PLATTFORM INDUSTRIE 4.0

GUIDELINE

IT security in Industrie 4.0

First steps towards secure production

What basic principles lie behind the term "Industrie 4.0"? First of all, production processes in Industrie 4.0 are digitally linked to an increasing extent, and secondly there is a growing trend to form inter-company cooperation and value creation networks. The (fully) automated communication across widely differing interfaces makes it possible to act faster and more dynamically, to carry out production processes more efficiently and to extend conventional fields of business by adding new, platform-based business models.

The essential prerequisite for a successful implementation of Industrie 4.0 is a **secure** and **trustworthy treatment of data and a reliable protection of inter-company communication from external attacks**. Inter-company value creation networks can only be established and profitably used if the data streams are unambiguous and able to allocate to secure identities.

Secure entry into digital and networked production

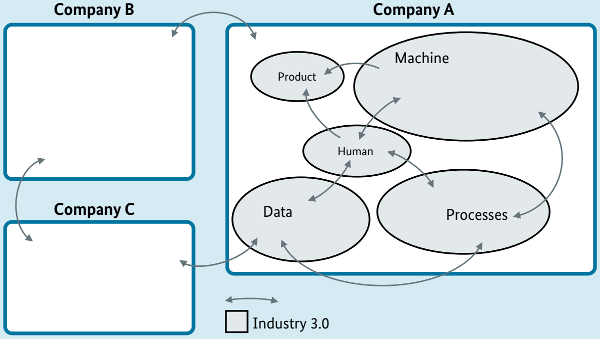
In their transition to the value creation networks of the future, working group 3 of the Plattform Industrie 4.0 ("Security of networked systems") offers guidance especially to small and medium-sized enterprises (SMEs) to help them to make a secure entry into digital and networked production.

Not every SME will need to establish or initiate its own value creation networks in the future. But to ensure that business is not lost, SMEs should be able to cooperate and act independently in the future cooperation networks of their business partners or customers. One of the major challenges in this process will be to develop the necessary **digital competence** to enable them self to preserve **digital sovereignty and freedom of action** and to **protect their corporate assets** even in Industrie 4.0.

A scenario for the future: order-based production in dynamic value creation networks

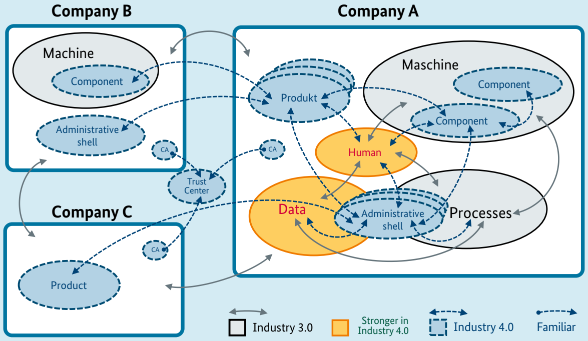
Due to the increased use of information and communication technology, in the next few years **flexible value creation networks** in Industrie 4.0 will progressively replace classical production chains with their largely hierarchical structures: business companies will offer free production capacity via a digital platform and thus increase the utilisation 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.

Flow of information in the classical business model of Industrie 3.0



Networking within a company is already in place.

Digital networked value creation networks of the future Industrie 4.0



The automated communication between companies will be extended to provide greater agility by direct communication between the entities (e.g. people, machines and products) of the participating companies.

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** – from production and planning through to logistics and supplier management – are **digitally networked** both internally and between companies.

The scenario of this future “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 are 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 third party interference. Value creation networks will be successfully established and ready to operate when they can be based on validated, verified and thus **secure identities**. Only then can the communication partners be unambiguously and reliably identified and the transmitted data validated.

Cooperation networks in the future: challenges for IT security

Companies can participate in future value creation networks if they fulfil the **basic requirements for secure and trustworthy communication**: it must be possible to exchange order, production and process data between the companies in the network without any possibility of access by unauthorised third parties.

The fundamental requirement for inter-company cooperation is to have company-specific processes which recognise the **relevant corporate assets** and their necessary protection level. What data and information must be given special protection in your company within complex value creation chains? Setting up your company to participated in a prosperous Industrie 4.0 context therefore initially requires an openness for new information technology which can, for example, facilitate the direct exchange of order-specific data with your own manufacturing execution system (MES).

From the IT security perspective, the **authentication of communication partners and systems** is especially important in Industrie 4.0. It must be ensured that the sender is the claimed party and that the information reaches the desired recipient. Can the information received be unambiguously ascribed to the original author, even in the fully automated communication cascades of Industrie 4.0? Similarly, checking the authenticity of the query and the integrity of the order data are relevant tasks on the basis of which the capacity of the production resources must be evaluated, and depending on the result, an automated order for the input products, raw materials and consumables must be made.

A large number of queries with widely differing content must be expected. Therefore, **in IT processes** it will also be especially necessary to use **standards for identification, authentication and authorisation**. The exchange of an increasing volume of (production) data requires the use or provision of cloud-based services and data platforms. This is possible if there are standardised and secure methods which ensure the protection of the goals of confidentiality, integrity and availability throughout the process.

The number of parties, machines and workpieces involved also requires the administration of **user accounts and authorisations** – and this goes far beyond the boundaries of the individual organisation. Simple, secure and standardised methods to integrate the “identity providers” into your company's own user management are therefore indispensable. They enable this task to be reliably determined even in complex structures and hierarchies.

Analysis: where is my company from an IT security perspective?

To prepare your company and its associated products for the future deployment of Industrie 4.0, it is essential for SMEs to decide in advance on how the company could be integrated and positioned in Industrie 4.0 value creation networks. This should enable conclusions to be drawn about the need to protect the corporate values and the necessary security measures.

The focus is on the **“CIA” triad of protection goals** for data exchange: **C**onfidentiality, **I**ntegrity and **A**vailability. In addition, authenticity (identification and authorisation of the communication partner) is becoming increasingly important in Industrie 4.0.

In the following selection of security features, the processes which are critical for success have the highest priority. This includes protection from sabotage and the protection of business secrets, such as production know-how.

To make it easier for companies to **carry out their own risk analysis**, the working group “Security of networked systems” recommends that the following central questions should be answered:

- What manufacturing competence and capacity can be offered or should be integrated?

- What data must be provided – when, to whom and how – in the framework of an inter-company process chain, and what data is needed when, by whom and how?

- How critical is this data for confidentiality and integrity within the company?

- In particular: how can compliance with data protection law be ensured in the treatment of customer data?

- What cooperation partners are available for resource sharing within distributed production and value creation networks, and to what extent must confidential data be exchanged with these partners?

- What contracts may need to be concluded with cooperation partners, e.g. in relation to the allocation of responsibility and liability for any faults or disruption, or the ownership rights for the data provided or processed?

- What machines, components and products should be communicated externally by your company's production department in an Industrie 4.0 process and then require identity with the corresponding characteristics?

- How can secure external communication be ensured in production to guarantee the integrity and confidentiality of the information transmitted?

- Which members of staff are responsible for IT security in the company's production and administration departments?

Act now: what can be done today within your company to ensure a secure start in Industrie 4.0?

The steps which should be initiated to develop your company from an IT security perspective, and especially its own production, depend primarily on the individual situation of each company. The above questions will help to reach an initial self-assessment.

Successful participation in networked value creation networks in Industrie 4.0 requires the necessary IT security. In many cases, the basic requirements can be fulfilled by measures which are easy to implement.

In the opinion of the working group, the following topics should usually be given priority in order to meet the requirements for Industrie 4.0:

1. The persons responsible for security in an information security management system (ISMS) must be designated and trained.

2. Measures must be established and implemented to heighten the awareness of the production personnel for IT security risks.

3. Security concepts for network access points (remote maintenance, WiFi, cloud, etc.) must be developed and implemented.

4. Provisions must be defined for the use of removable data storage media (USB sticks etc.) and external hardware (programming devices, diagnostic systems etc.).

5. Awareness must be created for risks in the use of smartphone and tablet systems in production.

6. Security precautions to protect from malicious software in production must be demanded when purchasing new machines and equipment.

7. Up-to-date operating systems, production software and security updates must be demanded from manufacturers.

CONCLUSION: Industrie 4.0 is characterised by cooperation with many partners in a spirit of trust. To ensure that Industrie 4.0 can be successful and achieve its potential for German SMEs, your company must now be brought up to date so that it is in a condition in which the future security requirements can be fulfilled.

Further information can be found, for example, in the following publications:

- Industrie 4.0: On the way to the smart factory – the electrical industry is pushing forward, ZVEI – German Electrical and Electronic Manufacturers' Association
- Ausblick Security Industrie 4.0, ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V. Nur auf DE *(in German)*
- Fragenkatalog Industrial Security – Einfach anfangen, Verband Deutscher Maschinen- und Anlagenbau (VDMA) *(in German)*
- ICS Security Compendium, Federal Office for Information Security
- Light and Right Security ICS (LARS ICS), Federal Office for Information Security *(in German)*
- VdS Guidelines for Information Security – Cyber Security for Small and Medium Enterprises, VdS Schadenverhütung GmbH
- Security in Automation – INS study, DIN/NAM/VDMA
- Status Quo der Security in Produktion und Automation – Studie, Verband Deutscher Maschinen- und Anlagenbau (VDMA) *(in German)*

This publication is a result of the WG on the security of networked systems (Plattform Industrie 4.0).

AUTHORS OF THE WG ON THE SECURITY OF NETWORKED SYSTEMS:

Dr Lutz Jänicke, PHOENIX CONTACT Cyber Security AG | Michael Jochem, Bosch Rexroth AG | Dr Wolfgang Klasen, Siemens AG | Dr Bernd Kosch, Fujitsu Technology Solutions GmbH | Michael Krammel, Koramis GmbH | Lukas Linke, ZVEI | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik (BSI) | Michael Sandner, Volkswagen AG | Andreas Teuscher, Sick AG | Thomas Walloschke, Fujitsu Technology Solutions GmbH | Steffen Zimmermann, VDMA

Imprint

Published by
Federal Ministry for Economic
Affairs and Energy (BMWi)
Public Relations
11019 Berlin, Germany
www.bmwi.de

Text and editing
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Design and production
PRpetuum GmbH, Munich

Illustrations
Kzenon/Fotolia (cover); welcomia/
istock (p. 2); cookiecutter/Fotolia (p. 4)

Status
April 2016