Security In Industrie 4.0 - Challenges and Solutions for the Fourth Industrial Revolution

Michael Waidner*†, Michael Kasper†

*Technische Universität Darmstadt
Security in Information Technology (SIT)
64289 Darmstadt, Germany
waidner@informatik.tu-darmstadt.de

†Fraunhofer Institute for
Secure Information Technology (SIT)
64295 Darmstadt, Germany
{michael.waidner, michael.kasper}@sit.fraunhofer.de

***Abstract*—Information technology (IT) is one of the most important drivers of innovation in production and automation. In Germany, the term Industrie 4.0 summarizes various activities and developments involved in the evolution of industrial processes in production, logistics, automation, etc. Many research and development projects work on different aspects of these developments. In the view of politics, industry, and IT enterprises, sufficient IT security is considered an essential prerequisite for the future of production. Although many current IT security solutions can be applied in Industrie 4.0 context, they do not satisfy requirements of processes in Industrie 4.0. Work needs to be done on underlying security mechanisms as well as on security architectures.**

I. Security in Industrie 4.0

The industrial sector is of paramount importance for the German economy. Thus, Industrie 4.0 is a cross-industry issue, explored by *Verband Deutscher Maschinen und Anlagenbauer* (VDMA), *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien* (BITKOM), and *Zentralverband Elektrotechnik- und Elektronikindustrie* (ZVEI). Elsewhere, particularly in the USA, the topic is not only mainly driven by the IT industry and frequently detached from the respective industrial context. There the topic is known as the *Industrial Internet* but much more as the *Internet of Things*. In Asia Pacific Industrie 4.0 also gaining a momentum, there referred to as »Industrial Internet of Things« (IIOT), »Intelligent Manufacturing« or »Digital Industry 4.0« [31].

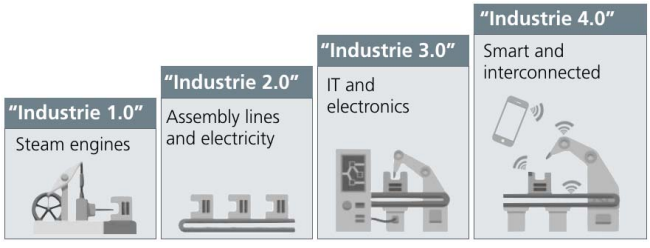

Figure 1: Industrial Revolution

Using cloud services, customers may be closer involved in product design and production planning, possibly resulting in completely new standards for product personalization. Cloud services also provide an opportunity to make workflows dynamic, which may lead to new virtual organisations and new types of work. Such IT-driven industrial development is called the Fourth Industrial Revolution in Germany, or Industrie 4.0 - resp. I4.0 in short; which is determined by 1) horizontal integration through value networks, 2) end-to-end digital integration of engineering across the entire value chain, and 3) vertical integration and networked manufacturing systems.

There are foreseeable security impacts of integration. The paradigm shift from industrial automation in Industrie 3.0 to Industrie 4.0 requires the development of new security and protection mechanisms for the faster and more flexible collaborative value networks and smart production systems (cf. Figure 1). The development of holistic protection concepts with innovative technologies for Industrial IT security along the value chain need to be established [2, 17, 34]. From a research perspective, the foundation is intended to be laid by several public-private initiatives, e.g. [4, 12], I4.0 innovation and research labs [10, 13, 18, 25] and national-fundend reference projects focusing on I4.0 cyber-security, e.g. IUNO [3].

A. IT Security in Industrie 4.0: Old and New Challenges

In the industrial sector, the term *security* is almost synonymous with *operational safety*, meaning the protection of the physical environment, e.g. people, infrastructure, machines and equipment from the consequences of more or less random mistakes coming from the cyber-physical production systems (CPPS) (cf. Figure 2). Industrial plants are always tempting targets for economically and politically motivated saboteurs. However, significantly through the vision of Industrie 4.0 and marked increase of serious attacks, the need for a rigorous protection of ICS and Industrial IT has entered the spotlight. Resilience and protection against sophisticated cyber attacks by insider, spies and organized crime included.

Wide Attack Surface of CPPS: Today's production IT is being attacked with the same strength and methods as today's business IT. Examples of the vulnerability presented by almost any IT system are well known. In June 2010, Stuxnet demonstrated that an industrial plant can be de-

978-3-9815370-6-2/DATE16/

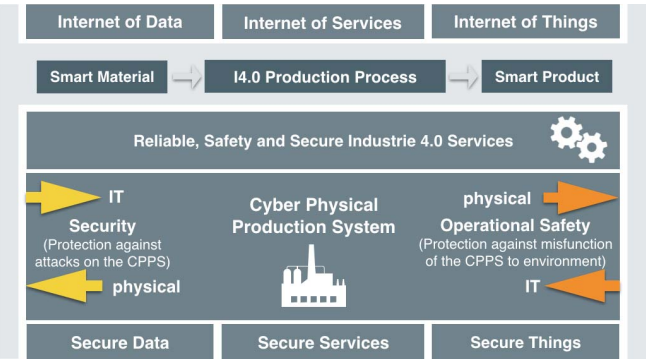

Figure 2: Industrie 4.0 Building Blocks

stroyed by a purely digital attack [6, 21]. Until then, such attacks were considered merely hypothetical threats. Since July 2013, Edward Snowden has been revealing the nearly unlimited possibilities the US American secret service NSA, the British secret service GCHQ and other services have to spy on and manipulate IT systems. One can only deduce that other countries have similar spy programs.

On its fundament, smart factories in the Industrie 4.0 consists of several interoperating CPPS, built of interconnected embedded systems using I4.0 services that control physical processes through sensors and actuators. In general, a systematic protection from such attacks tends to run behind the implementation of IT itself and is usually accompanied by a delay - resulting in security gaps, vulnerabilities and serious threats, e.g. [5, 7, 8, 16, 23, 33]. On the physical layer, a CPPS, or more general an embedded system, is typically subject to lower-level attacks e.g. implementation attacks and physical cryptanalysis, including invasive hardware attacks, side-channel attacks, fault-attacks and hardware reverse-engineering, low-level silicon attacks, up to semi-invasive frontside/backside emissions and FIB-attacks even on high integrated SoC's [20, 24].

The risk that such gaps may be exploited must be rated as very high, especially in industry. The raising interconnectedness as well as the increasing complexity of processes, both coming along with Industrie 4.0, enlarge the attack surface and higher risks.

II. Challenges and Solutions

Until now, IT security solutions are focused predominantly on protecting business IT. In principle, the known concepts may be transferred to production IT as well. However the two worlds differ significantly in their details. In business IT, for example, integrity and confidentiality are the primary objectives. Accordingly, attacks are frequently countered at the expense of availability: Once an attack is detected, uncritical systems may simply be shut down. On the other hand, in production IT, a fast system restart is typically harder to accomplish. In the production setting, the primary goal is to avoid physical injury or damage to human, the environment, and equipment. Thus, confidentiality is considered subordinate; the primary objectives are integrity and availability.

Further differences result from, for example, the stricter realtime requirements in production; the potentially low memory and computing capacities of CPS and, from an IT standpoint, the exceptionally long lifecycle of industrial plants [15]. Additionally, in contrast to business IT, the areas of design protection, configuration data (knowledge) protection, and detecting forged physical or cyber-physical systems (anti-piracy protection) have to be considered. Many industrial sectors also have specific legal requirements in place for the logging or monitoring of experiments and events, e.g. to allow for accountability or provenance. With the transition to Industrie 4.0, it is also necessary to prevent big data analyses. For example, protocol data analysis might endanger employee data privacy or reveal a customer's secret production data to the equipment manufacturer. To master the requirements outlined, IT security in Industrie 4.0 must be considered holistically. Security requirements need to be viewed and guaranteed throughout the complete lifecycle of production systems and products. Cyber security concepts for CPPS in the I4.0 are required that addresses the various security and privacy risks at all abstraction levels. This includes different aspects, such as security blueprints, security-by-design and secure engineering of CPPS, trustworthy infrastructures and platform security, knowledge protection as well as usability and legal aspects. In particular security and privacy aspects must be preserved during the lifetime of smart manufacturing and smart products.

Next we discuss six important IT security challenges for Industrie 4.0 mentioned above, and examine possible approaches. We will focus on solutions for protecting CPPS platforms which are at core of smart production systems as enabler for Industrie 4.0.

A. Reference Designs and Blueprints

Medium-sized machine engineering and manufacturing industries play a fundamental role in Germany. However, small and medium-sized enterprises often lack the willingness or resources to grapple with the topic of IT security. For engine manufacturing companies, IT security is not a core issue; instead, it is a feature to be guaranteed, preferably in a simple and modular way.

Therefore, those industries desire a standardized approach to protect production within a manufacturing plant, the enterprise, and along cross-company value-added supply chains as well. The approach is to be based on a catalog of standardized measures and should ultimately be realized through technologies, IT products, and services compliant with that catalog. Reference models should describe standards and best practices to define which combinations of measures and security architectures make sense and how these may be combined across both units and enterprise boundaries while

ensuring IT security. Doing so should result in a suitable level of IT security reviewable by an external body through the application of metrics and measuring methods.

However, reality is still quite different from this ideal. Today's IT security is characterized by manufacturer-specific, insular solutions and selective protective measures. End-to-end security in a heterogeneous environment and across enterprise boundaries is an open challenge for research and development. Various standards do already exist, e.g. for encryption, secure communication, encryption key management, authentication and authorization, as well as security monitoring and incident response. But these concepts and solutions are frequently too complex for the use in production IT and vertical integration between business IT and production IT.

Several frameworks already exist that allow to implement manufacturer-independent, cross-company security. However, due to their high flexibility and expandability, these frameworks remain highly complex and too unspecific for the industrial use sought here. Thus, plant manufacturers and integrators also lack concrete specifications for realizing adequate security, both, during the design phase and in operation. An initial approach to the vision outlined above is provided by the industry-specific, informal guidelines (best practices), and obligatory standards for IT security.

B. Security-By-Design for Single and Combined Systems

Currently, engineers in I4.0 do not have a uniform methodology for considering the security and protection requirements of industrial systems during the early stages of system design. Thus, IT systems are often evaluated only after the functional design has been developed and are to be completed afterwards with security measures. This subsequent integration of security solutions often causes high efforts for rework, and hence, according to experience, comes with unnecessarily high costs both for manufacturers and operators.

Figure 3: Security Engineering Lifecycle

Particular challenges also exist regarding the testing of IT security solutions in an industrial environment. On the one hand, these solutions are supposed to protect complex systems against attacks; on the other hand, they have to meet high requirements regarding both, real-time and safety. Especially the latter cannot be tested easily: In order to check the solution's operational suitability, it must be tested under real life conditions and over the complete lifecycle (cf. Figure 3).

Until now, this has not been possible without taking some risk in regards to reliability and real-time requirements. Protecting Industrie 4.0 from downtimes and attacks necessitates taking IT security and privacy protection into consideration already during the design phase of intelligent production plants, processes, and services - throughout a system's complete lifecycle. Establishing test alternatives and significant reference numbers (metrics) seems to be a promising way to evaluate the attack protection of a system in a realistic way, minimize risks of failure, and encourage enterprises to invest in IT security.

In the IT world, appropriate methods and tools for secure software design, development, testing, and maintenance already exist. These methods and tools help to identify or even completely avoid vulnerabilities early on and over the complete product lifecycle. This knowledge has to be transferred from the IT world to that of production and automation. To do so, appropriate development standards and test tools are necessary which have to meet the specific requirements of the I4.0 production world. The existing standards for secure IT application development (e.g. ISO 27034 should be transferred to the industrial realm and linked to the safety standards. Domain-specific and cross-domain concepts exists also, and thus, Industrie 4.0 can build on a number of concepts from existing standards and previous work. Existing standards and concepts need assist to migration from Industrie 3.0 to Industry 4.0, e.g., IEC 62541, IEC 62443, etc. (cf. [32] for a list of relevant standards and norms in the industrial sector).

C. Reliable Infrastructures and Secure Identities

In the future, machine and equipment manufacturers will no longer distribute and sell only production equipment. For example, these manufacturers see a major part of their future profit growth in product related services in Industrie 4.0. In the ideal concept, the various companies form a virtual enterprise for a certain amount of time to offer services to a client. From a technical point of view this can only be reached through comprehensive network linking on different levels, which comes by the cost of numerous risks: At the equipment/machinery level, the increased interlinking provides attackers with multiple access opportunities.

Especially in regards to interconnected production and automation equipment, there are legitimate fears that attackers may be able to manipulate machinery or spy on production data without being detected. This combination of extreme flexibility and strong reliability in service-oriented industrial networks places a high demand on the security and trust.

Reconfigurable Hardware Platforms: Since many applications in the industrial field require real-time performance and flexibility, reconfigurable hardware become more and more attractive. Hardware platforms like e.g. Xilinx

Zynq SoC, next-generation Xilinx MPSoC Ultrascale+, or Microsemi SmartFusion2 provide a respectable security architecture, hardened cryptographic functionalities and protection mechanisms promising to counter those attacks [26, 27]. To enable agile functionalities and services on CPPS, enterprises will likely implement and activate software components or hardware functionalities (e. g. optimized IP cores in FPGA supported controls as service) dynamically.

Trusted Platforms and HSM: In general, security and trust architectures for IoT systems are common due to the broad range of underlying devices considered as embedded systems [30, 35]. Strong mutual trust is necessary for different partners to cooperate on those platforms. It is common sense, that a pure software security solutions cannot sufficiently protect the integrity of a secure system. In this context, the creation of secure elements (»trust anchors«) based on secure hardware are highly important, e.g., Trusted Platform Module, (Specialised) Hardware Security Moduls (HSM), and/or Trusted Execution Environments. Such trust-anchors are a necessary prerequisite to harden CPPS against attacks and to provide protection of the integrity of the software [1, 14, 19, 22, 28].

Respective concepts, for example in the context of *Trusted Computing*, have to be adapted accordingly to the requirements of I4.0. This will guarantee for the real-time capable end-to-end security and involved integrity checks of CPPS platforms and services. Intel and ARM provide several hardware security extensions architectures, which are widely available in industrial devices and mobile devices e.g, smartphones and tablets. With ARM TrustZone or Intel Software Guard Extensions (SGX) a range of software-defined/hardware-enforced security extensions are available for embedded systems. Under certain circumstances (e.g. availability of secure memory, secure boot, non-volatile monotonic counter, etc.), those extensions has the potential to serve as basis for separation mechanisms, trust and security provider and efficient verification of identities of machines, equipment, and services [9, 11, 22, 35].

Software/Run-time Layer Security: A CPPS - considered as integrated mixed-criticality system - is typically exposed to several attack vectors. At run-time level, software might be compromised by malicious code, memory attacks, malware insertion, configuration modification, hardware/software trojans, unintended IO sensor/actuator control, and denial-of-service attacks, etc. Thus, CPPS built in an environment which needs separation functionality for available machine functionalities and IT services. Other than monolithic kernel based operating systems, microkernel-based architectures allows separated application stacks with different safety and security levels to run on the same hardware (cf. Figure 4) in real-time.

Microkernel and Hypervisor solutions, e.g. Sysgo PikeOS, QNX Neutrino or Greenhills Integrity enabling safe, secure, and reliable CPPS requirements according to IEC 61508 up

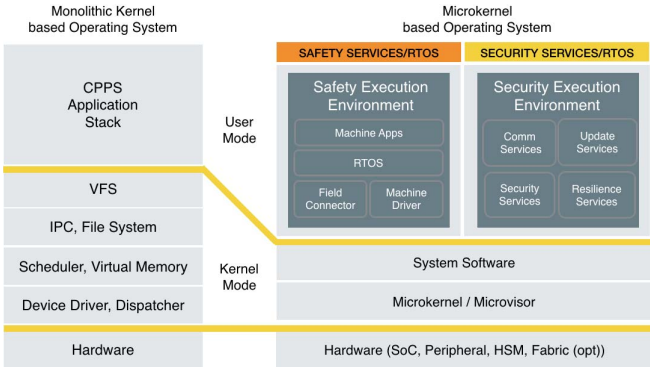

Figure 4: Monolithic/Microkernel-based Platform (CPPS)

to Safety Integrity Level 4 (SIL 4) and up to CC EAL 6+ High Robustness (also applicable in railway (CENELEC EN 50128), medical (IEC 60601), nuclear (IEC 61513), process control (IEC 61511), and automotive domain (ISO 26262)).

As example for such a platform, Figure 4 gives an abstract view on a generic CPPS research project consisting of a microkernel/microvisor-based security architecture. The architecture hold several platform services and functionalities for multilateral security and safety requirements. Here we concentrate on the security core services as follows:

Upgrade and Platform Management Services: In general, the complexity of a sophisticated CPPS makes a faultless condition difficult to reach. Therefore, identification and correction of identified errors and vulnerabilities through software/firmware updates at runtime are very important. It must be ensured, that neither an unauthorized update is carried out, nor an authorized update can be prevented. (Firmware) Over-the-Air upgrading allows a machine to update software components, machine apps or innovative software/hardware services. These modular and self-configuring units require a proactive security architecture that guarantees reliability and integrity as well as enables seamless-automated reconfigurations, platform management and updates at runtime.

Resilience Services: In view of the increasing complexity and threats, CPPS operators also need the option to monitor their IT infrastructures efficiently, and detect and ward off attacks, in terms of platform resilience. Thus, for the successful operation of industrial networks in Industrie 4.0, processes for both, intelligent monitoring and autonomous decision-making are required. For example, it would be fatal if an attacker was able to modify quality defining process parameters in self-regulating machinery without being detected, thus causing immense damage. Low-level device attacks often begin when an adversary modifies environmental parameters beyond specified operating ranges, temperature variation, voltage or clock glitching, JTAG debugging, etc. A self-monitoring module provides context awareness and self-calibration (sensing context), self-monitoring (status of

the CPPS platform and its components) and self-healing (fault diagnostics and response) and self-adaptation (contextual reconfiguration) or if CPPS platform state changes (e.g., component failure). Those run-time security protects against unwanted and adversarial activities and autonomous responses to potential attacks.

Security and Cryptographic Services: The service provides a software stack to the available HSM and cryptographic functionalities on which basis the platform verify integrity and protect sensitive information. Using reliable and efficient cryptographic mechanisms for protecting data from/to the CPPS has to be considered as a default standard and not as an exception. For this, the service provides a modular API to usage of available hardware accelerators or available cryptographic software engines, e.g. random generator, hash algorithms, symmetric/asymmetric primitives (AES, ECC, RSA, etc.), secure memory, monotonic counter, physical uncloneable functions), security application support (secure boot, integrity checks, etc.). It allows access to efficient cryptography primitives form a fundamental requirement for security-enhanced applications.

Communication Gateway Services: The high real-time requirements pose particular problems for efficient and effective safeguards. The communication service need to provide industrial protocol services and secure routing and gateway functionalities on the base of existing standards and extensions. The service requires multilevel and lateral security and the high requirements with respect to real-time and latency tolerances.

D. Knowledge Protection and Anti-Piracy Protection

The fast flow of information - also passing company boundaries - is of central importance in Industrie 4.0. Valuable knowledge present in smart products and documents must not be transferred and distributed carelessly, neither should process knowledge about production methods and systems. Therefor, in the future, enterprises will have to organize and manage their intellectual property in a fundamentally different way within the framework of federated data management. Here, the legitimate copyright holder's interests lie in thwarting plagiarism and theft or at least making it visible.

Through sensors and actuators as well as the increasingly flexible organization of production, new knowledge formats are being created in Industrie 4.0. Beside well-known designs and construction data, manufacturing data such as production parameters on programmable logic controller systems (PlC) or software/hardware configurations on dynamic production platforms (»Platform as a Service«) gain importance. Protocol data allow for drawing conclusions about design and construction data, hence are as worth being protected as these. On the other hand, protocol and processing data, in the sense of a product memory, may help to meet the legal burden of proof. However, these data need to be especially secured against manipulation and unauthorized access.

Embedding Copyright Protection: For manufacturing products, sensitive data are transferred to outside production systems, where they are often used by foreign CPPS and systems. This situation demands embedding methods and techniques for copyright and intellectual property protection of construction data and production parameters. Processes from digital photography, where meta information or watermarks are embedded into image files, may serve as models for this. To allow for the verification of the creatorship of digital data in a definite and court-proof manner tools from classic cryptography are well suited. These reliable mechanisms have to be adapted to service-oriented and interconnected production and control systems. Applied research has to develop processes that link information about the creator, copyright holder, version, and manufacturing process knowledge inextricably with the data. Security sensitive data and information should be uncoupled from machines and production systems, and should be made accessible upon necessity only.

Industrial Rights Management: In principle, information can be protected by safeguarding communication, encrypting data, and ensuring a selective reduction of information content. Additionally, I4.0 is in need of industrial rights management in combination with secure and trusted execution platforms where copyright holders' execution requests can be enforced. The platform need to provide proofs of production conditions (parameters) for a specific manufactured product, including which production standards and quality, and with which manufacturing tolerance the production process was conducted. Methods of enterprise or digital rights management, respectively, already being used might be adapted to fit Industrie 4.0.

E. Usability - The Human Factor

Various approaches to Industrie 4.0 already exist, such as lean production, collaborative engineering or via horizontal integration beyond the value added supply chain. Small and medium-sized enterprises frequently lack sufficient knowledge about potential threats, risks, and existing security solutions. This may cause new security incidents in the production sector. At the same time the reliable control and real-time execution of system critical functions must be guaranteed as a matter of principle, even in cross-linked and IT controlled flow processes. Software based protection and security controlling functions have to be executed reliably and in real-time, e.g. transmitting emergency commands to protect human life. Such emergency shut-off scenarios have to work also in Industrie 4.0, based on a near real-time capable linking-up via the internet or intranet, respectively.

This also has to be ensured in case of wireless signal transmission, or when triggered by mobile devices such as tablet computers. Industrie 4.0 will provide the factory work-

ers of the future with more interesting, flexible, and self-determined forms of working, but it will also place higher demands on the people, as the growing risks can only be mastered by trained personnel aware of security. Therefore, besides the respective basic training on IT security, concrete guidelines are required, describing how to securely install, configure, and periodically inspect the respective industrial plants and equipment.

F. Legal Certainty and Data Protection

Industrie 4.0 is designed mainly for distributed services in a connection of various associated providers. Besides the technological challenges of such platforms, the legal and judicial requirements have to be taken into consideration from the beginning [29]. If not, legal uncertainties and incalculable liability risks may severely interfere with the industrial development of Industrie 4.0 concepts and hence, their realization. Additional demands arise in Industrie 4.0 due to the unclear legal framework of conditions governing self-organizing and service-oriented production platforms. Compared to that of conventional, more rigidly organized industries, the legal certainty when using these platforms is distinctly less clear and by far more complex for both the customer and the producer.

III. Conclusion

Today IT security is already an important issue in the industry and a decisive factor for the success of Industrie 4.0. With the measures outlined here, it should be support to address the challenges posed by industrial IT security in a targeted manner and deal with current as well as approaching dangers effectively. In order to achieve this, classic IT and industrial production must grow together more closely. First steps are done with the establishment of several initiatives and projects, especially with national-fundend reference projects like IUNO [3]. However, the necessary national and international efforts being made should be increased and bundled, because innovation is more necessary than ever.

References

[1] S. Berger, R. Cáceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "vtpm: Virtualizing the trusted platform module," in *15th Conference on USENIX Security Symposium*, 2006.

[2] J. Beyerer, J. Jasperneite, and O. Sauer, "Industrie 4.0," *Automatisierungstechnik*, vol. 63, no. 10, pp. 751–752, 2015.

[3] Bundesministerium für Bildung und Forschung (BMBF), *IUNO - Nationales Referenzprojekt IT-Sicherheit in Industrie 4.0*, 2015. [Online]. Available: http://www.iuno-projekt.de

[4] ——, "Die neue Hightech-Strategie," 2014. [Online]. Available: http://www.hightech-strategie.de

[5] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *Industrial Informatics, IEEE Transactions on*, vol. 9, no. 1, pp. 277–293, Feb 2013.

[6] T. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, April 2011.

[7] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," in *Proceedings of the 23rd USENIX Security Symposium*, 2014, pp. 95–110.

[8] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan," in *26th Annual Computer Security Applications Conference, ACSAC*, 2010.

[9] J.-E. Ekberg, K. Kostiainen, and N. Asokan, "Trusted execution environments on mobile devices," in *ACM SIGSAC conference on Computer & communications security*, ser. CCS '13, 2013.

[10] European Commisson, *European Factories of the Future Research Association*. [Online]. Available: http://www.effra.eu

[11] A. Fitzek, F. Achleitner, J. Winter, and D. Hein, "The ANDIX research OS - ARM trustzone meets industrial control systems security," in *13th IEEE Int. Conference on Industrial Informatics, INDIN*, 2015.

[12] Fraunhofer Gesellschaft, "Industrial Dataspace," 2015. [Online]. Available: http://www.fraunhofer.de/de/forschungsfelder/industrial-data-space.html

[13] Fraunhofer IOSB-INA, *SmartFactroyOWL*. [Online]. Available: http://www.smartfactory-owl.de

[14] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A virtual machine-based platform for trusted computing," in *ACM SIGOPS Operating Systems Review*, 2003.

[15] T. Heer, O. G. Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[16] R. Johnson, "Survey of scada security challenges and potential attack vectors," in *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*, Nov 2010, pp. 1–5.

[17] H. Junker, "IT-Sicherheit für Industrie 4.0 und IoT," *Datenschutz und Datensicherheit*, vol. 39, pp. 647–651, 2015.

[18] Karlsruher Institut für Technologie (KIT), *Industrie 4.0 Collaboration Lab*. [Online]. Available: https://www.imi.kit.edu/2449.php

[19] M. Klimke, "Benefits and Values of the Trusted Platform Module," *Escar*, 2014.

[20] J. Krämer, M. Kasper, and J. Seifert, "The role of photons in cryptanalysis," in *19th Asia and South Pacific Design Automation Conference, ASP-DAC*, 2014, pp. 780–787.

[21] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security Privacy, IEEE*, vol. 9, no. 3, pp. 49–51, May 2011.

[22] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative instructions and software model for isolated execution," in *2. Workshop on Hardware and Architectural Support for Security and Privacy HASP*, 2013.

[23] B. Preneel, "Cryptography and information security in the post-snowden era," in *IEEE/ACM 1st Int. Workshop on Technical and Legal aspects of data Privacy and Security*, 2015.

[24] S. Tajik, D. Nedospasov, C. Helfmeier, J. Seifert, and C. Boit, "Emission analysis of hardware implementations," in *17th Euromicro Conference on Digital System Design*, 2014, pp. 528–534.

[25] Technische Universität Darmstadt, *Effiziente Fabrik 4.0*. [Online]. Available: http://www.effiziente-fabrik.tu-darmstadt.de

[26] S. Trimberger and J. Moore, "FPGA security: Motivations, features, and applications," *Proceedings of the IEEE*, vol. 102, no. 8, 2014.

[27] ——, "FPGA security: From features to capabilities to trusted systems," in *51st Annual Design Automation Conference, DAC*, 2014.

[28] Trusted Computing Group, "TPM 2.0 Library Specification Approved as an ISO/IEC International Standard," 2015.

[29] C. Tschohl, "Industrie 4.0 aus rechtlicher Perspektive," *Elektrotechnik und Informationstechnik*, vol. 131, no. 7, pp. 219–222, 2014.

[30] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for internet of things," in *2nd National Conference on Emerging Trends and Applications in Computer Science*, 2011, pp. 1–6.

[31] J. W. und Björn Conrad, "Industrie 4.0: Deutsche Technologie für Chinas industrielle Aufholjagd? Fahrplan für Industrie der Zukunft." MERICS, 2015.

[32] VDE Association for Electrical, Electronic & Information Technologies, *Normen und Standards im Bereich Industrie 4.0*. [Online]. Available: https://www.dke.de/de/std/Industrie40

[33] J. Viega and H. Thompson, "The state of embedded-device security (spoiler alert: It's bad)," *IEEE Security and Privacy*, 2012.

[34] M. Waidner, M. Kasper, T. Henkel, C. Rudolph, and O. Küch, *Eberbacher Gespräch zu "Sicherheit in der Industrie 4.0"*, SIT, 2013.

[35] Z. Yan-ling, P. Wei, and Z. Xin-guo, "Design and implementation of secure embedded systems based on trustzone," in *Embedded Software and Systems, 2008. ICESS '08. International Conference on*, 2008.