and that damage potential of a successful attack is minimized [3, 15].

C. *Threat analysis and risk assessment (R3)*

Threat analysis and risk assessment must be taken as the basis for the procedure in the development of security solutions. In order to ensure the security of the production and the produced product within the Industrie 4.0, the production processes and applications of the produced product must be taken into account [3, 5, 7].

D. *Application-specific security solutions (R4)*

The type and level of security measures should vary based on the threat situation, the value of the considered assets, as well as the present process protection requirements. It should not be defined uniformly [3, 5].

E. *Usability (R5)*

For developing security procedures and measures, the user-friendliness, a holistic, extendable and simple approach and balanced implementation are the key factors. If the measures provide semi-automated assistance and are application-friendly, the user acceptance will be increased [3, 7].

IV. Security Concept Cornerstones

Most enterprises in the industrial landscape would agree that they are severely limited to solve the described challenges and the requirements of IT security in Industrie 4.0. Having taken all these factors into account a process model, which consists of a data model and an algorithm as its core element is developed to consider the challenges and cope with the requirements.

After giving a brief overview of the developed process model, the data model will be described first in section B, the algorithm with its main methods will be explained in detail in section C and a prototypical implementation of an *Industrie 4.0 Toolbox IT-Security* will be explained in detail in section D.

A. *Process Model Level*

As shown in figure 1, on the process model level the developed algorithm accepts different industrial systems as input. Further threat analysis and risk assessments are finalized for the input system. The algorithm acquires and filters security measures from a database. It eliminates security measures that are irrelevant for the given system based on its identified, significant characteristics.

As an output, the algorithm generates a customized catalog of optional security measures represented in a comprehensive framework, the so-called *Industrie 4.0 Toolbox IT-Security*. The algorithm is based on the developed data model and suggests suitable security measures for the input system. As the core element of the process model level, the algorithm is designed using pseudo code for generating the *Industrie 4.0 Toolbox IT-Security*.

Due to a large number of systems and processes within the Industrie 4.0, creation of a static *Industrie 4.0 Toolbox IT-Security* is not sufficient. A procedure oriented *Industrie 4.0 Toolbox IT-Security* is expected to provide relevant security measures depending on the system and application. These security measures and their properties are presented in a technological *Industrie 4.0 Toolbox IT-Security*, as the result of the whole process and data model.

In the following, the components of the process model level will be explained, starting with the database, followed by the system and ends with the toolbox.

Database

The database is essential for the whole model as it stores all important data that was identified by the data model and is significant for the process model itself. Information about system details, security attacks and threats and their correlation to compatible security measures are combined into this database so that the algorithm can use this information to create the expected results. In order to maintain its impact, this database must always be updated with any new systems, arising cyber-attacks and their corresponding security measures. After generating a specific *Industrie 4.0 Toolbox IT-Security*, it would be likewise stored in the database and therefore can be used or updated for similar systems without running through the whole evaluation again.

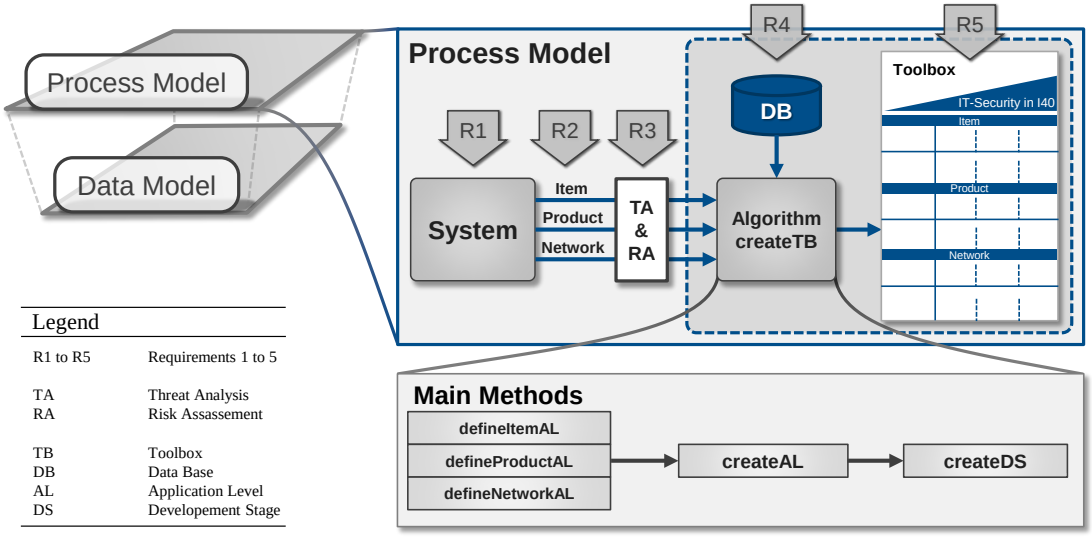

Figure 1. Process Model and Data Model as security concept cornerstones

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

System as input

The input in the process model is an arbitrary system or subsystem that needs to be secured. A system in this context consists of one or more components as hardware or/and software that interact together, building one whole system that is integrated into any industrial process. These are mostly CPS but not exclusively. To enable the algorithm to work with this system, it must be analyzed and represented according to the developed data model. Therefore, the system is divided into three main categories: items, products and networks, which will be referring as components. More information about these three categories will be provided in the section Data Model Level.

Industrie 4.0 Toolbox IT-Security as output

The *Industrie 4.0 Toolbox IT-Security* is an informative framework to represent the results of the foregoing analysis process of the given system as the output of the presented algorithm. It consolidates important information including characteristics of the given system and Industrie 4.0 along with the properties of risk assessment and threat model. The generated toolbox does not recommend the optimal solution for the given system nor can it replace the whole role of an IT expert of implementing a security measure, as it requires mostly more complex analysis and examination of more properties. More likely it is an approach to reduce the efforts and time invested in such a process enabling people with limited knowledge in IT security to take first steps towards designing more secure systems without having to rely on external IT security expertise right from the start. Section D will present the layout and the information provided in such a toolbox in detail.

B. *Data Model Level*

The data model aggregates various properties of Industrie 4.0 and IT security, which are represented in classes and attributes. The developed data model is represented as a UML class diagram in figure 2. To give a simplified overview of the data model's structure and components only classes are presented, attributes and operations are leaving out. The operations are defined in prospect to the algorithm. The attributes are significant characteristics and necessary information of each class prepared for the operations to use them while running the algorithm.

The first class is the **class system**. As explained before, a given system is the input for the algorithm and it would be divided into the three groups: **item**, **product** and **network**, which are the further **classes** in this model.

Any system should consist of at least one item. An **item object** can be for example a server, a machine or simply confidential data, namely any item that can't be divided into smaller items or where sub items are not necessarily to be secured individually. In this way, not only a system but also different assets are secured to fulfill the requirement of secure data. Most objects that are of this class are items with known threats and corresponding security measures.

A **product object** is comparable to the **item object** yet it is defined as a separate class. The **class product** describes only new and innovative products, wherefore no or only limited security-related information are established. Both, **item** and **product objects**, are parts of industrial processes in case there are more than one item and an innovative product in the given system and can be secured as well.

The reason why it is necessary to divide the system into three categories is to adopt the defense in depth strategy by securing each component standing alone and as part of a network. Therefore, the **class network** is necessary.

Hereby, relevant information about each class to enable the measures-filtering process is stored. Especially, attributes like technical requirements reflecting the industrial process, the use case of the system, common threats and security goals are very important. Furthermore, properties of the networks like for example its topology structure or its transmission medium. And according to these attributes amongst other the algorithm is enabled to search for suitable security measures.

To secure an **item** or **network object** the **class threat** is defined. This class holds specific information about a well-known threat or cyber-attack that is related to an **item** or **network object**. Furthermore, it is related to the additional **class risk** and **class security measure**. The risk resulting from a threat is evaluated so that the component is secured depending on its risk level.

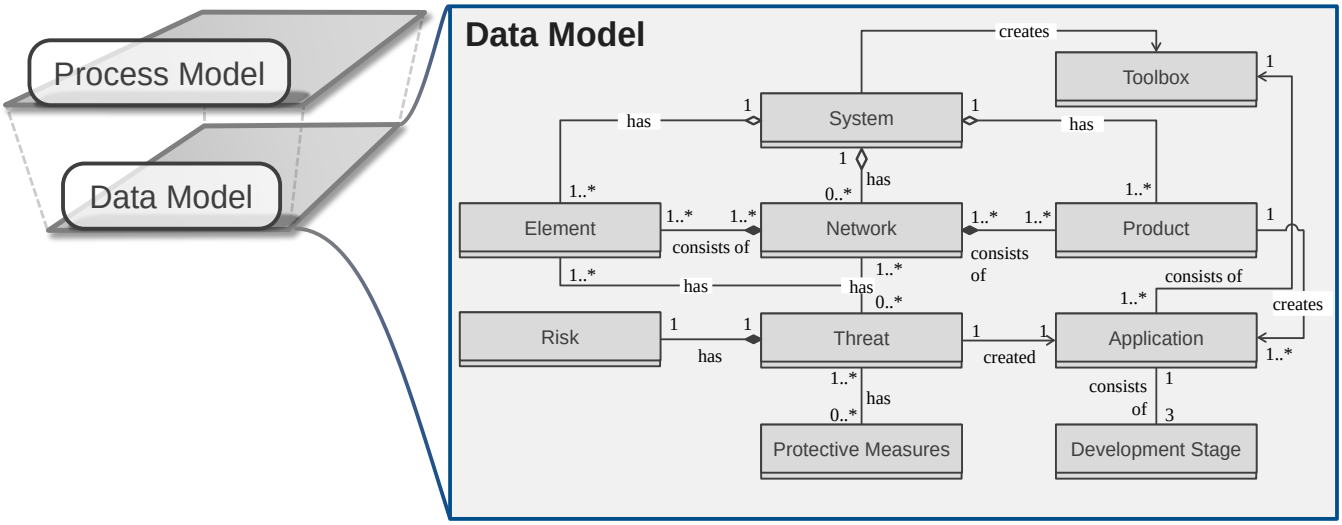

Figure 2. Data Model Level

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The **class security measure** is likewise related to threats and corresponding security goals, items and networks. Most security measures can be deployed for more than one threat case and for different items or networks. Therefore, it has many attributes describing when and how it can be used along with its advantages and disadvantages in a structured and a unified way. In addition to that, each security measure in regards to costs, user-friendliness, latency and security strength is evaluated. These properties are key factors while choosing between many optional security measures as this choice will differ conforming to the use case and preferences of the user. Especially, when talking about Industrie 4.0 the latency factor is very determining. Many industrial processes are in real-time and hence it wouldn't tolerate a security measure that would cause latency within this critical process.

The strength of a security measure is defined as its ability to withstand a direct attack [18]. A user can hereby weigh between how secure he wants his system or components to be and how much is his system will be worth in terms of costs and effort. The result of the user's preferences concerning a component is hence added to the object of this component.

The **class threat**, **class risk** and **class security measure** along with their attributes fulfill the requirements resulting from the threat modeling and risk assessment process, whereas the **class system**, **class item**, **class product** and **class network** represent industrial systems and processes. To represent the result of the security process within the *Industrie 4.0 Toolbox IT-Security* the **class toolbox**, **class application level** and **class development stage** are defined. In this model, a **toolbox object** consists of horizontally arranged **application level objects**. Each **application level object** is defined by a component, namely an item, a product or a network, a threat and the targeted security goal and thus describes an application level of a cyber-attack and its properties. An **application level object** is composed of three security measures each represented as a **development stage object**.

C. Algorithm as core element

The algorithm in our model is designed to support the Defense in Depth strategy by securing a system and its components. The input of the algorithm is hence a system categorized into items, products and networks. The output is a collection of suggested security measures represented in an *Industrie 4.0 Toolbox IT-Security* that is conformingly divided into three categories. The algorithm contains three main operations that are responsible for each of the three categories (Listing 1). To give an overview, the scope of the description of the algorithm is limited in the important parts of the pseudo code.

```
1  PROCEDURE createTB (item, product, network)
2      TB := defineItemApplicationLevel (item)
3      TB := defineProductApplicationLevel (item)
4      TB := defineNetworkApplicationLevel (item)
5  END PROCEDURE
```

Listing 1. Main method for creating *Industrie 4.0 Toolbox IT-Security*

The operation **defineProductApplicationLevel** generates the application level for the products of a given system. The approach for securing a product differs from the approach adopted for items or networks due to the lacking experience with this new product. For a new product, well-known threats or cyber-attacks is not looking for, but rather try to categorize the product to a technology level. Determined by the identified technology level the algorithm suggests a rather general security measure. After gaining more experience with this product, it can then be considered as an **item object**.

The operations **defineItemApplicationLevel** and **defineNetworkApplicationLevel** perform similar steps to generate the application level for their components. Each operation goes sequentially through the list of components of a given system. For each component, it identifies its security goals and subsequently it identifies the threats related to a security goal. Based on the assets of the component item or network, the process in which it is involved and the properties of this specific threat the risk associated with this threat is evaluated. To avoid unnecessary efforts and expenses items or networks according to their risk level are secured, so that low-risk threats are sorted out without searching for suitable security measures. After filtering the threats, the algorithm starts searching for security measures in the database that matches the user's requirements of the component and the network properties for the case that the component in consideration is a network and not an item.

After identifying suitable security measures for a specific application level, each of the above-described operations calls the operation **createApplicationLevel** given the identified collection of security measures and the user's preferences concerning the component (Listing2). The security measures' collection is categorized into three different levels analogous to the three levels of security strengths described earlier this section. For each category, the algorithm searches for the relatively best security measure that matches the user's preferences. In some cases, the user's priority throughout the security process is to deploy economical or user-friendly measures and thus the security measures would be selected in correspondence to the user's preferences.

```
1  PROCEDURE createApplicationLevel (component, measures, featuresPrio)
2      if component == Product then
3          name := setProductALName (TBProductAL)
4      else
5          name := seALName (component, protectionTarget, threat)
6      end if
7      measuresCategories := sortMeasures (measure)
8      for all (measuresCategories) do
9          optimalMeasure := getOptimalMeasure (measuresCategories, featuresPrio)
10         developmentStage =: createDevelopmentStage (optimalMeasure)
11     end for return applicationLevel
12 END PROCEDURE
```

Listing 2. Main method for creating development stage

The selected security measure is then given to the operation **createDevelopmentStage** as an input value. This operation is responsible for generating a new **development**

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

stage object based on the information derived from the security measure (Listing 3). As stated earlier in this section, a security measure is evaluated by its security strength, so that by default the development stage are sorted accordingly. Furthermore, the other three evaluation factors of the security measure are explicitly mentioned and represented in a **development stage object**, so that the user is provided with enough information about the selected security measure. In addition, the technical requirements of the component that couldn't be fulfilled by the suggested security measure are also explicitly mentioned, for the user to be informed about the properties of the suggested security measures.

```
1  PROCEDURE createDevelopmentStage (optimalMeasure)
2          stage := setStage (optimalMeasure)
3          stageName := setStageName (optimalMeasure)
4          if further Measures != EMPTY then
5              Point to further Measures furtherMeasures
6          end if
7          stageRealtime := setRealtime (optimalMeasure)
8          stageCosts := setCosts (optimalMeasures)
9          stageEffort := setEffort (optimalMeasures)
10         if missingRequirements != EMPTY then
11             Do not point to fulfilled Requirements missingRequierements
12         end if return developmentStage
13 END PROCEDURE
```

Listing 3. Main method for creating development stage

D. Prototypical Implementation of an application level in the Industrie 4.0 Toolbox IT-Security

The basic concept to generate the *Industrie 4.0 Toolbox IT-Security* of a given system is developed. At the same time, it can be classified as an informative intermediate solution for users with no or little IT security knowledge by representing the solution and the relevant characteristics in an illustrative way. The structure of the *Industrie 4.0 Toolbox IT-Security* is defined in application level vertically and development stage horizontally. An application level displays IT security themes in Industrie 4.0, where every application level is broken down into different technological and sequential stages. The highest stage represents the highest IT security measures. As an example for one variation of application levels, which results from the call of the procedure **createApplicationLevel** the application level *Network* includes the component *Sensor-Network*, the protection Target *confidentiality* and the threat *eavesdropping* is shown in figure 3. The development stages *AES*, *Public-Key Encryption* and *Random-Key Predistribution* with their properties *realtime*, *costs* and *effort* will be returned by the call of the procedure **createDevelopmentStage**. In addition, these properties will rate as *yes/no* or *low/medium/high*.

Network			
Sensor-Network confidentiality eavesdropping	**AES** Realtime: Yes/No Cots: low/medium/high Effort: low/medium/high	**Public-Key Encryption** Realtime: Yes/No Cots: low/medium/high Effort: low/medium/high	**Random-Key Predistribution** Realtime: Yes/No Cots: low/medium/high Effort: low/medium/high

Figure 3. Application Level Sensor-Network

V. CONCLUSION

The change of the industrial landscape by Industrie 4.0 is described by introducing the horizontal and vertical integration of Industrie 4.0 and the digital enterprises. Consequently, a security culture is one of the important key prerequisites for Industrie 4.0. The diverse characteristics of production IT security, the enterprise chain of security measures, and the coming complex networked circumstances of Industrie 4.0 forms challenges for the production IT security.

After characterizing the approaches to IT security strategy and design in Industrie 4.0, Defense in Depth for present systems and Security by Design for new systems, and the Challenges of IT security in Industrie 4.0 for the German industrial landscape results in five requirements. In order to cover these requirements a process model, which consists of a data model and an algorithm as its core element is developed. As a prototypical implementation security measures and their properties are presented in a technological *Industrie 4.0 Toolbox IT-Security*, as the result of the whole process and data model.

REFERENCES

[1] H. Kagermann, W. Wahlster, and J. Helbig, *Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Securing the future of German manufacturing industry*, April 2013.

[2] E. Abele, R. Anderl, J. Metternich, A. Wank, O. Anokhin, A. Arndt, T. Meudt, M. Sauer, *Effiziente Fabrik 4.0 - Einzug von Industrie 4.0 in bestehende Produktionssysteme*, published in ZWF – Zeitschrift für wirtschaftlichen Fabrikbetrieb, pp. 150-153, 2015.

[3] BITKOM, VDMA, ZVEI, *Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht der Plattform Industrie 4.0*, April 2015 https://www.bitkom.org/Publikationen/2015/Leitfaden/Umsetzungsstrategie-Industrie-40/150410-Umsetzungsstrategie-0.pdf, [accessed on November 10, 2016].

[4] R. Anderl, *Industrie 4.0 – technological approaches, use cases, and implementation*, published in *at – Automatisierungstechnik 2015*, vol 63, pp. 753-765.

[5] BMWi, *IT-Sicherheit für Industrie 4.0*, http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0-langfassung,property=pdf,bereich=bmwi2012, sprache=de,rwb=true.pdf, [accessed on November 30, 2016]

[6] T. Bauernhansl, M. ten Hompel, B. Vogel-Heuser, *Industrie 4.0 in Produktion, Automatisierung und Logistik. Wiesbaden*: Springer Fachmedien Wiesbaden, 2014.

[7] K. Böttinger, B. Filipovic, M. Hutle, S. Rohr, *Leitfaden Industrie 4.0 Security – Handlungs-empfehlungen für den Mittelstand*. Frankfurt am Main, VDMA, 2016.

[8] T. Phinney, "IEC 62443: Industrial Network and System Security", Published in ISA. http://www.isa.org/autowest/pdf/Industrial-Networking-and-Security/Phinneydone.pdf, [accessed on November 10, 2016]

[9] D. Kuipers, M. Fabro, *Control Systems Cyber Security: Defense in Depth Strategies - Recommended Best Practice: Defense in Depth*, INL-Idaho National Laboratory, 2006.

[10] Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies - Control Systems Security: National Cyber Security Division*, 2009.

[11] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, *Challenges for Securing Cyber Physical Systems*. https://chess.eecs.berkeley.edu/pubs/601/ [accessed on November 10, 2016].

[12] Plattform Industrie 4.0, *Neue Chancen für unsere Produktion – 17 Thesen des Wissenschaftlichen Beirats der Plattform Industrie 4.0*, http://www.its-owl.de/fileadmin/PDF/Industrie_4.0/Thesen_des_wissenschaftlichen_Beirats_Industrie_4.0.pdf, [accessed on November 19, 2016].

[13] BMBF, *Zukunftsbild Industrie 4.0*, http://www.bmbf.de/pubRD/Zukunftsbild_Industrie_40.pdf., 2014, [accessed on Nov.17, 2016, 2016]

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[14] Y. Wang, G. Wang, R. Anderl, *Generic Procedure Model to Introduce Industrie 4.0 in Small and Medium-sized Enterprises*, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2016, 19-21 October, 2016, San Francisco, USA, pp971-976, ISBN: 978-988-14048-2-4.

[15] K. Stouffer, J. Falco, K. Scarfone, *Guide to Industrial Control Systems (ICS) Security -NIST Special Publication 800-82.Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC): Recommendations of the National Institute of Standards and Technology*. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.353.2376. [accessed on November 15, 2016]

[16] R. Anderl, A. Picard, Y. Wang, J. Fleischer, S. Dosch, B. Klee, J. Bauer, *Guideline Industrie 4.0 – Guiding principles for the implementation of Industrie 4.0 in small and medium sized businesses*, VDMA Forum Industrie 4.0, Frankfurt, 2015, ISBN: 978-3-8163-0687-0

[17] BMWi, *Autonomik für die Industrie 4.0*, http://www.autonomik.de/de/1003.php, [accessed on July 10, 2016].

[18] Bundesamt für Sicherheit in der Informationstechnik, *IT-Sicherheitskriterien*,1989. https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/Zertifizierungnach CC/ITSicherheitskriterien/DeutscheITSicherheitskriterien/dtitsec.html, [accessed on November 19, 2016]

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)