PLATTFORM INDUSTRIE 4.0

Conference Report

Securing Global Industrial Value Networks – Synchronising International Approaches

May 14th to 15th, 2018

Content

Setting a milestone for a common security vision

At a time when digitalization and new industrial business models are rapidly changing value networks across sectors, companies and borders Industrial IT Security is high on a global agenda. Connectivity and data-exchange across borders have the potential to foster strong and sustainable growth for the global economy. At the same time companies initiating cross-company cooperation within international value networks are facing challenges like complex security mechanisms, differences in security infrastructure and varying national regulatory approaches.

The conference "Global Industrial Value Networks – Synchronizing International Approaches" marked an important milestone addressing these Industrie 4.0 security topics. It featured panels that expanded on issues of global relevance from the need for a trustworthy secure Industrie 4.0 ecosystem, to secure authentication schemes and secure communication technologies.

The exchange between partners at the conference contributed to more transparency on national objectives the various regulatory frameworks and related instruments. We very much appreciated to learn about frameworks and ideas from representatives from Japan, China, the U.S. as well as France and Italy and the EU.

We would like to use this opportunity to express our profound gratitude to all partner organizations, experts and supporters for their valuable input, ideas and drive – without you, our exchange would not have been so successful.

With the conclusion of the conference, the work has just started. We are looking forward to continually engage on these topics with our partners in the future.

1. Top-Level Summary

Steps towards a secure industrial ecosystem

> *"Security will be the enabler of Industrie 4.0 in the value creation networks."*
>
> Frank Lubnau, CDO Industry Robert Bosch GmbH

Industrial IT Security is a top priority on the global agenda of decision makers in politics as well as in companies. The common vision of the front runner of Industrie 4.0: establish a compatible legal, technical and organizational framework for a secure Industrie 4.0 ecosystem to enable new data-driven business models, and to ensure that data is securely stored, processed and transmitted within an international value chain network.

During the conference "Global Industrial Value Networks – Synchronizing International Approaches", more than 140 representatives of companies and political institutions from China, France, Italy, the EU, Japan and the U.S. came together for the first time to exchange various international views and increase transparency on national regulatory frameworks and related objectives and instruments.

The participants intensively discussed about next steps. The future I4.0 security ecosystem needs to establish a global infrastructure for trusted communication and cooperation in general among participating businesses. Security-by-Design has proved to be the superior principle for setting up secure ecosystems.

How industry and regulators can further contribute to foster this global security solution is described in the following key points for joint action.

1. It was agreed that international cooperation between the I4.0 initiatives and policymakers need to be established and strengthened with a view to creating compatible legal, technical and organizational framework conditions, which permit the cross-border sharing of sensitive data in a manner that supports business models.
2. One important area is the creation of an international infrastructure, which permits the cross-border authentication and authorization of communication partners like people, machines and software processes.
3. International standardization is an important element to establish compatible legal, technical and organizational framework conditions, particularly with regards to criteria and metrics for (automated) evaluation of the trustworthiness of partners and their products in the value.

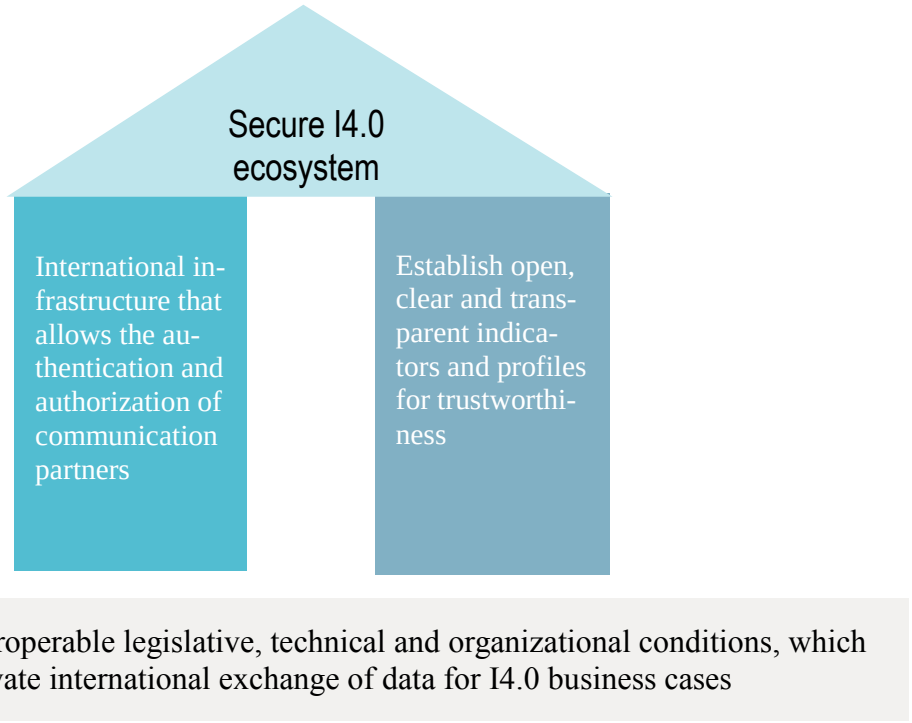

Figure 1: Preconditions for a secure I4.0 ecosystem

2. Motivation

As global networking increases, what is the best way to ensure IT security? Where companies engage in cooperation, what is the best way to determine whether the sender and recipient of the data really are who they claim to be (identity)? Are they actually authorized to send or receive the information (authenticity)? How can it be ensured that data is protected during transmission and cannot be manipulated (confidentiality, integrity)? Many questions, one answer:

An international approach is required

> *"Global industrial value creation networks require comprehensive security architectures for all participating parties (clients, manufacturers, service providers and suppliers), no matter what country they are in, as well as interoperability of security policies and recognized bodies and transparent structures for the assignment of user identities."*

Michael Jochem, Robert Bosch GmbH and chair of the Working Group "Security of networked systems" of Plattform Industrie 4.0.

Overall Goals

Against this background the goals of the conference were to create transparency, to reach a common understanding and to outline possible steps to achieve necessary international standardization and governance structures. On this basis the goals were:

- to ensure the interoperability of the different approaches,
- to show up the different regulatory views und projects,
- to develop a common understanding on the part of the international stakeholders as to how an Industrie 4.0 ecosystem could work, and
- to develop a trusting relationship between of the international I4.0 initiatives.

Objective of the conference

"Security is a basic precondition for value creation in industry, as this is increasingly based on digital networks. If the challenges are global, the solutions need to be global too. For this reason, we are looking to engage in international dialogue and are delighted that partners from China, France, Italy, Japan and the U.S. have accepted our invitation. In a first step, this conference aims to create transparency about national regulatory frameworks and the related objectives and instruments. We also wish to develop a common understanding amongst industry and policy-makers about the need for international solutions in order then to take the next steps together for global and globally compatible security solutions."

Prof. Dr. Ulrich Nussbaum, State Secretary at the Federal Ministry for Economic Affairs and Energy

Security as an enabler

Frank Lubnau, CDO Industry Robert Bosch GmbH, pointed out that Security will be the "enabler" of Industrie 4.0 in the value creation networks. A holistic approach should take into account the specifics of the domains, and it thus becomes a cross-sectional task. Security by design should become an overarching principle for development, deployment and operation.

"We are never done and have to consider continuous new requirements. Within Bosch, security is an essential aspect of the Bosch quality promise."

Frank Lubnau, CDO Industry Robert Bosch GmbH

EU providing the impetus

"The European Commission has good experience with harmonizing national regulations. Regarding digitization the scope of the European Commission is to foster the digital single market, and, hence, the evolution of digital industrial value chains across borders. Therefore, it has taken several measures like, e.g., the Commission's data package and EU cyber security act to make progress in this regard."

Dr. Roberto Viola, Director General for Communications Networks, Content and Technology, European Commission

The conference: starting a process

During the conference international top-level stakeholders and decision makers from industry, governments and regulatory bodies presented various approaches on how to cope with the challenges of securing global industrial value networks and the necessary international standardization. Overall nearly 150 participants from industries, government and science made the conference a fruitful starting point for the international exchange of ideas and approaches to ensure the interoperability of different concepts. This approach of combining the regulatory and the technical expert view was a complete success. Each segment of the stakeholder parties was able to gain insights into the positions of the others. That is an important step on the way to a functioning I40 environment.

3. International Business Case as Basis for the Discussion

Business Case – Networked Production

Our basic understanding is that security is not an end in itself. Security is one of the central enablers of new business models in connected industry. Due to the increased use of information and communication technology, in the next few years flexible value creation networks in Industrie 4.0 will progressively replace classical production chains with their largely hierarchical structures: business companies will offer free production capacity via a digital platform and thus increase the utilization of their own machine capacity. Other companies will take up the capacity, which is offered, and thus temporarily extend their own production facilities on a job-specific basis.

Especially for SMEs, such distributed production networks provide an opportunity to offer specific products and services on the market in an almost infinite quantity, competitively and in high quality. This concept is based on a situation in which all relevant departments of the business are digitally networked both internally and between companies.

The business case for such "order-based production" goes significantly beyond merely controlling and steering an order in the company's own production facilities. Instead, in Industrie 4.0 cooperation networks will be established between companies. This cooperation will be initiated in a fully automated way, which will also include the necessary vertical and horizontal networking of the production systems of the network partners.

A fundamental technical requirement for the implementation of such networks is that the communication chain must be **protected from unauthorized third-party interference**. Value creation networks will be successfully established and ready to operate when they are based on validated, verified and thus **secure identities**. Only then the communication partners can be unambiguously and reliably identified and the transmitted data validated.

In order to highlight this, the discussion of the various security aspects focused very specifically on an I4.0 business case for the distributed manufacture of shoes.

The German company Desma Schuhmaschinen GmbH supplies machines, automation solutions and moulds to footwear manufacturers worldwide. Since a couple of years, they have been taking advantage of digital manufacturing technologies and have – together with shoe brands – set up an order-controlled production process: with the use of an online configurator, customers design shoes according to their individual preferences and biometric properties. The production process starts on a digital platform when a customer places a new order. The order is forwarded to a producer who has the available capacities and meets the qualification requirements and price expectations of the shoe brand. For this purpose, the shoe brand transmits the production-relevant information (CAM data) directly to the production facilities – a robot or 3D printer. The producer starts producing the shoes.

The shoes are identifiable and traceable throughout the entire production process. A digital twin of the shoes contains all relevant data and information. The shoe brand is continuously updated on the status of the order and can check before delivery whether the shoes meet the quality requirements. After production, the shoes are delivered directly to the customer. All agreed documentation data (product memory) is automatically sent to the shoe brand.

This order-controlled production allows shoe brands to integrate external production modules next to their own shoe production facilities. They can flexibly expand their production capabilities and capacities and respond to changing market and customer requirements without tying up capital. At the same time, the producer of the shoe

increases its efficiency by offering its capabilities and free capacities on the market. In addition, new business models like flexible contract manufacturing are possible. The transition to the so-called platform economy and the conversion of B2B business into B2C are closely linked

Need of international interoperability of regulations and technical approaches

Cross-border cooperation between companies in particular highlights the **need for compatible national legal provisions**.

The first day of the conference focused on the tensions between different regulatory frameworks. Dr. Ulrich Nussbaum, State Secretary in the Economic Affairs Ministry, opened the conference by providing insights into the policy framework in Germany. High-level representatives of the European Union and from ministries, regulatory authorities and industrial initiatives from China, Germany, France, Italy, Japan and the U.S. sketched out their approaches and identified areas where alignment is possible.

On the second day, the experts discussed technical aspects of security in four sessions. The dialogue was structured around questions of (1) a cross-border security architecture for value creation networks, (2) conditions for secure communication, (3) secure identities and (4) the evaluation of trustworthiness. Plattform Industrie 4.0 offered its concepts in the four areas to provide a basis for discussion. The four issues have been selected to provide a framework for this international discussion.

The concepts of Plattform Industrie 4.0 can serve as an impetus for the international expert community and do not claim to be complete; on the contrary, they should be supplemented or challenged by the conference participants.

Contribution towards the "transparency" objective

For the first time, the contributions by the I4.0 organizations from China, Japan, the U.S., France and Italy provided an overview of different international views and approaches from the point of view of both industry and government. The conference showed clearly that there is a desire to develop common solutions: the presence of numerous government representatives, including from Japan and China, highlighted the relevance of this issue.

A comparison of the substantive approaches to secure I4.0 ecosystems, secure identities, secure communication and trustworthiness shows that the initiatives are not far apart from one another on many of the issues. The participants took a positive view of the technical concepts of Plattform Industrie 4.0.

4. Challenges and Findings

In addition to comparing the concepts developed by Plattform Industrie 4.0 with the solutions of the international partners with a view to creating transparency, the conference also aimed to develop a common understanding of the need for internationally interoperable solutions and to identify the need for action in terms of standardization and policymaking.

The business case (Figure 1) was intended to help developing this common international understanding of the networked production as described above. The challenges imposed by the a necessary I4.0 ecosystem are shown very realistically.

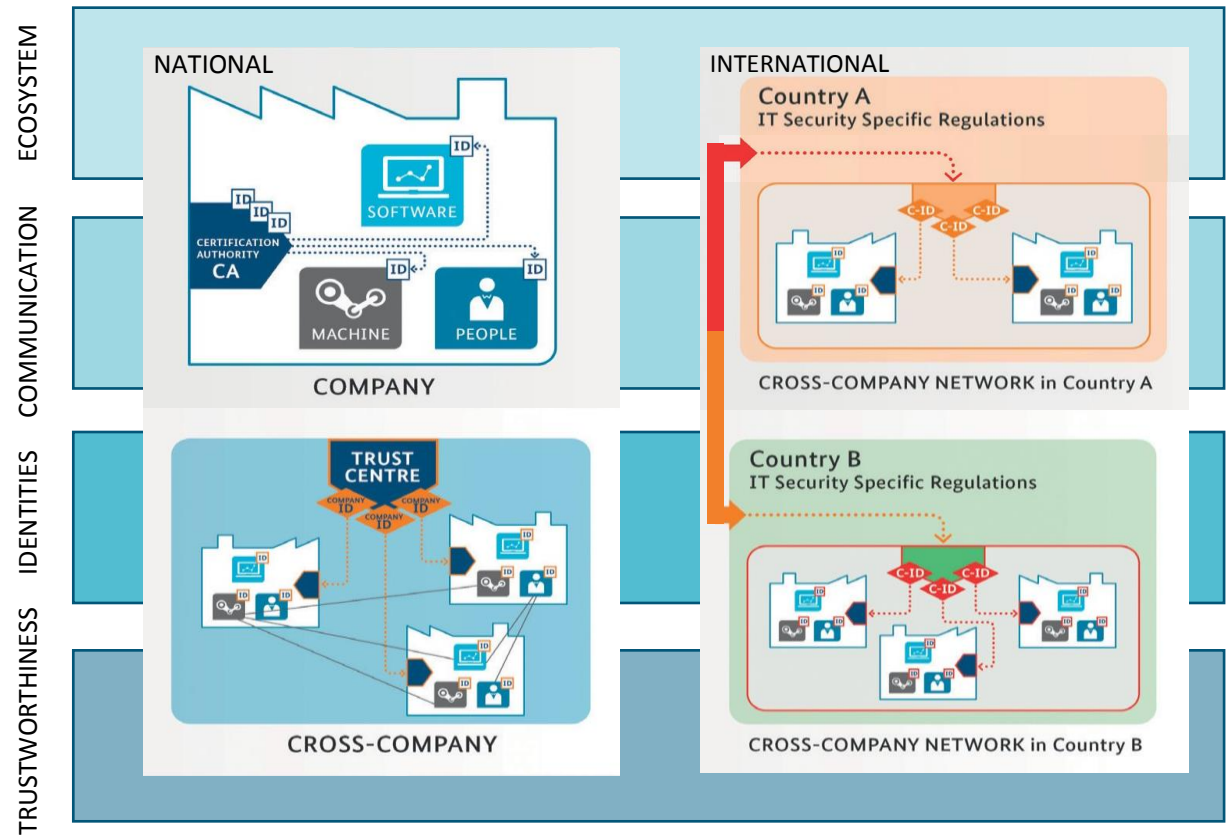

Figure 2: Overall business case of I4.0 production

Challenges and need for action

The future I4.0 security ecosystem needs to establish a global infrastructure for trusted communication and cooperation in general among participating parties as indicated in Figure 1. This infrastructure needs to support certificates for various purposes:

- Managing and/or providing secure identities which can support authentication at different identification levels for companies, personnel, machines, software and devices, as far as necessary for the support of automated cooperation for business and manufacturing.
- Establishing secure communication channels between different companies in different parts of the world.
- Managing and (perhaps) providing certificates which certify implemented
- security levels regarding processes and devices of participating companies.
- Supporting different trustworthiness levels depending on the requirements of projects and business cases.
- Providing robust, secure, and trustworthy processes for JOIN and LEAVE of global I4.0 participants.
- Facilitating secure and trustworthy participation and migration to I40 especially for small and medium enterprises which have yet to establish secure operations with external partners.
- Supporting continuous security and trustworthiness across value networks and supply chains

Harmonized and standardized policies are indispensable for the support of international and global value networks. Stakeholders operating on a global scale need to be able to act independent of the location of specific sites and premises.

I4.0 in an overview perspective – the panel discussions

Panel 1: Identifying security challenges along the industrial value chain

During the first panel, representatives from the industrial sector and Industrie 4.0 initiatives all over the world discussed the need for cybersecurity and trustworthiness for global industrial value networks. Moreover, they identified security requirements at different stages of the value network and across national borders and described security challenges and possible approaches from their point of view. They focused on the security challenges for implementing global industrial value networks and which technical, organizational, sociological and regulatory obstacles need to be tackled in order to realize I4.0. Finally, they addressed the norms and standardization requirements they see and the issues which should be at the centre of future cooperation of the Industrie 4.0 initiatives.

- *Takashi Amano, General Manager, Cyber Security Center, Toshiba Corporation // Robot Revolution Initiative*
- *Jean-Michel Brun, Chief Security Architect Schneider Electric*
- *Michael Jochem, Director Innovation Cluster Connected Industry - Robert Bosch GmbH // Chair of working group "Security of networked systems", Plattform Industrie 4.0*
- *Zhuo Peng, Senior Information Security Expert, Sany Heavy Industry Co.,*
- *Yuri Rassega, Chief Information Security Officer (CISO) at Enel*
- *Thomas Walloschke, Director Security Strategy, Fujitsu Technology Solutions // Steering Board Member and WG11 Chairman Alliance for Internet of Things Innovation (AIOTI)*

Common understanding of key messages

- Security-by-Design has to be established as a leading principle for both the physical asset and its digital twin
- International standards regarding common security policies, categories and measurements of trustworthiness, processes to determine (automatically) the trustworthiness of potential business partners and a secure I4.0 ecosystem must be elaborated.
- International discussions of the approaches and the elaboration of requirements on these topics should be the starting point.
- Governments need to support global I4.0 production via harmonized regulations and powerful digital infrastructures.

Panel 2: Policy approaches: How do authorities respond to the challenges of industrial internet security?

Industrie 4.0 creates new challenges for cybersecurity. In the second panel, representatives of the national security agencies from China, Japan, France, the U.S., Germany and the EU shed light on their tasks ahead and discussed the need for regulation regarding cybersecurity for global industrial value networks. They focused on different approaches ranging from legal requirements to voluntary initiatives. Additionally, they discussed their responsibilities to guarantee a trustworthy international exchange to enable compatibility across borders. For the first time, the contributions by the I4.0 organizations from China, France, Italy, Japan and the U.S. provided an overview of different international views, objectives and approaches from the point of view of both industry and government.

- *Dr. Demosthenes Ikonomou, Head of Operational Security, European Union Agency for Network and Information Security (ENISA)*
- *Koji Nakao, Distinguished Researcher and advisor cyber security, National Institute of Information and Communications Technology (NICT) / National Center of Incident Readiness and Strategy for Cybersecurity (NISC)*
- *Sandro Mari, Technical Officer High Institute of Communications and Information Technologies (ISCOM), Technical Coordinator of the Italian National CERT (Computer Emergency Response Team)*
- *Arne Schönbohm, President German Federal Office for Information Security (BSI)*
- *Matthew Scholl, Division Chief Computer Security, National Institute of Standards and Technology (NIST)*

Key findings / common understanding:

- It was clearly seen that there is a desire to develop common solutions: not least, the presence of numerous government representatives, including from Japan and China, highlighted the relevance of this issue. Everyone was interested in identifying interfaces for an international alignment of the regulatory framework and highlighting the aspect of standardization.
- There was agreement that IT security guidelines are needed, which at least cover basic requirements, but also should cover additional requirements.
- Here, a common understanding is needed of what components should be covered by the guidelines. It may be the case that sector-based approaches are required.
- There are signs of a development which starts with guidelines at national level, followed by self-checks to examine the robustness of the guidelines, with a view to ultimately producing international guidelines.
- In this context, certification and standards play a major role in terms of the measures to be taken; it is therefore necessary to review existing frameworks, bodies and standards.

Toshikazu Okuya, Japanese Ministry of Economy, Trade and Industry

Outlook Speech: Japanese "Cyber/Physical Security Framework"

The presentation gave insight into current threats of the emerging cyber/physical world and provided an outlook on how the Japanese "Cyber/Physical Security Framework" aims to support the manufacturing sector to address this challenge.

The presenters emphasized that cyber and physical spaces in our future society will be highly integrated. Products, services and data will be connected to each other and supply chains will transform from linear into non-linear forms. Cyber threats will also expand under this structural change. Threats arise from malware such as the famous „WannaCry"-attack, as well as from undocumented functions in physical components. While such cyberattacks focused on IT-Systems in the past, they are shifting more and more to industrial sights with potentially fatal consequences such as the Ukraine power outage in 2016.

To meet this challenge the introduced framework aims to articulate risks and let organizations manage them as well as increase the competitiveness of products & services through increased security.

Within the framework, a new non-linear supply chain is defined as a "Value Creation Process". To clarify the risks in this process, the process will be structured by three layers (cyber space, cyber/physical space and the conventional "supply chain") and six elements (organization, people, component, data, procedure, system) of the process. The emerging matrix allows to identify potentials risks and to develop fitting and sophisticated countermeasures.

To run the framework in an altered value creation process, trust of the value creation partners is essential. Therefore, the presenter suggested to create equipment and services that meet high security standards and to confirm for existing equipment and services that they meet required standards. To confirm trust, the presenter suggested to create and manage a trust list through which anyone can check, whether a specific product was produced according to standards or not. Further on, it was proposed to build and maintain a trust chain by structuring networks of trust lists as well as the detection and prevention of attacks against the trust chain.

Panel 3: Security as an enabler of global smart manufacturing

Panellists discussed how existing international approaches can be synchronized to enable and support the establishment of new industrial value networks. In a global value creation network trust in the partners is mandatory. In this discussion company and government representatives considered different possibilities and responsibilities to ensure trust, verify identities and protect intellectual property. The panel discussion was focused on measures which need to be taken to ensure an equal level of trust across borders to assess whether the different approaches taken by ministries are compatible. The panel was in complete agreement that identities are the starting point for communication in Industrie 4.0 and that the confidentiality of data is an important aspect worthy of protection.

- *Jean-Michel Brun, Chief Security Architect Schneider Electric*
- *Dr. Demosthenes Ikonomou, Head of Operational Security, European Union Agency for Network and Information Security (ENISA)*
- *Michael Jochem, Business Chief Digital Office - Industrial Technology, Robert Bosch // chair* of *Plattform Industrie 4.0's working group on the security of networked systems,*
- *Koji Nakao, Distinguished Researcher and advisor cyber security, National Institute of Information and Communications Technology (NICT) / National Center of Incident readiness and Strategy for Cybersecurity (NISC)*
- *Matthew Scholl, Division Chief Computer Security, National Institute of Standards and Technology (NIST)*

Common understanding of key messages

- Internationally verifiable identities have to be established as the starting point of trustworthiness.
- Intellectual property has to be protected when it is exchanged for production purposes.
- Regional regulations need to support international value creation.

5. Deep Dive into Four Key Issues

The Plattform Industrie 4.0 working group "Security of networked systems" has identified four key issues concerning the security in global industrial value networks: (1) a secure ecosystem, (2) secure communication, (3) secure identities and (4) trustworthiness. The working group also derived hypotheses on how these issues could be addressed in global standardization and governance as well as technical concepts to deal with these issues.

Secure ecosystem

Use case

The shoe brand and the end customer (buyer of the shoes) might be located in different countries than the producer of the shoe. First, producer and supplier need to set up a framework between the two companies to ensure interoperable security policies. Apart from this, both must ensure they meet national requirements by – for example – obtaining certificates. Ideally a common regulatory framework will have been set up so they do not need to invest resources in applying for additional certificates accepted by both partners.

Overall requirements for a secure ecosystem:

- Establish Security-by-Design as an overarching principle
- Guarantee security for the physical asset and the digital twin
- Establish trust centre which cooperate internationally on the cross-border authentication of communication partners

Draw up interoperable regulatory frameworks for the countries of origin of the partners in the value creation networks

Challenge

Global value networks require comprehensive security architectures covering all participants, no matter which country they are located in. Integrity of products, processes and machines must be assured across these value networks and during the whole lifecycle.

Thesis

Crossing borders requires a governance structure recognized by all participants, interoperable security policies and a common regulatory framework that allows interaction to the extent necessary.

Co-Speaker Dr. Evangelos Gazis, Huawei

Suggested technical concept

Security-by-Design has proved to be the superior principle for setting up secure ecosystems. Subsequent supplements to fix security of a system are not constructive and sufficient. More and more, security measures will be integrated within the industrial applications itself rather than just within the network layers and will support end-to-end security. Security-by-Design must also cover the digital twin: security for the physical instance, its digital twin and their interactions must take place in a concerted way to ensure a comprehensive security level for the whole system.

The secure transfer of data between, for example, two machines across borders needs Certification authorities or trust centres in each country. The trust centres function as trusted instances and subscript certificates in security domains. Award and withdrawal of permissions must be under the control of the respective domain. Standards and processes for the trusted coupling of certification authorities of the respective security domains are necessary. For this to work abroad, the trust centres need to have contracts with each other to create the prerequisites for a secure communication to meet national requirements. There are no fitting templates yet. Concepts and implementations could be based on contracts between companies operating the national infrastructures.

"The discussion revealed agreement about the need for Security-by-Design as a general principle for shaping and implementing cybersecurity. The availability of high-quality and standardized security architectures is regarded as a precondition and enabler for Industrie 4.0.

A global and trustworthy security infrastructure is required in order to enable efficient international cooperation in the I4.0 context. This infrastructure needs to support the trustworthiness of value chains and permits security both for the digital model and for the physical realization of production over the entire industrial lifecycles.

Plattform Industrie 4.0 has been engaged in successful cooperation with Japan's Robot Revolution Initiative for several years. Resulting from this cooperation, a position paper was presented which underlines the principles of Security-by-Design and trustworthiness of value chains and announces further joint work on global standards for achieving these security objectives."

Dr. Wolfgang Klasen, Siemens AG, and chair of the "Standards" subworking group of Industrie 4.0 Security

Secure communication

Use case

To achieve order-controlled production in lot size 1, essential data is provided "just-in-time" from a decentralized source, rather than being stored in centralized systems for long periods in advance. When the producer is receiving the shoe order from the shoe brand, the costumers' personal data for the shoe production is exchanged in real time. The owner of the shoe brand and producer can set up user and identity management (authentication and authorization) to ensure secure communication. Furthermore, they should use data encryption and signatures.

Challenge

Secure communication in an international multi-company value chain needs to consider and synchronize security requirements of all stakeholders.

Thesis

The exchange of data across company boundaries requires interoperable security policies and a recognized body and a transparent governance structure for the allocation of identities.

Special requirements for secure communications:

- Set up a standardized classification of information in line with the protection goals
- Ensure that all parties involved in the value creation network have standardized interoperable security policies

Co-Speaker - Dr. Takeshi Yoneda, Mitsubishi Electric // Robot Revolution Initiative

Suggested technical concept

Authenticity and trustworthiness of the communication peers must be evaluated automatically in the autonomous interactions by the trust centre. Both the confidentiality of information and at the same time the inspection and control of communication must be considered.

Hence, this concept has to take into account the requirements of the different stakeholders. A communication of an internal asset to an external peer may include confidential data for which end-to-end encryption might be favourable. At the same time the operator of the asset has to ensure the proper operation of its systems and therefore wishes to inspect all communication with his networks or with external entities.

In any case both parties wish to maintain the integrity and authenticity of the communication. Today's protocols need to be amended to support these requirements.

The secure exchange of data between companies and across borders requires interoperable security strategies and transparent structures to assign identities.

This makes it possible to verify the authenticity, integrity and trustworthiness of communication partners. Attention needs to be paid both to the confidentiality of the information and the verification of the communication.

"Secure communication is key to the successful implementation of Industrie 4.0. Communication links several stakeholders and their respective security requirements. Secure communication imposes demands on secure identities and the consideration of the trustworthiness of the communication partners. These issues are thus closely interrelated and require a holistic solution with a common understanding of the classification of information and security policies.

Integrity and authenticity are the basis for every trustworthy exchange of information. Confidentiality is a particular challenge, particularly in communications involving more than one company. In some ways, it conflicts with needs to control the flow of information, as access to transferred data is needed to detect attacks or harmful software.

Secure communication requires standards supported by all stakeholders. These standards need to be coordinated at international level in order to involve the globally active partners in value creation."

Dr. Lutz Jänicke, Phoenix Contact GmbH & Co. KG and chair of the "Secure Communication for Industrie 4.0" subworking group

Secure identities

Use case

For the secure production of shoes, all parts of the production line (robots, 3D printers) and persons must be equipped with a secure identity within the producer. This reduces the risk of third-party access to the production facilities via identity theft. In addition, secure identity management by a certification authority helps the shoe producer to be considered trustworthy by prospective clients.

Challenge

If people, machines and software speak with each other, they must know who they are talking to. The interactors of Industrie 4.0 must be provided with identities.

Thesis

In Industrie 4.0 the entities must be provided with secure identities. Within each company, a certification authority service is required to supply these identities with the necessary trust.

Special requirements for secure identities:

- Every entity involved in the communication (person, machine, product, software) of a company must have at least one secure identity.
- Secure identities must be issued within a company by a trusted authority.
- In case of machine-entities, secure identities must be inseparably bound to the entities itself.

Co-Speaker Jean-Michel Brun, Schneider Electric // Industrie du Future

Suggested technical concept

A global definition of staged and standardized security levels and a common understanding of and stakeholder agreement on digital identities are needed as preconditions for secure communication in and between companies in I4.0. The international standard IEC 62443 describes some basic definitions of identities (ID), unique identities (UID) and secure identities (SID). This can be used as a guideline for the worldwide collective migration process from I3.x to I4.0 along the value network.

For the secure identity level, a trusted authority is needed to create, issue, manage and monitor SIDs, which would be based on certificates, distributed to machines, persons and software processes. A trusted authority (CA) is required to manage the identities of all entities in a security domain. From today's perspective, a public key infrastructure (PKI) appears as a possible solution[1].

For the processing on the bases of secure identities between companies/security domains, the mutual recognition of the entities and the setting of a commonly agreed security level is prerequisite.

For entities with a long-term service life, such as cyber-physical production systems (CPPS), crypto-agility and post-quantum cryptography (PQC) is needed.

[1] Additional remark: The European Commission's eIDAS Regulation EC/910/2014 has provided rules on how to become a certified trust services provider for a certain period in Europe. Also, the definition of the EU Trust Mark offers authorities, companies and citizens the possibility to have this trust services provider vetted by an authority in terms of its security. The validity of the EU Trust Mark is limited to 12 months. After this time, a re-assessment is required. More than 50 trust service providers are currently registered in Europe and can issue, among other things, certificates for identities, electronic seals and electronic signatures.

"Secure digital identities are becoming increasingly important for digital processes via networks, web and cloud. The two-day workshop in the Economic Affairs Ministry in Berlin showed that graduated security is required, as proposed in IEC 62443, and a broad coverage of the identities of persons, machines, high-grade objects and even software. There is also an international consensus that secure digital identities are the precondition for secure communications between companies, which are also a fundamental security pillar for I4.0.

Each company involved in the I4.0 ecosystem (each participant) must have a trusted authority, which issues identities via certificates within the company to machines and software processes.

To scale amongst different companies, trusted third parties are needed to confirm the authenticity of the distributed authorities.

In Europe, this role can be played by public and private institutions which are licensed by the EU in line with eIDAS or in a similar manner. It is necessary to examine approaches to this outside Europe.

Important preconditions for the applicability of secure digital identities include mutual recognition and a common understanding of the security level selected."

Dr. Detlef Houdeau, Infineon AG

Trustworthiness

Use case

For the shoe brand and consumers, it is important that their data is only released to trusted partners and their data is safe from third-party access. Therefore, for example, when selecting a producer through a platform, the shoe brand can make a high level of trustworthiness a central requirement for winning the contract for production.

Special requirements for trustworthiness:

- Trustworthiness must be established as a qualitative decision-making criterion for commercial action along the entire value chain.
- The criteria for determining trustworthiness must also be drawn up, along with the relevant metrics. The company organization and the skills of the staff must also be considered (maturity).
- The integrity (correctness) of the shared data must be ensured as a basis for trustworthiness.
- The concepts to assess trustworthiness and the protection of integrity must be internationally standardized in order to make international value creation networks more flexible.

Co-Speaker Robert Martin, The MITRE Corporation // Industrial Internet Consortium

Challenge

For a successful information exchange, there must be trust in the security of the communication link and in the secure processing of information by the relevant communication partner. Aside from the technical aspects, a successful information exchange depends on the relevant partners having a firmly embedded, reliable and measurable approach to operational security. The term 'trustworthiness' is used to describe the quality of existing and future relationships between companies, people, systems and components. Integrity is an important goal for all the five key system characteristics of trustworthiness; without integrity, the trustworthiness comes into doubt.

Thesis

If cooperation with new partners is ad hoc, organizational and technical solutions should be set up to evaluate the degree of trustworthiness and to be able to transmit it to the potential partners in an automated way (comparable to intelligent scoring and rating at Amazon, etc.).

Suggested technical concept

Trustworthiness describes the level of trust that an entity meets. The term is used to describe the quality of existing and future relationships between companies, people, systems and components. The integrity of a unit is an important component of the trustworthiness, since without system and data integrity no statements can be made about the assumed behaviour of a unit. The characteristic categories for the total trustworthiness are: security, safety, privacy, reliability and resilience. The concept applies equally to information technology (IT) and operational technology (OT) – contextually with a different weighting of categories.

"For a successful, trustworthy information exchange, trust must exist in the security of the communication connection and in the secure processing of the information by the respective communication partner.

A key contribution towards this is delivered by measures to protect integrity, which all stakeholders, i.e. manufacturers, integrators, operators and service providers, need to transparently and unambiguously communicate to their clients and demand from their suppliers. This helps to ensure that the client receives precisely what the supplier released and the client ordered.

The development and international standardization of automated procedures to evaluated trustworthiness and the protection of integrity will make a key contribution towards flexibilising global value creation networks. Automated surveys of protection of integrity and trustworthiness are a key precondition for ad hoc value creation networks, not least on a cross-border basis."

Michael Jochem, Robert Bosch GmbH and chair of the Working Group "Security of networked systems"

6. Next Steps

The conference is a milestone in the continuous global exchange about IT security issues.

The partners are working on requirements for standardization in the issues identified. This refers to both standardization in technical terms and the need for coordination in political terms.

The findings of the conference were summarized by the concluding panel.

- *Dr. Wolfgang Klasen, Siemens AG, and chair of the "Standards" subworking group of Industrie 4.0 Security*
- *Dr. Detlef Houdeau, Infineon AG*
- *Dr. Takeshi Yoneda, Mitsubishi Electric // Robot Revolution Initiative*
- *Robert Martin, The MITRE Corporation // Industrial Internet Consortium*
- *Michael Jochem, Robert Bosch GmbH and chair of the Working Group "Security of networked systems"*

The experts agreed that the following aspects must be processed and coordinated internationally as a priority, as illustrated in Figure 2 and mapped in a timeline

- Establish security by design as a leading principle
- Establish security as a quality feature of new digital business models. Security measures must be an integral element of the concepts and their realization. This applies both to the digital map and to the physical representation of the I4.0 system.
- Implement cross-company authentication and authorization on the basis of secure identities
    - The use of identities with needs-oriented graduated security characteristics must be ensured across the board. As far as possible, the identities must be bound irrevocably with the entities.
    - Define regional requirements for trust centres and balance them with other regional approaches, e.g. from Japan or China, in order to establish a common demand profile that is interoperable. This includes technical and organizational as well as regulatory demands.
    - Elaborate a policy regarding the international cooperation of regional trust centres.
- Implement secure communications (company-wide/ cross-company) that consider the demands regarding the security goals of the stakeholders.
    - Define architecture and protocols that support integrity and confidentiality goals as well as attack detection capabilities.
    - Elaborate standardized rules and agreed policies for the access to each communication partner in the supply chain.
    - Establish a common and standardized classification of data and information to enable its automatic handling and controlled usage.
- Establish open, clear and transparent indicators and profiles for trustworthiness at company, system, and product level.
    - The integrity of the shared data must be ensured as a basis for trustworthiness.
    - Identify the targets of trustworthiness among organizations, people, systems, procedures, components (e.g. parts, products, devices) and data along the lifecycle.
    - Identify the trustworthiness assurance and levels for the targets, which may be requested or identified automatically from each participant of the value chain.
- Develop a common roadmap with joint next steps and priorities and provide input for the ongoing international standardization work. Press ahead with international standardization in order to ensure interoperability of the security measures.
- In all the measures, the company organization and the skills of the workers must be continuously developed in order to meet the current security requirements

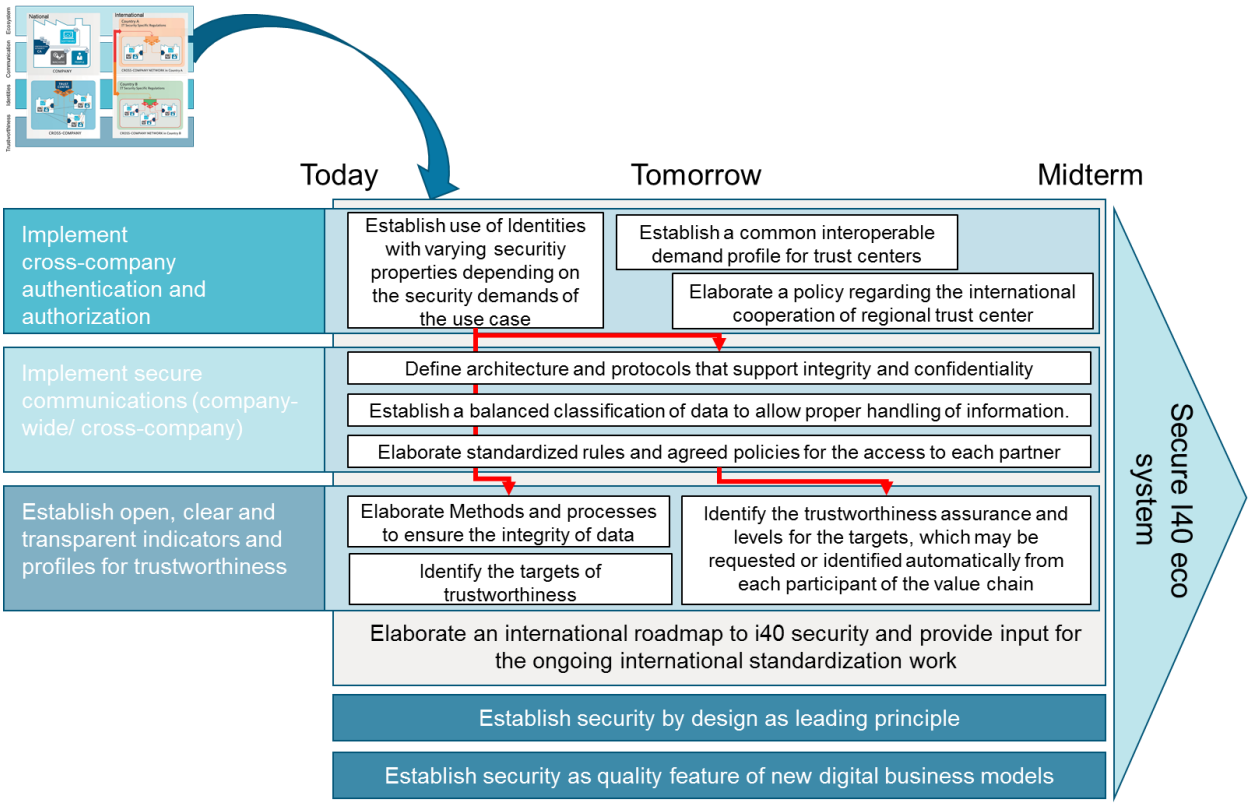

Figure 3: Next steps to achieve a secure I4.0 ecosystem