Risks of Industrie 4.0 - An Information Technology Perspective

T. Usländer[1], C. Thomalla[2]

[1]*Fraunhofer IOSB, Karlsruhe, Germany. E-mail: thomas.uslaender@iosb.fraunhofer.de*

[2]*Fraunhofer IOSB, Karlsruhe, Germany. E-mail: christoph.thomalla@iosb.fraunhofer.de*

ABSTRACT: The term "Industrie 4.0" denotes the advent of the fourth industrial revolution which will be characterized by the optimized and networked use of information across the complete life cycles of both products and production assets. The exploitation of Industrie 4.0 paradigms in terms of economic benefit, flexibility and better-informed decision taking requires the availability and provision of adequate information across all engineering and production value chains in an interoperable way, preferably based upon international standards. Up to now, a hierarchical structure of information technology (IT) systems, the so-called automation pyramid, is predominant in industrial production environments. This leads to a separation of office and production networks that shield the safety- and real-time critical field and controller level from inadequate access from upper levels and remote users. Now, with the application of the paradigms of the Internet of Things and Services (IoTS), there is an architectural trend towards a mash-up of networked smart devices and services, deployed within and across enterprises in order to enable new higher-level services and business models such as smart maintenance. This contribution considers this architectural IT paradigm shift from a risk management perspective.

Keywords: Industrie 4.0, information technology, Internet of Things, vulnerabilities, cyber security.

1. INTRODUCTION

Since its inception in 2013, the German initiative Industrie 4.0 has raised substantial interest among the industrial stakeholders, starting with Germany, in the meantime around the world. This is due to the quite challenging high-level vision, which, once the Internet of Things and its related and emerging technologies will be fully exploited, will have disruptive and decisive effects on business levels. New business models based on cyber-physical systems and (big) data analytics are expected to change the way of industrial production in such a way that it may be called the 4th industrial revolution. Most members of the Industrie 4.0 community rather think in terms of decades than years as to when the full vision will be state-of-the-art.

Hence, the term "Industrie 4.0" denotes the advent of the 4th industrial revolution which will be characterized by the optimized and networked use of information across the complete life cycles of both products and production assets. The exploitation of Industrie 4.0 paradigms in terms of economic benefit, flexibility and better-informed decision taking requires the availability and provision of adequate information across all engineering and production value chains in an interoperable way, preferably based upon international standards. Such information is the result of aggregation and fusion functions applied to (big) data from various heterogeneous sources, often under real-time conditions and from production plants under constant change and different ownership. This comprises a challenge for the provision of an efficient, secure and dependable information management infrastructure.

2. ARCHITECTURAL CONSEQUENCES OF INDUSTRIE 4.0

Up to now, a hierarchical structure of information technology (IT) systems, the so-called automation pyramid, is predominant in industrial production environments. This leads to a separation of office and production networks that shield the safety- and real-time critical field and controller level from inadequate access from upper levels and remote users. Now, with the application of the paradigms of the Internet of Things and Services (IoTS) (Usländer, 2014), there is an architectural trend towards a mash-up of networked smart devices and services, deployed within and across enterprises in order to enable new high-level services and business models such as smart maintenance.

According to the vision statement of the Platform Industrie 4.0 (2014) the step towards I40 requires the “availability of all relevant information in real-time by the connection of all entities that are participating in a value chain” as well as “the capability to derive the optimal added value” at any process step in the chain. Entities may be humans, objects and systems. From the technological perspective, these ideas coincide with the application of the principles of distributed processing and the emerging Internet of Things and Services to the domain of industrial production (Usländer and Epple, 2015).

This vision results in dynamic and self-organizing value chains across enterprise borders which may be optimized according to criteria like cost, availability, resource consumption etc. These new applications require interoperability across systems and the access to necessary data in a granularity they need and not just aggregated data at the respective level of the automation pyramid (Schleipen et al, 2011). Commonly Manufacturing Execution Systems (MES) serve as such data hub for production information interchange.

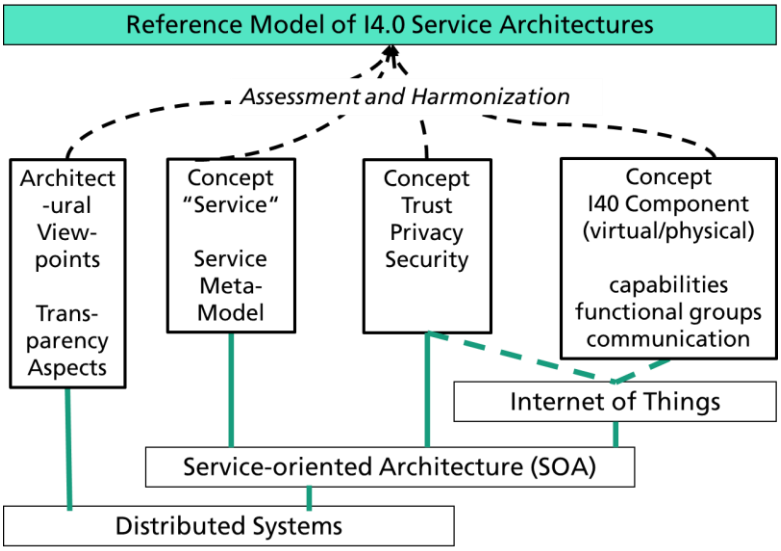

Fig. 1: Influencing Concepts for a Reference Model for Industrie 4.0 Architectures

These requirements prevent a complete segregation between Office IT and production IT, or more general, between networks with different security needs. But network segregation is essential for IT security, as it forces an intruder to overcome several barriers and allows different security policies in the networks.

The access of a wide range of different data sources raises the question of how a common data repository should look like. The use of jointly maintained data heavily depends on digital sovereignty, i.e. control over the own data, privacy and protection, especially intellectual property rights (IPR), thus sustaining independence.

3. RISKS AS SEEN FROM AN ICT VIEWPOINT

This contribution considers this architectural IT paradigm shift from a risk management perspective. What are the new risks and vulnerabilities associated with respect to security and dependability of production systems and critical infrastructures? How can these risks be taken into account already in the requirements analysis and design phase? What can be done in existing production environments for risk mitigation? The contribution provides a terminological structure and mirrors possible answers to these questions at emerging IoTS reference architectures. Organizational risks and avoidance strategies are not in the focus here.

3.1 Design Principles

For new production systems security is a functional requirement and security by design a design principle. This may be achieved by protecting the information flows, the data sources and sinks and intellectual property. Other means are monitoring the production line IT using security software.

Technically the information flow in a production system, data sources and sinks may be protected by encryption to prevent misuse and unauthorized access. When using public networks, an end-to-end encryption is necessary. Restricting the access to the systems and networks protects the data as well. This may be refined to a defense-in-depth strategy.

Unique and secure identification for products, processes and machines and integrity of the components is needed for secure information exchange throughout the entire manufacturing process. It may contain the security classification of the assets and be used for determining the overall security of a system.

Production line IT security software comprises intrusion detection systems (IDS) or rather more comprehensive software for cyber-attack detection and response for industrial control systems. One approach to detecting and mitigating cyber-attacks, that adopts several key features for improving cyber-protection, uses security enclaves, perimeter defense and interior anomaly detection, an event correlation framework, a countermeasure management system, open source tools and standards, is PRECYSE (McLaughlin et al, 2014). A security enclave is a subset with common security policies, in order to minimize the attack surface and the impact of security breaches. Enclaves may be defined by logic function, role or physical location. A production infrastructure can be divided e.g. into Process network, supervisory control and data acquisition (SCADA) network, Office Network and Central System enclaves.

There the enclaves are monitored by a comprehensive set of tools in order to protect all classes of IT assets. For enclaves that include specialized SCADA operations, customized tools can be adopted to enhance security monitoring capabilities. This network

segregation is one means to enhance IT security, as it makes it more difficult for an intruder who then has to overcome several barriers.

For an IDS architecture, the target infrastructure segmentation into multiple security areas is an architectural approach, which reflects the enclave model. Such a model basically introduces a multiple instantiation of modules devoted to data extraction, anomaly detection, alert correlation and countermeasure selection, replicating a logic building block for each segregated part of the monitored network. For existing systems this design decision results in a separate security system enclave (Krauss and Thomalla, 2016).

The framework segmentation organizes the functions in a distributed manner, where each identifiable portion of the target network system, i.e. SCADA Network, Office Network, external/ Perimeter Network, is managed, as for security data collection and correlation by a separate enclave instance, communicating with other instances. The domain model can be regarded as a special form of static, design time, application partitioning, where the services provided by the platform are shared between the domain logic layer and the central layer.

Of course production IT software with built-in security functions like an IDS increases complexity or a particular critical safety function of a subsystem raises the risk of cyber-attacks and thus might make the system vulnerable.

Security focuses on confidentiality, integrity and availability, whereas safety means not to endanger either people or the environment and requires operational safety and a high degree of reliability. As security is a prerequisite for safety, increasing the first will make the production processes safer. If an intruder is able to interfere with the data acquisition, he may easily change sensor data making the control system react in panic and the process running out of control.

As existing production environments were often planned for a lifetime of 30 years or more, during that time functions may be added, additional sensors included and connections for remote maintenance, or to enterprise resource planning (ERP) systems installed. As a result, networks that were separated before, e.g. Office IT and production IT, are no more. In general at that time security was no functional requirement for the application. Then the connection of production systems to the internet made them vulnerable by external threats and attackers. For risk mitigation these systems need an IDS.

The above IDS solution fits into existing or to-be-created SCADA systems as it does not alter too much, to further enable the proper functioning of the existing control system. It interferes as little as possible with the underlying SCADA system, which results in some kind of "minimal-invasive" security platform supervising the operational system (Krauss and Thomalla, 2016). But when implementing security measures like cryptographic processes or authentication procedures one has to consider the impact of these on time-critical functions or resource availability.

To support collaborative industrial business processes, a jointly maintained data repository has to ensure security and privacy of the data. The owner of the data has to decide upon who is allowed to use the data, e.g. his own medical history or data in a supply chain. The confidence in data sovereignty is a crucial point for the acceptance of a project called Industrial Data Space as a secure data container compared to a cloud. The Industrial Data Space provides basic services like the anonymization of data, integration services and the setting of expiry dates for the use of the data.

3.2 Risks

Among the risks is the fact, that there is currently a lack of fully standardized operating platforms for implementing adequate safety and security solutions that have been tailored to the specific requirements of industry in terms of their implementation and cost. Sometimes there are solutions for specific problems available but they have yet to be implemented. Today's IDS still cannot detect reliably breaches of the system, if the attack patterns are rather unknown. There is no easy way to integrate new technologies into older ones and old systems will need to be upgraded with real-time enabled systems. Ideally there would be a continuous surveillance of a plant without having physical access to it and without interfering with its control system.

In general safety and security solutions have to be user-friendly to be accepted, as people tend to avoid using processes and applications that are not.

Historically in production people are not IT specialists. Innovations in IT advance faster than they do in production, which may explain the different life cycles as well. Awareness-raising for security will lead to a demand for more and better skilled personnel. The need for inter-disciplinary training of all the people involved in production is growing and has to prepare the required workforce. Security awareness often plays a key role, particularly with regard to IT security issues. Currently the level of security awareness in different industries varies strongly.

When cooperation between several different partners in a value chain is required, it will be necessary for partners to have a high level of confidence in each other's competence.

There is insufficient monitoring of risk assessment indicators, particularly with regard to industrial IT security. Analysis and assessment of IT security right at the planning phase is not yet available.

3.3 Standards

There are standards for risk management like ISO 70021 (ISO, 2008), IEC 62443 (IEC, 2012), which was formerly ISA 99 and recommendations like the VDI/VDMA risk analysis (VDI, 2008).

The standard IEC 62443 introduces a holistic view of management, system, and component. It explains concepts like zoning, conduits and security assurance levels (SAL) for industrial environments and may be used as a standard for certifications. Applying 62443 shows how security requirements can be derived.

It comprises risk identification, classification, and assessment. It suggests methodologies for risk management and implementation, system development and maintenance, information and document management, and security threat analysis. A risk assessment, combined with a vulnerability assessment and threat scenario analysis, specifically identifies cyber vulnerabilities that may be eliminated.

The threat and risk model identifies and evaluates the threats and risks with regard to the protection targets integrity, confidentiality, availability, authentication and authorization. For the analysis, identification and evaluation of risks and new challenges both people and processes and all layers of the IT infrastructure of industrial production environments are taken into account.

While the threat model refers to aspects such as the potential attackers, the possible attack vectors, and assets worth protecting, the risk model allows based on specific parameters (e.g. exposure of a production plant, danger to life, financial risks, etc.) to estimate an overall risk.

4. CONCLUSIONS

This contribution considers the new risks and vulnerabilities associated with respect to security and dependability of Industrie 4.0 and how these risks can be taken into account in the design phase. Security incidents may raise the risk for the population, especially in critical infrastructures like the chemical industry or at water and power suppliers. As security is a prerequisite for safety, increasing the first will reduce the risk of disastrous incidents caused by production processes. Doing so increases security and reliability of supply e.g. with water and energy, which are technically close related to production.

Safety and security cannot simply be broken down into functional components but should instead be seen as a process. A part of disaster risk management deals with fail safe procedures, which often do not exist or are not implemented. There is no standardization for recovery yet. The integration of safety and security is still missing.

Strong support by the top-management for the implementation of IT security is essential. There still is a lack of standardization, poor work organization and availability of products for security.

5. REFERENCES

IEC-62443-1-1 (ISA99.01.01): Security for industrial automation and control systems. Terminology, Concepts and Models, Draft 1, Edit 7, August 2012. IEC-62443-2-1 (ISA99.02.01) Security for industrial automation and control systems Part 2-1: Industrial automation and control system security management system Draft 6, Edit 4, September 2012.

IEC-62443-2-2 (ISA99.02.02) Security for industrial automation and control systems Part 2-2: Operating an IACS Security Program, Draft 1, Edit 4, March 2011.

ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, September 2008.

ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management, 2005.

Krauss, Daniel; Thomalla, Christoph (2016). Ontology-based Detection of Cyber-Attacks to SCADA-Systems in critical Infrastructures, Int. Conference on Digital Information & Communication & its Applications (DICTAP 2016), Konya, Turkey.

McLaughlin, Kieran; Sezer, Sakir; Smith, Paul; Ma, Zhendong; Skopik, Florian (2014). PRECYSE: Cyber-attack Detection and Response for Industrial Control Systems, Proceedings of the 2Nd International Symposium on ICS \& SCADA Cyber Security Research 2014, 2014, isbn 978-1-78017-286-6, p. 67-71.

Plattform Industrie 4.0 (2014). Was Industrie 4.0 (für uns) ist. http://www.plattform-i40.de/blog/was-industrie-40-für-uns-ist

Plattform-i40, (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report of the Industrie 4.0 Working Group, http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_ Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf

Schleipen, Miriam; Münnemann, Ansgar; Sauer, Olaf (2011). Interoperabilität von Manufacturing Execution Systems (MES) – Durchgängige Kommunikation in unterschiedlichen Dimensionen der Informationstechnik in produzierenden Unternehmen, *at - Automatisierungstechnik* 59 Nr. 7, S. 413-424, Oldenbourg Wissenschaftsverlag, 2011.

Usländer, Thomas; Epple, Ulrich (2015). Reference model of Industrie 4.0 service architectures: Basic concepts and approach. *Automatisierungstechnik:* AT 63 (2015), No.10, pp.858-866 ISSN: 0178-2312.

Usländer, Thomas (2014). The trend towards the Internet of Things: what does it help in Disaster and Risk Management? *Planet@Risk*, Volume 1, Number 1.

VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung. Beuth, 2008.