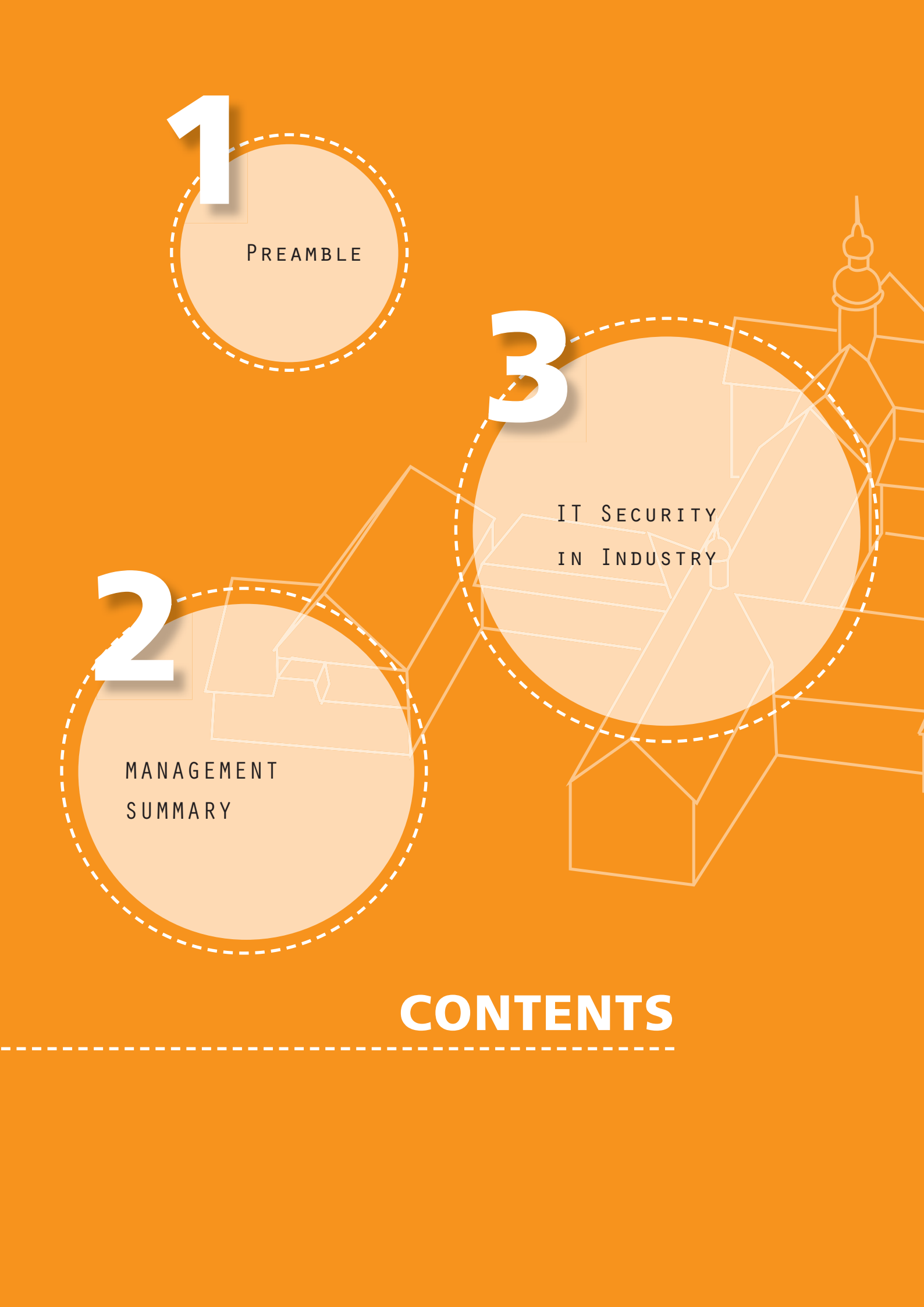
Fraunhofer SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

EBERBACH TALK ON »SECURITY IN INDUSTRIE 4.0«

07/2015

Eberbacher Gespräche



CONTENTS

4 Challenges and Solutions

5 Conclusion

1. PREAMBLE

Applied research on IT security requires dialogue between science and enterprise to obtain application relevant responses to fundamental questions, for example: What are the current challenges for IT security and privacy protection? What is to be expected in the future? What can and shall technology achieve? Where are the limits of what is technically feasible? Where are new ideas necessary?
The Fraunhofer SIT »Eberbach Talks« provide a forum for such a dialogue. Experts from commerce and administration as well as the scientific community meet at Kloster Eberbach in Rheingau for one day to work together in finding answers to these questions as they relate to specific topics. In October 2013, the topic was »Security in Industrie 4.0«. The participants were:

Prof. Dr.-Ing Reiner Anderl	Technische Universität Darmstadt
Klaus Bauer	TRUMPF Werkzeugmaschinen GmbH + Co. KG
Dr. Thomas Bornkessel	Rolls Royce Aeroengines Deutschland
Dr.-Ing. Thorsten Henkel	Fraunhofer SIT
Stefan Hoppe	OPC Europe
Holger Junker	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Michael Kasper	Fraunhofer SIT
Dr. Sven Kleiner	:em engineering methods AG
Dr. Ulf Lange	Bundesministerium für Bildung und Forschung (BMBF)
Dr. Thomas Rollmann	Miele & Cie. KG
Dr. Carsten Rudolph	Fraunhofer SIT
Dr. Harald Schöning	Software AG
Michael Voeth	Robert Bosch GmbH
Friedrich Vollmar	IBM Deutschland
Prof. Dr. Michael Waidner	Fraunhofer SIT / Technische Universität Darmstadt

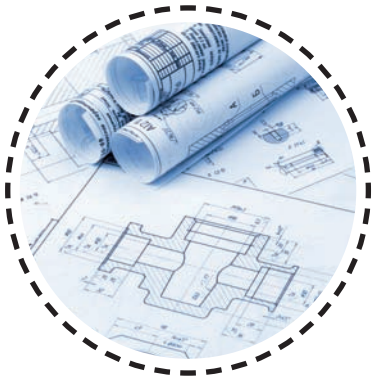
The results presented in this paper are supported by the participants but do not necessarily reflect the view of their respective employers.

2. MANAGEMENT SUMMARY

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, logisitics, 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. However, although many current IT security solutions can be applied in Industrie 4.0 context, they do not satisfy all requirements of processes in Industrie 4.0. Work needs to be done on underlying security mechanisms as well as on security architectures.

On October 1st 2013, the Fraunhofer Institute for Secure Information Technology hosted the Eberbach Workshop »Security in Industrie 4.0« to formulate guidelines and recommendations for a secure Industrie 4.0. Within the context of this workshop, representatives from the industry, research, and politics identified the most important practical challenges in the realm of IT security. Among these the following points are to be considered:

- Establishing adequate security throughout the entire machine and equipment lifecycles
- Creating a clear description of IT security in the industrial environment as well as a meaningful assessment of industrial IT security
- Connecting information technology security with functional safety and resolve dependencies
- Protecting industrial infrastructures and communication while considering real-time requirements and the dynamics and complexity of advanced cross-domain production processes
- Dealing with privacy, data protection, data security and legal requirements for services that can be international, cross-enterprise and involving different legislations

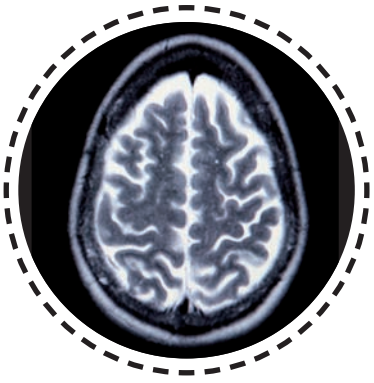


Reference Designs and Master Plans

»Security by Design« for Individual and Complete Systems

Reliable Infrastructures and Secure Indentities

Knowledge Protection, Anti-Piracy Protection and Verifiability



Usability – The Human Factor

Legal Certainty and Data Protection

2. MANAGEMENT SUMMARY

To address these key points, participants identified specific approaches applicable in six areas:

1. Reference Designs and Master Plans
Production engineers, integrators, and operators need specific recommendations for system planning and operation. Besides the need for baseline protection and minimum standards, modernizing today's plants requires a maturity model with which transition strategies can be developed and the necessary investment requirements reliably planned. Communication between IT experts and experts in production and automation requires to establish common terminology and systematics that can be used uniformly.

2. »Security by Design« for Individual and Complete Systems
IT security needs to be considered very early in planning and design phases. In order to support this concept of security by design, methods and tools meeting the industrial world's technological and organizational requirements must be developed. To evaluate and compare systems and component security, security metrics and clear evaluation criteria are also required.

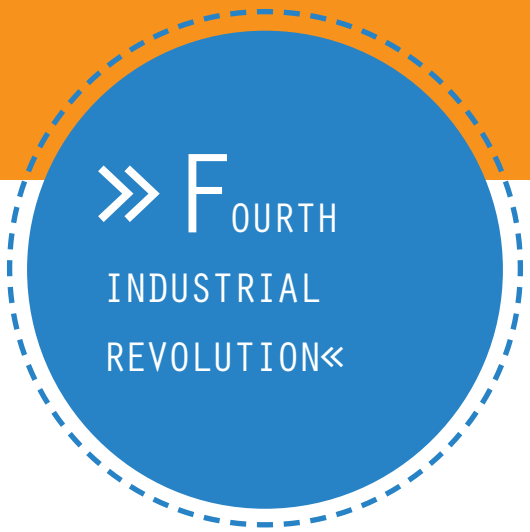
3. Reliable Infrastructures and Secure Identities
Industrie 4.0 processes rely on information and communication infrastructures. Therefore, reliability and resilience in Industrie 4.0 needs reliability and security of these infrastructures. In contrast to current IT networks, devices shall have secure identities and their system integrity needs to be protected. Work is required to design reference architectures of infrastructures that can provide end-to-end security. An essential part of such implementations are systems that constinuously monitorI identity and integrity of involved cyber-physical systems (CPS), automatically detect and reports anomalies, and establishes mechanisms to defend, recover and redress in case of attacks.

4. Knowledge Protection, Anti-Piracy Protection and Verifiability
Enterprises continuously develop new business models using new technology. However, distributed cross-enterprise processes increase the danger that property rights are violated. Therefore, mechanisms to effectively protect assets such as designs as well as manufacturing and production data are necessary. Verifiable security solutions for the protection of knowledge and property rights as well as the detection of piracy are required. These solutions must be verifiable by all relevant entities in the process.

5. Usability – The Human Factor
Usability in the context of IT security in Industrie 4.0 has several aspects. First, users should not be hindered by security technology, as this motivates the deactivation of security functionality and thus enables new attacks. It should be noted that attacks can cause physical damage or injuries. Another aspect is the usability of security technology itself. Processes such as management, security monitoring, installation or decommissioning need to be very efficient and user-friendly. Finally, social engineering and insider attacks need to be considered.

6. Legal Certainty and Data Protection
The decentralized organization of Industrie 4.0 poses new questions regarding liability and warranty issues that have to be answered to avoid the delay of the industrial innovation. Interdisciplinary work is required to develop foundations for legal certainty and data protection for decentralized and globally distributed processes in Industrie 4.0.

3. IT SECURITY IN INDUSTRY



Since the 1970s, we have been able to observe how classic production and automation engineering are consolidating with information technology. Machines, assembly lines and factories are being »digitalized«, meaning they are being augmented by IT elements such as storage, processors, software, and communication technology. After the year 2000, the Programmable Logic Controller-based machine control systems of the 20th century were replaced by »Cyber-Physical Systems« (CPS). Such systems are physical objects with embedded IT elements that are freely programmable and that are able to communicate with other CPS digitally.

Within one production plant CPS typically communicate via closed industrial data networks. However, more and more CPS can also be accessed via the Internet. This supports the integration and collective optimization of production and business processes and, at the same time, enables the outsourcing of production functionalities such as design and quality control to other locations, companies, or freelancers.

This Internet based integration of production IT and business IT allows the industry to partake in the further development of information technology directly.[1] This is how the IT megatrends mobile computing, cloud computing, and big data have become important drivers of innovation in industry. For example, cloud services are optimizing commodity flows and complex supply chains. Big data algorithms predict machine failures, thus reducing downtime and maintenance costs.

1 In this case, the term »business IT« refers to all information and communication technologies typically used in both business and private areas. Respective technologies in the productive realm, i.e. in factories, production plants, machines and their specific connective infrastructures, are termed »production IT« in this text.

STUMBLING BLOCKS IN THE PATH OF IMPLEMENTING INDUSTRIE 4.0 FROM THE ENTREPRENEURIAL PERSPECTIVE

Source: VDE-Trendreport 2013, http://www.vde.com/de/verband/pressecenter/pressemeldungen/fach-und-wirtschaftspresse/2013/seiten/34-2013.aspx (in German only)

43%

Missing Standards & Regulations

43%

High Qualification Demand

66%

Inadequate IT Security

31%

Large Investments

3. IT SECURITY IN INDUSTRY

There are other forseeable impacts of this integration: 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 in short.[2]

The industrial sector, for example automobile manufacturing and machine & plant engineering as well as automobile manufacturing, is of paramount importance for the German economy. Therefore, 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) to equal degree.[3] This is an appropriate cross-industrial approach to the issue and may prove to be the deciding factor in determining who leads the worldwide competition. 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«.

IT Security in Industrie 4.0: Old and New Challenges

Until today »security« in industry is almost synonymous with »operational safety«, meaning the protection of people, the environment, and equipment from the consequences of more or less random mistakes. Only through the vision of Industrie 4.0 and first upcoming IT-based attacks the idea of »security against attacks«, i. e. the protection against attacks by saboteurs, spies and organized crime, has entered the spotlight.

This systematic protection from attacks tends to run behind the implementation of IT itself and is usually accompanied by a delay – resulting in security gaps. The risk that such gaps may be exploited must be rated as very high, especially in the Industries. Industrial plants are always tempting targets for economically and politically motivated saboteurs and spies. The raising interconnectedness within and among businesses as well as the increasing complexity of processes both coming along with Industrie 4.0 enlarge the target surface, hence result in a further increase of risk.

2 Forschungsunion and Deutsche Akademie der Technikwissenschaften (acatech): Implementation recommendations for the future-oriented project Industrie 4.0; Berlin, April 2013; Online: http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf (in German only).

3 Web pages of the initiative »Plattform Industrie 4.0«: http://www.plattform-i40.de (in German only)

1. Infection with Malware via Internet and Intranet
2. Implanting Malware via Removable Media And external Hardware
3. Social Engineering
4. Human Misconduct and Sabotage
5. Intrusion via Remote Maintenance Access
6. Internet Linked Control Components
7. Technical Misconduct and Force Majeure
8. Compromised of Smartphones in the Production Environment
9. Compromised on Extranet and Cloud-Components
10. (D)DoS Attacks

THE TOP 10 THREATS OF INDUSTRIAL CONTROL SYSTEM SECURITY 2014

Source: BSI-CS 029 | Version 1.10 , 03.2014, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_005.pdf?__blob=publicationFile (in German only)

3. IT SECURITY IN INDUSTRY

The Eberbach Talk participants presume that 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 destroyed by a purely digital attack. 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 and the British secret service GCHQ have to spy on and manipulate IT systems. One can only deduce that other countries have similar spy programs.

Until now, IT security research and development focused predominantly on protecting business IT. In principle, the known concepts may be transferred to production IT as well. However the two worlds, however, 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 personnel, the environment, and equipment. Thus, confidentiality is considered subordinate; the primary objectives are integrity and availability.

Further differences result from, for example, the stricter real-time requirements in production; the potentially low memory and computing capacities of CPS and, from an IT standpoint, the exceptionally long lifecycles of industrial plants. 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 acustomer'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.

4. CHALLENGES AND SOLUTIONS

The Eberbach Talk participants identified six IT security challenges for Industrie 4.0 and discussed possible approaches.

4.1 REFERENCE DESIGNS AND MASTER PLANS

Medium-sized machine & plant installers and their customers 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 and their customers, IT security is not a core issue; instead, it is a feature to be guaranteed, preferably in a simple and modular way.

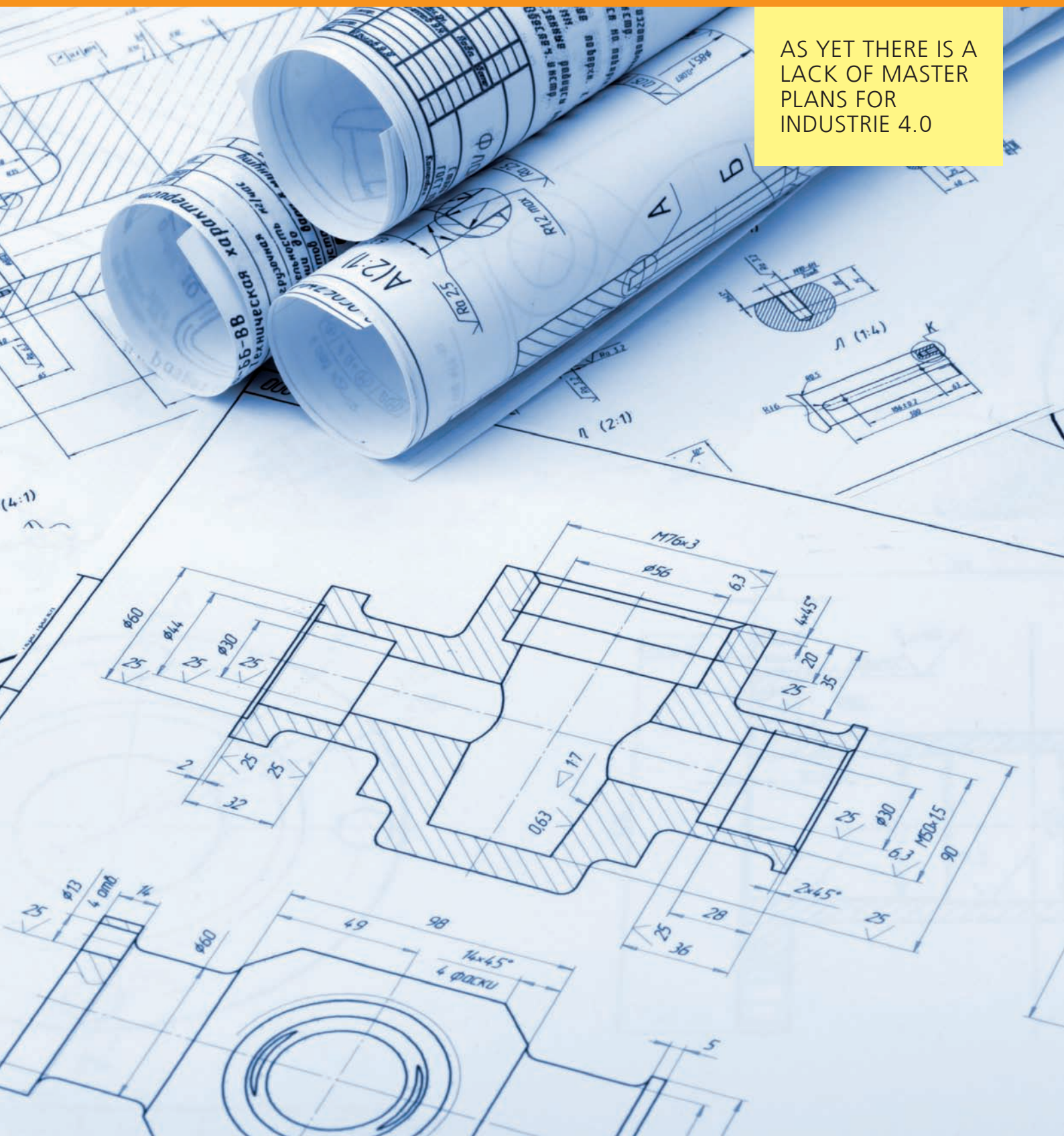
Therefore, this industry desires a standardized approach to protect production within a manufacturing plant, the enterprise, and along cross-company value-added supplychains as well. The approach is to be based on a catalog of standardized measures and should ultimately be realized through technologies, 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. If an enterprise uses this approach, it will be given a precise »master plan« with which it will predictably achieve the desired IT security level without necessitating its own IT security expertise.

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. However, these 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 such as webservices 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. According to the Eberbach Talk participants, this issue has not yet been sufficiently addressed by known Industrie 4.0 pilot projects.

A comprehensive solution to this problem requires a significant and long-term investment into research and development. However, a number of measures exists which can be realized on a near-term. These measures should be tackled urgently remains.

Guidelines, Minimum Standards and Maturity Models
An initial approach to the vision outlined above is provided by the industry-specific, informal guidelines (best practices), and obligatory minimum standards for IT security. In order to develop guidelines and minimum standards, specific characteristics and protection requirements have to be determined within an



AS YET THERE IS A LACK OF MASTER PLANS FOR INDUSTRIE 4.0

4. CHALLENGES AND SOLUTIONS

respective industrial sector, and based on these information, a threat and risk analysis has to be performed. Industry specific scenarios, examples, rules of conduct, and policies may be developed from the results. Within rather short-term research projects, the proposed guidelines and minimum standards should be realized as showcases and evaluated with regard to their costs and benefits. Based on the results collected from these projects, applying metrics and methods of measuring, multi-level maturity models can be generated. These models will allow, enterprises to both pursue the goal and schedule the transition from a low to a higher level of security over a period of time. In the medium term, this approach may contribute to formal IT security certification for industrial plants and plant components.

Best Practices for Developers, Manufacturers and Operators

While extensive public training material and best practice collections on many topics related to several forms of development are already available in the IT industry, there are hardly any specialized best practices for the industrial context or software development of industrial machinery, respectively. A multiplicity of parties is involved in an industrial environment. Thus, in addition to information and training material for industrial equipment software developers need best practices for equipment manufacturers are needed with regard to the conceptual design of production plants.

Manufacturer-Independent Security Models and Semantics

Due to its complexity, retracing an existing production environment including its IT security features is already a challenge. In principal, there is a need for industry independent semantics and respective IT security models. This is why machine manufacturers and operators are currently unable to present security features of machines, plants and processes in a standardized manner, i. e. without regard to the manufacturer/operator.

In the machine building industry, various approaches are known for modelling as well as formally describing automation and production environments. These approaches are to be combined with the respective IT security methods, which enables the relatively fast modelling of a cross-industry approach for designing industrial machines while including IT security. This approach will also facilitate the determination and description of equipment and services within the industrial context. The notation must be must be machine-interpretable so that other assessments can be made, based on the semantic models.

THE AUTOMATION PYRAMID

4. CHALLENGES AND SOLUTIONS

4.2 »SECURITY BY DESIGN« FOR SINGEL AND COMBINED SYSTEMS

Currently software developers do not have a uniform methodology for considering the security and protection requirements of industrial systems during the early stages of software 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 [4].

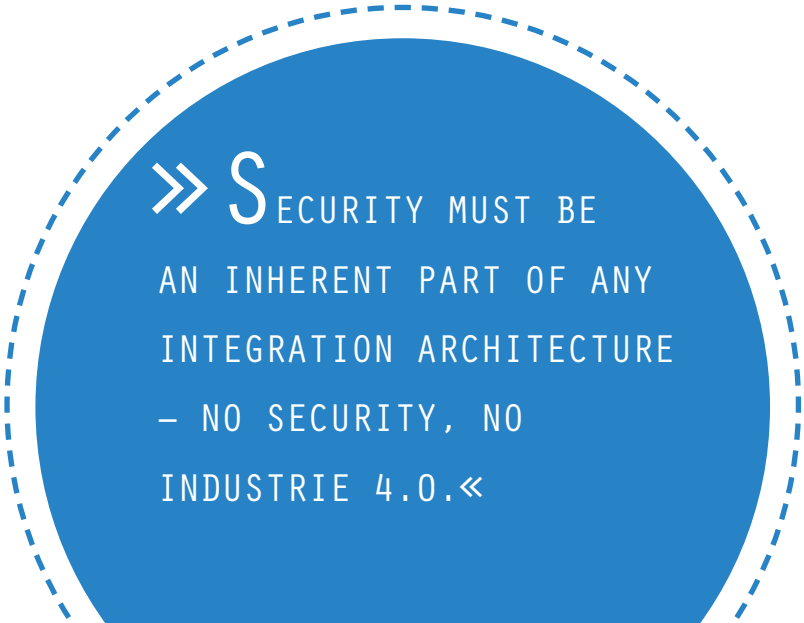
Particular challenges also exist regarding the testing of IT security solutions in an industrial environment. On the one hand, these solutions are supposed to protect complex systems against attacks; on the other, they have to meet high requirements regarding both real-time and safety. Especially the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

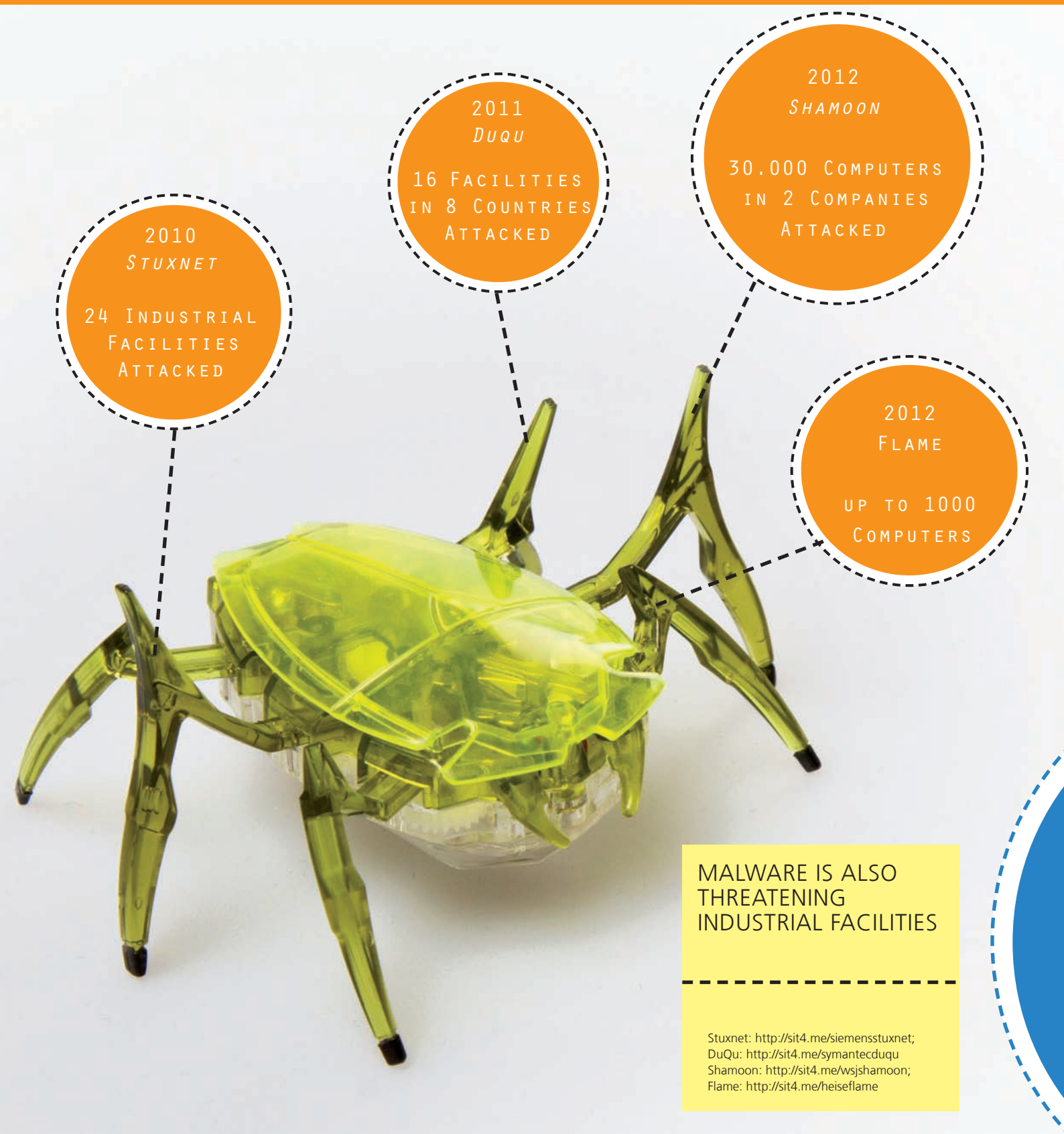
Secure Engineering

In the IT world, appropriate methods and tools for secure software development already exist. These methods and tools help to identify or even completely avoid vulnerabilities early on. 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 production world. The existing standards for secure IT application development (e.g. ISO 27034 / 27036) should be transferred to the industrial realm and linked to the safty standards.

To be able to support »security by design« with efficient test services, from the industrie's point of view, it is desireable to adapt testing tools to the industrial context where applicable. Considering this, techniques such as threat and risk analyses have to be adapted in such a manner that those responsible in the industries, who often do not have an IT background, are capable of assessing the results and applying the techniques efficiently. Furthermore, tools enabling an automated vulnerability analysis of both source code and industrial processes need to be developed. For example, there are currently hardly any tools available for the static code analysis of the programming languages and tools commonly used in the industry (e.g. Assembler, Scout, HIMA ElOP II SPS, CoDeSys, Step-7, or languages according to EN 61131-3).



4 Michael Waidner, Michael Backes, Jörn Müller-Quade (Hrsg.): Entwicklung sicherer Software durch Security by Design; SIT Technical Report, Fraunhofer Verlag, München, 2013; https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Trendbericht_Security_by_Design.pdf



MALWARE IS ALSO THREATENING INDUSTRIAL FACILITIES

Stuxnet: http://sit4.me/siemensstuxnet;
DuQu: http://sit4.me/symantecduqu
Shamoon: http://sit4.me/wsjshamoon;
Flame: http://sit4.me/heiseflame

4. CHALLENGES AND SOLUTIONS

Metrics
To make integrating IT security into industrial equipment and plants a profitable effort manufacturers must be able to advertise these innovative security features to the market. Therefore, in the short term, companies would like to have metrics to benchmark IT security features in equipment and components. Detailed information enables companies to compare the different products, giving manufacturers of secure products the opportunity to set themselves apart from less secure competitors. Operators and integrators, on the other hand, are in a better position to consider IT security features when selecting machinery.

Cross-Manufacturer and Cross-Industry Test Centers
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. Within this context, experiences in other business sectors show that offered solutions often do not yet provide the required level of IT security, or that their protection against attacks has not yet been proven by meaningful tests. This would damage the reputation of Industrie 4.0 sector and could cause enormous economic loss.

» INDUSTRIE 4.0 CAN ONLY BE REALIZED ALONGSIDE SUPPLY CHAINS, WHICH PRESUPPOSES RELIABLE AND DYNAMICALLY VERIFIABLE TRUST«

Currently no open testing centers exist furthering the systematic identification of security vulnerabilities in the overall complex of realistic industrial environments and evaluating potential risks (e. g. unintentional vulnerabilities, targeted spy software). Therefore, companies would like to have a test environment in which manufacturers and service providers can check their solutions modularly on an industry and manufacturer independent IT security platform. This would also enable reliable validation of new added value processes, software based services, CPS and associated IT security solutions on standardized operating platforms and reference architectures.

4.3 RELIABLE INFRASTRUCTURES AND SECURE IDENTITIES

Companies are already facing major challenges to protecting enterprise IT and production systems from intruders adequately. Patch management and complicated update processes hinder daily practices in industrial networks. In the ideal Industrie 4.0 concept, the various companies form a virtual enterprise for a certain amount of time. This virtual enterprise has flexible supply chains capable of adapting quickly to market changes. To achieve this, the partners have to interconnect various horizontal and vertical processes closely and in a trusted manner.

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 – e. g. with mobile end devices in radio networks. Within this context, it is particularly problematic that production systems in highly networked environments represent easy targets for attackers.

The network linking is also performed on the process level along value added supply chains, for example through connecting clouds. For example, to facilitate the establishment of virtual market places on which production activities can be offe-


4.0
13406
ERP

4. CHALLENGES AND SOLUTIONS

red as services, businesses have to trust virtual partners and their service qualities. This combination of extreme flexibility and strong reliability in service-oriented industrial networks places a high demand on the security and trust architecture.

In view of the increasing complexity and threats, plant operators also need the option to monitor their IT infrastructures efficiently, and detect and ward off attacks. This also involves integrity checks of machinery and plants. Efficient cryptography and lightweight primitives form the basis with which enterprisesmay verify integrity and protect sensitive information. The Eberbach Talk participants strongly recommend the encryption of all sensitive data. Using reliable and efficient cryptographic mechanisms for protecting data has to be considered as a default standard and not as an exception. The goal is to provide reliable encryption that is capable of running in real-time.

Modular Security Architecture

Strong mutual trust is necessary for different partners to cooperate. Reliable concepts HW/SW architectures, and standards in IT security can create such a basis for trust, but they also have to allow for cost-efficient adjustments in order to support flexible business processes and specialized developments. 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. To generate new functionalities, enterprises will implement and activate software components or hardware functionalities (e. g. optimized IP cores in FPGA supported controls) dynamically. Upgrading a machine with software components, machine apps or innovative software services creates a new type of function modules. These modular and self-configuring units require a proactive security architecture that guarantees reliability and integrity as well as enables automated reconfigurations and updates. In this context, the creation of secure and especially trusted elements (»trust anchors«) is highly important. They enable the quick and efficient verification of identities of machines, equipment, and services. Respective concepts, for example in the context of »trusted computing«, have to be adapted accordingly. This will guarantee for the required real-time capable end-to-end security.

Monitoring and Intrusion Detection

For the successful operation of industrial networks in Industrie 4.0 processes for both intelligent monitoring and autonomous decision-making are required. This is due to the fact that single companies as well as entire value added supply chains have to optimize and manage their processes almost in real-time. These strong real-time requirements place special demands on efficient and effective protection mechanisms. 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. To enable companies to monitor their production plants efficiently and detect and avert attacks, defense abilities have to be increased. For example, this can be provided by plant manufacturer-independent »intrusion detection« and »honeypots« designed specifically for the industry.

According to leading IT security experts, adjusting existing processes and technologies may suffice to realize the measures delineated. This still has to be proved in practice through applying them in reference architectures and pilot projects. Production companies will be willing to invest in cryptography based end-to-end security only when this stress test has been successfully passed.

KNOWLEDGE WORTH PROTECTING ACCRUES IN EVERY SECTION OF INDUSTRIE 4.0

Production Process

Manufactor-related Data

Fabrication Steps

Protocol Data

Production Interface

Product-related Data

Software Configuration

Production Structure

Design Data

Components

Drafts

Corporate Environment

Design Data

Production Parameters

Corporate Structure

Personal Data

Corporate Processes

Corporate Data

Production Processes

4. CHALLENGES AND SOLUTIONS

4.4 KNOWLEDGE PROTECTION, ANTI-PIRACY PROTECTION AND VERIFIABILITY

The fast flow of information - also passing company boundaries - is of central importance in Industrie 4.0. Valuable knowledge present in 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 already worth protecting, 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. Also during production data requiring protection are generated , typically coming as protocol data. On the one hand, protocol data allow for drawing conclusions about design and construction data, hence are as worth being protected as these. On the other hand, protocol data, in the sense of a product memory, may help to meet the legal burden of proof, for example in the pharmaceutical industry; however, these data will need to be especially secured against manipulation.

To achieve adequate knowledge protection, data security, and integrity industry and science have to jointly develop reliable methods and tools to protect digital product memory as well as platforms that allow for the protection of information throughout the entire value added supply chain and product life cycle.

Embedding Copyright Protection

For manufacturing products, sensitive data are transferred to outside production systems, where they are often used by foreign systems. This situation demands embedding methods and techniques for copyright protection of construction data and production parameters. Processes from digital photography, where meta information is 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 accessable upon necessity only.

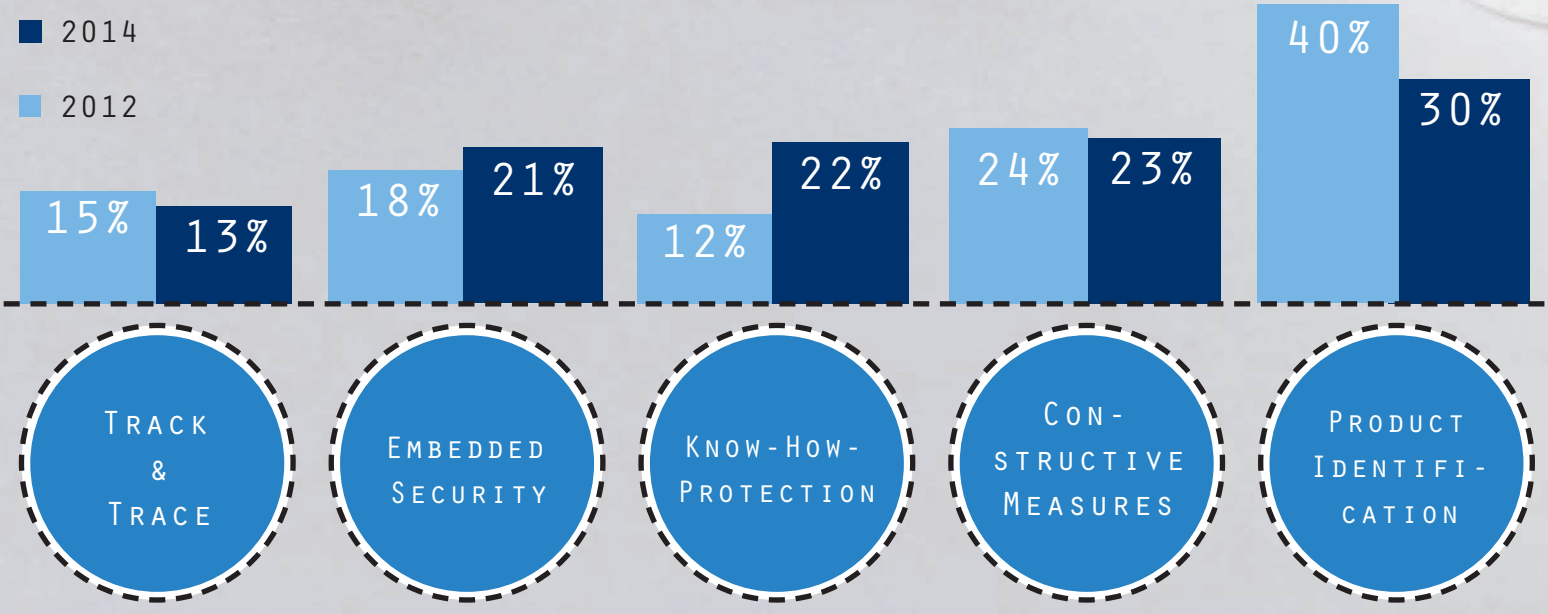
»INDUSTRIE 4.0 GENERATES NEW FORMS OF KNOWLEDGE THAT MUST BE PROTECTED LEGALLY AND TECHNOLOGICALLY.«

Industrial Rights Management

In principle, information can be protected by safeguarding communication, encrypting data, and ensuring a selective reduction of information content. Additionally, Industrie 4.0 is in need of industrial rights management as well as secure and trusted execution platforms

ORIGINAL OR FAKE?
WITH THE HELP OF WHICH TOOLS DO GERMAN PLANT CONSTRUCTION FIRMS PROTECT THEIR PRODUCTS?

VDMA, VDMA-Studie Produktpiraterie 2014, page 22



4. CHALLENGES AND SOLUTIONS

with which copyright holders' execution requests can be enforced. Amongst others, the following concerns have to be addressed: On which production system and under which production conditions (parameters) may a specific product be manufactured? With which production standards and quality, and with which manufacturing tolerance? Methods of enterprise or digital rights management, respectively, already being used have to be adapted to fit Industrie 4.0.

4.5 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. Especially small and medium-sized enterprises hope to profit from such new forms of production organization. However, they frequently lack sufficient knowledge about potential threats, risks, and existing security solutions. Lack of knowledge, limited security awareness, and false security assumptions may cause new security incidents in the production sector, and thus affect the wide acceptance and efficient realization of Industrie 4.0 concepts.

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 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 workers 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.

In the Future Manpower Will Be...

HOW IMPORTANT FOR FABRICATION WILL MANPOWER BE IN THE FUTURE?

Source: Produktionsarbeit der Zukunft, Fraunhofer Verlag 2013, page 50

4. CHALLENGES AND SOLUTIONS

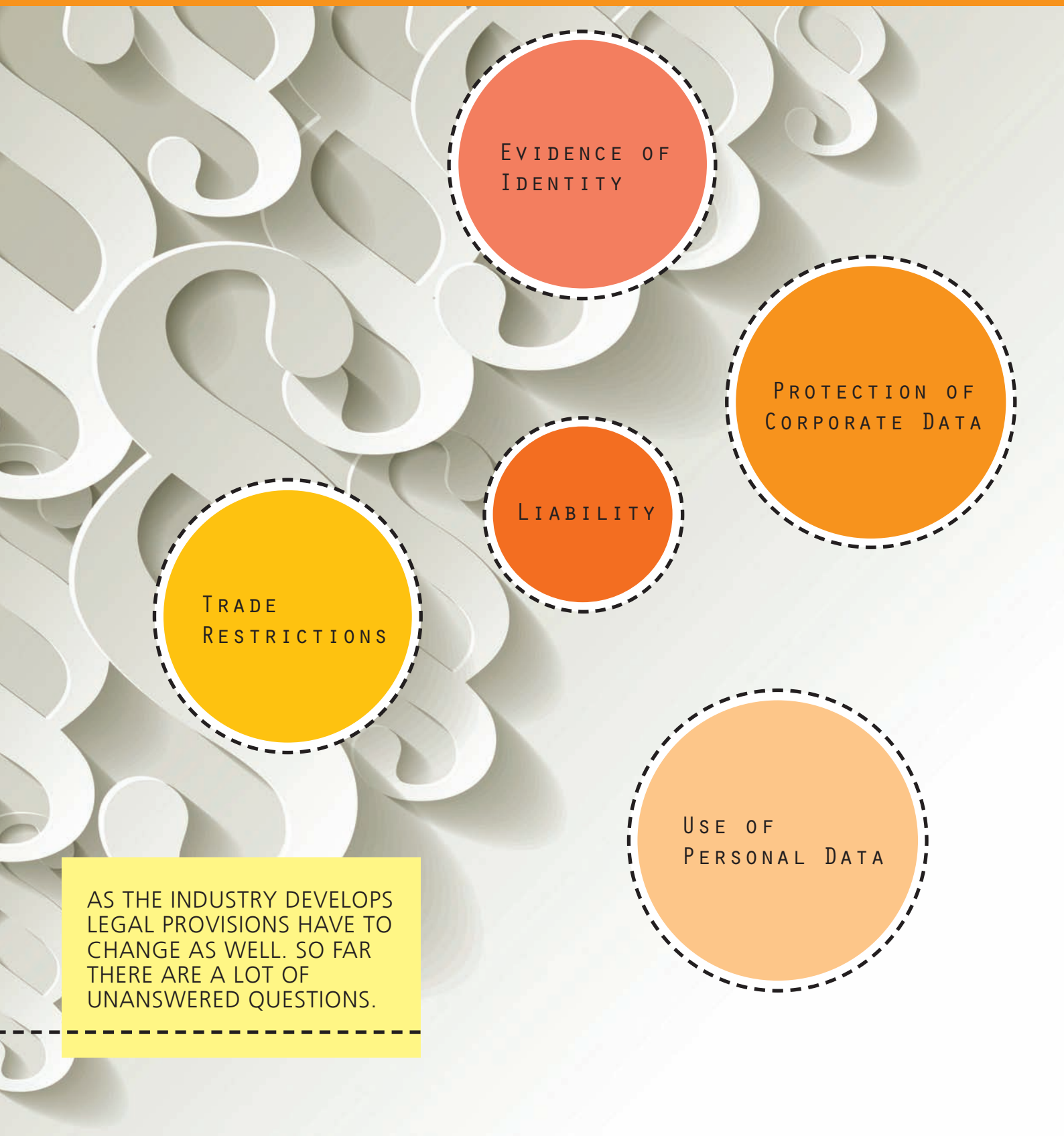
Beyond this, it may make sense to establish specific occupational careers that combine knowledge from mechanical engineering, IT security, and computer science.

The Eberbach Talk participants think that the enterprises have to arrange the industrial transformation process in a way appropriate to people. Human health and safety are the utmost priorities. To ensure this, user interfaces, access systems, and access protection systems have to be simple and comprehensible. For emergencies, alternative procedures need to be developed as well. To capitalize on the personnel's extensive experience and guarantee a high acceptance of the new organizational regulations, the staff should be actively involved when designing the company processes.

4.6 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 judical requirements have to be taken into consideration from the beginning. 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. Particularly in an international market it must be ensured that the partners involved really exist and are able to supply in the desired quality the deliverables offered, and also may be held liable. For decentralized production systems, this results in specific requirements of the partners' identity, the offered services' verifiability and effectivity, and the hedging of the contractual deliverables.



AS THE INDUSTRY DEVELOPS LEGAL PROVISIONS HAVE TO CHANGE AS WELL. SO FAR THERE ARE A LOT OF UNANSWERED QUESTIONS.

4. CHALLENGES AND SOLUTIONS

Especially data protection issues are problematic. The high data volume as well as heavy interaction and analysis (big data) between the involved parties introduces new challenges. This is as true for the protection of both business and production data as it is for personal data of both staff and customers. To minimize liability risks businesses do not only need the respective security technology; they also have to implement organizational measures that can only be developed within the context of legal certainty. Promoting the interaction of new technologies while facilitating individuals' information-related self-determination requires both the legal analysis and judicial designing of the industrial context. In Industrie 4.0, legal certainty is particularly important in facilitating the protection and guarantee of quality management in terms of company-spanning services.

This includes the following concerns: Does the partner really exist, and is he really who he claims to be? Who guarantees the reliability and quality of these new, highly dynamic services? Are the data submitted correct? Who is liable in the case of outage or errors? Who owns the rights to the data generated just within the production process? Which data are personal and, therefore, subject to privacy? These questions must be answered for companies to act reliably within their industries, both nationally and internationally.

5. 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 possible 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. The necessary efforts being made in Germany should be increased, because innovation is more necessary than ever. According to a KPMG study, several industrial companies are concerned about falling behind in international competition. Moreover, industries also lack employees able to understand and design the digitalization of production processes.

Businesses have adjusted their strategy accordingly: The study mentioned above remarks that the great openness to innovative breakthroughs in Germany is – at 77% – twice as high as that of foreign competitors. If the approaches detailed here are being elaborated and tackled, "Industrial Security made in Germany" can become an important sign of quality related to these innovations, and may contribute to ensuring the technical advance of German industry sustainably.

Editors
Michael Waidner
Michael Kasper
Thorsten Henkel
Carsten Rudolph
Oliver Küch

Editors' adress
Fraunhofer SIT
Public Relations
Rheinstrasse 75
64295 Darmstadt
Germany
Telephone +49 6151 869-282
Fax +49 6151 869-224
redaktion@sit.fraunhofer.de