Issue 03/2021

Industrial IoT Cloud Solution

What you should consider in your selection:

Whitepaper including checklist

adstec
Industrial IT

Marc Schmierer, since 2017 at ads-tec Industrial IT GmbH as a product manager and specialist for IIoT cloud solutions

Foreword

Despite its great growth potential, in large German companies the digitalisation rate in production is just under 30 per cent – in small and medium-sized enterprises it is as low as 20 per cent[1]. One reason for this could be the high number of providers of Industrial IoT cloud solutions. It's good to know what to look for when you're making your choice.

In the age of Industry 4.0 and the constant networking of people and devices, it is hardly surprising that an increasing number of companies are considering the topic of Industrial IoT and looking for suitable solutions. However, the issue raises a lot of questions for many companies: Should I opt for a totally remote maintenance solution? Or would a complete Industrial IoT cloud solution be better? And above all: What's the right solution for me?

This whitepaper outlines the most common considerations that we believe should be taken into account when making your selection. At the end of the whitepaper, you will also find a checklist that you can use to help you evaluate, decide and ultimately select your future Industrial IoT solution.

Marc Schmierer
ads-tec Industrial IT GmbH

Contents

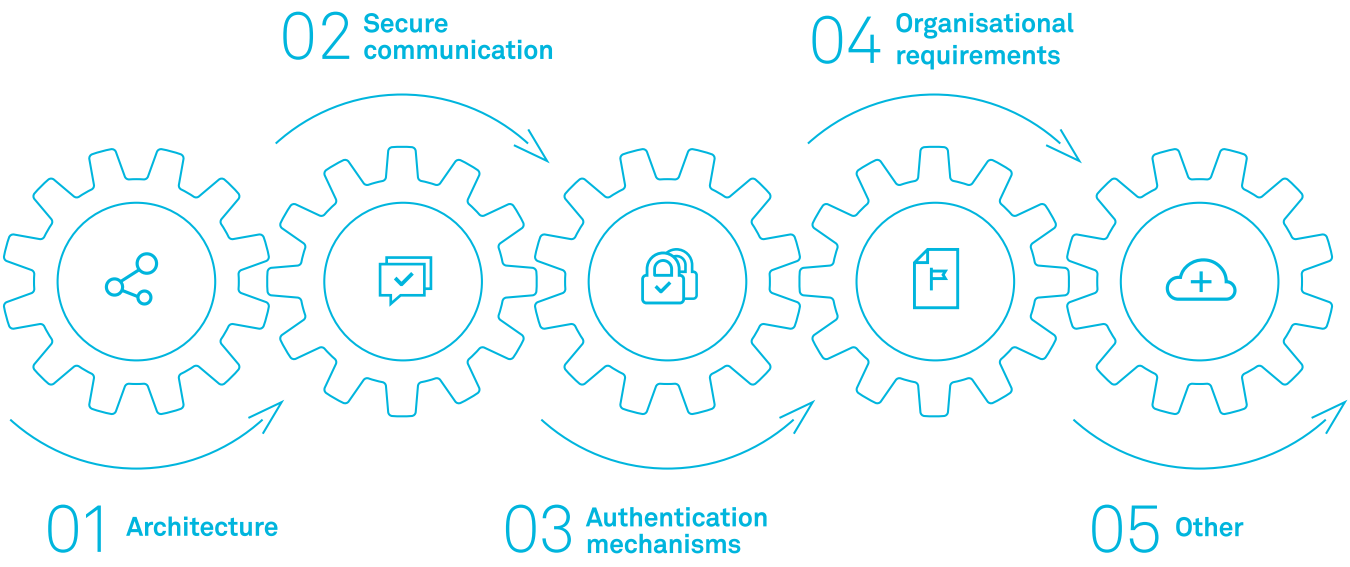
Security Standard

Does the solution offer the best possible protection for your machine & company data?

Make sure that your IIoT solution complies with the BSI's recommended guidelines.

One of the most important factors, and indeed the most important factor for many companies when looking for an IIoT solution, is security. Nobody wants to run the risk of having their company or machines hacked and sensitive data stolen or processes disrupted. Therefore, the key question you should consider when looking for an IIoT provider is: How high is the security level of the solution provided? The German Federal Office for Information Security (BSI) has defined guidelines for the protection of machine and system data, which IIoT providers can follow.

BSI Guidelines for the Protection of Machine and System Data



Source: German Federal Office for Information Security (BSI), September 2020

01 Architecture

The security of an industrial remote maintenance solution ultimately depends largely on its architecture. Therefore, there are some requirements that should be taken into account during the planning and integration of a remote maintenance solution.

Uniform solution
To reduce the risk of a hacker attack, you should avoid "uncontrolled growth".

Remote maintenance components in the DMZ
Remote maintenance components should be located in an upstream Demilitarised Zone (DMZ) rather than in the production network. Firewalls can be used to specify exactly which devices may be accessed.

Granularity of the communication links
Remote access should be restricted to a minimum, i.e. one access per IP and port, as this can reduce the scope of a possible attack.

Connection establishment
Connections should only be established internally (e.g. company network) to externally (e.g. remote maintenance server).

75%

of IT & security experts consider an increase in cyber attacks as their greatest concern during the pandemic[2]

02 Secure communication

Communication and communication channels are also relevant when it comes to protecting machine and system data. Their security is ensured by established standard solutions.

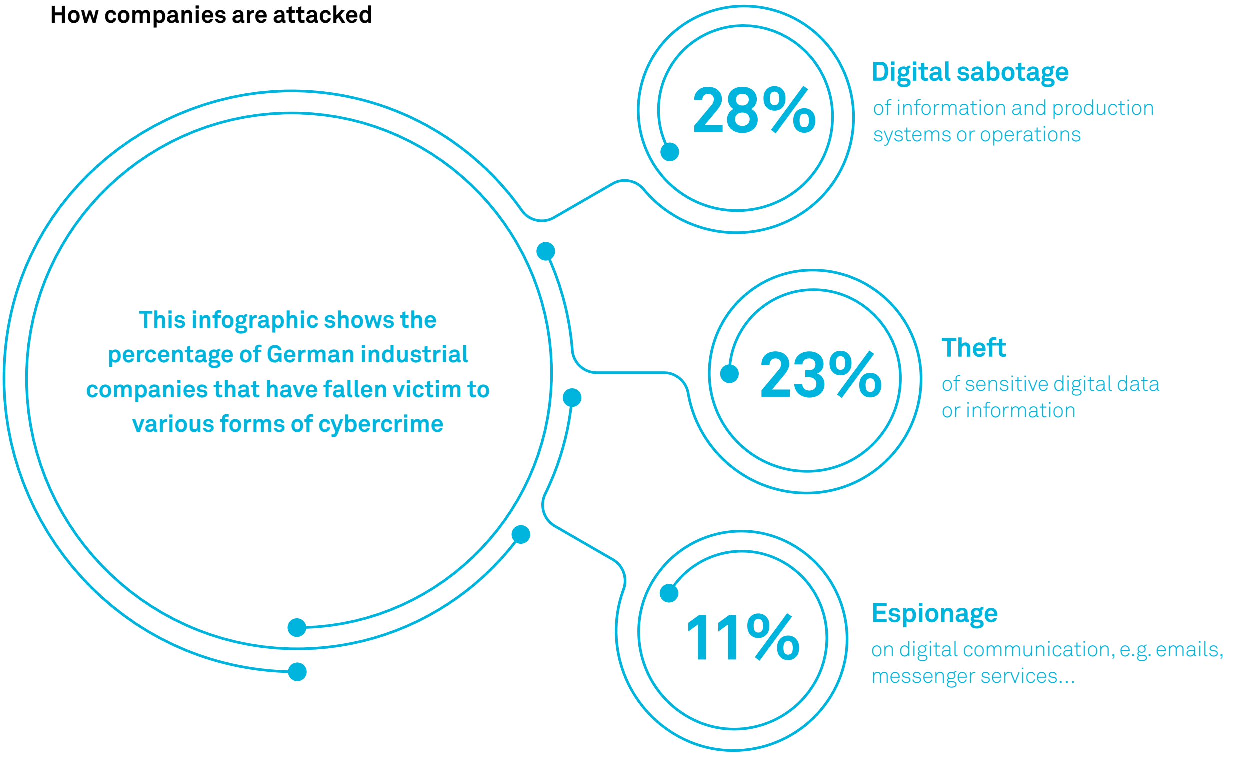
Secure protocols

Select a provider with established protocols. Recommended: the latest versions of TLS (OpenVPN), IPsec or SSH.

Secure processes

Any connection to the machine or system should be encrypted with a strong cryptographic method. Strong connections are AES key lengths of at least 192 bits.

How companies are attacked



This infographic shows the percentage of German industrial companies that have fallen victim to various forms of cybercrime

28% **Digital sabotage** of information and production systems or operations

23% **Theft** of sensitive digital data or information

11% **Espionage** on digital communication, e.g. emails, messenger services...

Source: Bitcom Research, Study on “Cyber Crime in German Companies” , 2019

03 Authentication mechanisms

Secure and reliable authentication of users is critical to the protection of machine and system data. This is the only way to ensure a sufficient level of security for industrial remote maintenance.

Granularity of accounts
It is essential that you avoid group accounts and only choose a provider that offers an account for each user.

Strong authentication mechanisms
For maximum security, two-factor authentication should be used instead of a password. For hardware-based solutions, providers with smartcards, USB tokens or one-time passwords are recommended, as it is not possible to copy hardware components here.

04 Organisational requirements

Architecture and technology are fundamental in protecting machine and system data, but to ensure maximum security, measures should also be taken to ensure safe integration and operation.

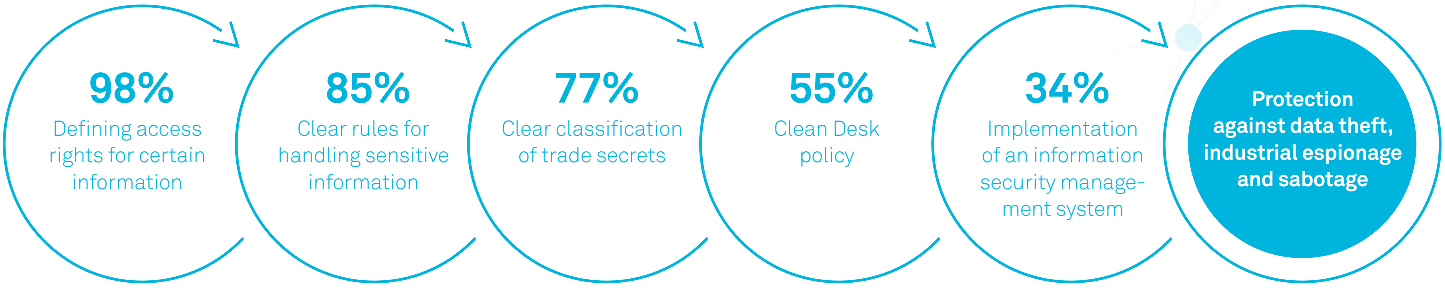
Inventory
Device access should be recorded, which means that it must be possible to trace who was connected to a device, when and for how long.

Time window
Access to the machine or system is granted either in the event of a malfunction or by setting a time window (e.g. key switch). In both cases, the activation or deactivation must be documented the activation or deactivation must be documented.

Patch process
Components should be patchable so that any potential vulnerability can be quickly fixed.

Logging & Alerting
The solution provider should record log-ins and trigger alarms if necessary.

Organisational measures during deployment
Alongside technical requirements, organisational measures play a significant role in the security standard of an IIoT solution. The results of this study, which surveyed over 1,000 companies, demonstrate clearly which organisational security measures are used by companies to protect themselves against data theft, industrial espionage and sabotage.


98% Defining access rights for certain information

85% Clear rules for handling sensitive information

77% Clear classification of trade secrets

55% Clean Desk policy

34% Implementation of an information security management system

Protection against data theft, industrial espionage and sabotage

Source: Bitcom Research, 2020 Study Report "Espionage, Sabotage and Data Theft - Economic Protection in the Networked World"

05 Other

Depending on the application, additional individual measures can also be taken to ensure the security of the remote maintenance solution.

Scalability
The solution should be able to adapt to changing circumstances, such as the number of machines and systems, but also to existing machines and brownfield machines.

Investment protection
When selecting an IIoT service platform, future requirements must also be taken into account.

IT Security made in Germany

IIoT providers who meet certain criteria are eligible to be awarded the trust mark "IT Security made in Germany" by the Bundesverband IT-Sicherheit e. V. (TeleTrust). TeleTrust, based in Berlin, is the first port of call for its members in Germany and Europe when they require expert information on topics related to IT security. Various forums and events give members the opportunity to exchange views on changing safety measures. The "IT Security made in Germany" trust certificate guarantees unrestricted, maximum transparency and the highest level of data security – all made in Germany. This means you not only benefit from the quality of the solution, but are also secure in terms of service and maintenance.

Tip: Ask the provider about their Security Guidelines. You can find information in these about which technical concepts are used, which manufacturers the provider works with and how problems are handled.

Required criteria for suppliers

1. The company's headquarters must be in Germany.
2. The company must offer reliable IT security solutions.
3. The products offered must not have any hidden accesses ("backdoors").
4. The company's IT security research and development must be carried out in Germany.
5. The company must be committed to complying with the requirements of German data protection law.

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

Source: Bundesverband IT-Sicherheit e. V.

„Networks should feature holistic, end-to-end security architecture.“[2]

Dietmar Schnabel
Regional Director Central Europe at Check Point Software Technologies GmbH

Functionality

Does the solution provide all the functionalities you need for your work?

Make sure that solution covers both your current as well as your future requirements

Imagine the following scenario: shortly after your platform has been launched, you realise that you need more IIoT functionality. However, this is not included in your platform. As you urgently need the functionality, you have no choice but to connect another service provider to your company network.

You should therefore clearly define in advance which functionalities you want from the solution in order to avoid uncontrolled growth at a later stage and prevent unnecessarily increasing the security risk.

Foresight not hindsight

When looking for an IIoT solution, you will encounter numerous providers with different approaches. The services offered range from VPN solutions and cloud-based approaches to provider solutions in the machine-to-machine (M2M) sector, and the product features of individual solutions differ significantly in some cases[3]. To find the right provider for you, you should define in advance which functionalities you currently need and which may be required in the future.

The German Federal Office for Information Security (BSI) also recommends forward-looking action in this regard, in order to avoid later uncontrolled growth. Therefore, when looking for a provider, you should already clearly define whether you will need further functionalities at a later point in time, such as visualisation and presentation of machine and/or system data in dashboards.

In this regard, it is advisable to choose a provider whose solution, in addition to the pure remote maintenance aspect, also includes additional IIoT functionalities that you can opt into flexibly and cancel again if they are not used. This allows you to react quickly to changing requirements and only pay for additional functionalities for as long as you use them. Platforms with open interfaces such as REST are particularly recommended in this regard. These offer additional investment protection for customer- and industry-specific topics such as machine learning, because future services can be directly integrated into the existing system.

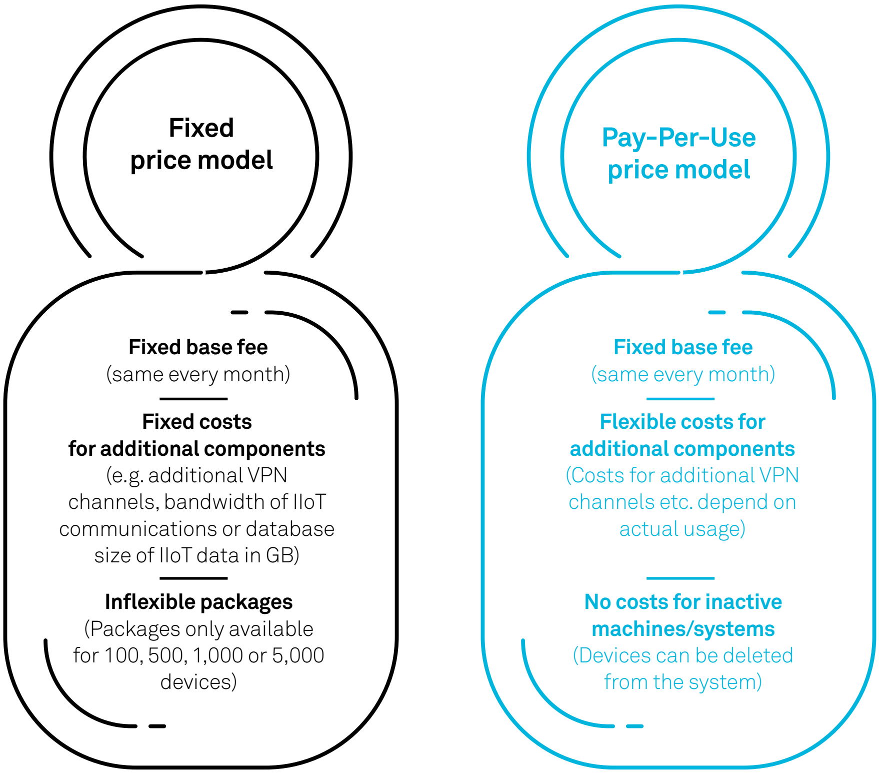
Tip: Some companies offer configuration phase workshops to assess both current and future requirements and tailor the IIoT solution to meet them.

Which price model is right for you and your requirements?

Carry out a break-even analysis for a better assessment.

Most IIoT service platform providers offer two billing models: the fixed price model and the flexible pay-per-use model. But which is more suitable for you and your requirements?
When making the final decision as to which of these two models is right for you, it is advisable to carry out a break-even analysis. This will help you to find out how many machines are needed to make one model more cost-effective than the other.

Fixed price model vs. pay-per-use model
Looking at the two common pricing models, you can see both similarities and differences. The difference between the models is the cost of other components such as maintenance, servicing, updates and ensuring the functionality of the platform.



Fixed price model

Fixed base fee
(same every month)

Fixed costs for additional components
(e.g. additional VPN channels, bandwidth of IIoT communications or database size of IIoT data in GB)

Inflexible packages
(Packages only available for 100, 500, 1,000 or 5,000 devices)

Pay-Per-Use price model

Fixed base fee
(same every month)

Flexible costs for additional components
(Costs for additional VPN channels etc. depend on actual usage)

No costs for inactive machines/systems
(Devices can be deleted from the system)

An important consideration when determining the appropriate pricing model is billing intervals. Both annual and monthly billing is common, with some advantages and some disadvantages to each, depending on how you use the service. If, for example, you need to adapt the functionality of your solution more frequently or the number of machines to be monitored will vary, then monthly billing on a pay-per-use basis is recommended. This allows you not only to keep better track of your costs, but also you have more security with your planning compared to annual billing.

When making the final decision as to which pricing model is most suitable for you and your requirements, you should carry out a break-even analysis. This allows you to determine the number of machines at which you should opt for one model over the other.

Handling, Adaptability & Scalability

How well can the solution be integrated into your company?

Make sure that the solution fits your requirements - and not the other way round.

User, rights and device management. Handling by different employees. Compatibility with different end devices. All these aspects require a highly adaptable and scalable IIoT solution. Therefore, when researching and selecting your IIoT service platform, make sure that it is adaptable to your needs and avoid inflexible products that would require you to adjust your processes and structures.

Intuitive handling
You should work with a solution that has clear structures and is intuitive to use so that you can manage issues such as users, rights and devices as efficiently as possible. This will help you save time, for example, when granting service staff access rights to certain machines or when assigning specific service cases to service staff.

No-Code-Platform
A key consideration in this context is the web interface. You should use a no-code-platform that does not require any special IT knowledge, such as programming skills, to operate. This will enable you to implement sophisticated IIoT applications, such as readout and visualisation of graphics of machine/system statuses, without the need to consult a specialist.

Adaptable solution
An adaptable solution can be identified, for example, by the fact that a provider isn't focused on a specific industry or end device and that its solution will work with the operating system that is currently used in your company and doesn't require you to install a new operating system.

Demand-oriented scalability
As your requirements in terms of the number of machines requiring maintenance may change over time, your IIoT solution should be capable of supporting a small as well as a large number of machines.

Tip: Ask the provider to show you relevant case studies with comparable framework conditions to make sure that the IIoT solution you choose really is adaptable.

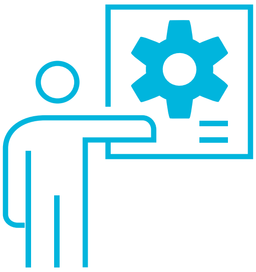
Conclusion

The more clearly you define your requirements in advance, the easier your decision will be in the end.

Management and strategy consultancy McKinsey & Company estimates that German companies could generate an additional 126 billion euros in value creation by 2025 through consistent digitalisation, which includes remote maintenance and IIoT[4]. So it's hardly surprising that many companies are currently actively looking for a solution. We believe that the selection criteria highlighted in this whitepaper are a good guide for choosing the right IIoT solution. The final decision about which IIoT solution is the best for you and your company depends largely on how clearly you define your requirements in advance – ideally, directly with the provider in a workshop or similar.

If you have several providers in mind at the end of your research, it can be helpful to watch a demonstration of the solution. Some providers offer seminars or online demos: register, allow them to explain the solution, ask questions and get a feel for the provider. This can give you a sense of whether the solution is what you had imagined.

If there are still several providers that you are considering, you should request non-binding trials of the solutions. Some providers provide test access specifically for this purpose or can send test devices that you can have your entire team test in your company.



Note: It's important not to rush your decision. Take your time and only implement a solution in your company that you have thoroughly tested and are completely convinced by.

Checklist

Checklist for selecting a suitable Industrial IoT solution
The following checklist contains, in our view, the most important aspects you should consider when selecting an IIoT solution. If you can tick off all the following points, your selection is highly likely to be a modern, secure and adaptable IIoT solution.

☑ Connection establishment

Does the solution ensure that connections can only be established from internal to external systems?

☑ Data transfer

Does it use the encryption standards recommended by the BSI?

☑ 2-factor authentication

Are passwords authenticated using a standard authenticator app and/or email?

☑ Communication recording

Can all connections, including visitor information and duration, be clearly recorded and assigned?

☑ No-Code-platform

Is it possible to create visualisations without special programming knowledge?

☑ Remote access

Is there an encrypted connection between the service provider and the machine operator during access?

☑ Identification

Is unique identification guaranteed through smartcards or a hardware certificate on a crypto chip?

☑ Rights management

Can user-defined groups/organisations be created and given specific rights?

☑ Encryption

Are secure cryptographic encryption methods used according to the current BSI recommendations?

☑ Adaptability

Can the solution be adapted to the customer's existing operating systems and end devices?

For questions, please contact ads-tec Industrial IT GmbH:
Tel.: +49 70 22 25 22-200   Email: sales@ads-tec.de

Sources

1 Lichtblau, K.; Schleiermacher, T.; Goecke, H.; Schützdeller, P.
Digitalisierung der KMU in Deutschland. Konzeption und empirische Befunde. 2018.
URL: https://www.iwconsult.de/fileadmin/user_upload/projekte/2018/Digital_Atlas/Digitalisierung_von_KMU.pdf (Stand: 19.11.2020)

Original quote from: Raphael Kiesel, Timo Heutmann, Jan Dering, Alexander Kies, Thomas Vollmer, Robert H. Schmitt
Whitepaper Cybersecurity in der vernetzten Produktion. 2020.
URL: https://www.ipt.fraunhofer.de/content/dam/ipt/de/documents/whitepaper/whitepaper-cybersecurity-in-der-vernetzten-produktion.pdf

2 Checkpoint Software Technologies
Umfrage zum Status der IT-Sicherheit nach der Corona-Hochphase. 2020.
URL: https://www.infopoint-security.de/check-point-umfrage-zum-status-der-it-sicherheitnach-der-corona-hochphase/a24059/

3 BSI-Veröffentlichung zur Cyber-Sicherheit
Fernwartung im industriellen Umfeld. 2018.
URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf;jsessionid=6A09424BCC4D7BFC46FC7D9B4E959FCE.internet082?__blob=publicationFile&v=1 (Stand: 11.07.2018)

4 McKinsey & Company (Hrsg.)
Digitalisierung im Mittelstand erhöht Wachstum in Deutschland um 0,3 Prozentpunkte pro Jahr. 2017.
URL: https://www.mckinsey.com/de/news/presse/di%ADgitalisierung-im-mittelstand-erhoht-wachstum-in-deutschland-um-03-prozentpunkte-pro-jahr (Stand: 15.01.2019)

Original quote from: Raphael Kiesel, Timo Heutmann, Jan Dering, Alexander Kies, Thomas Vollmer, Robert H. Schmitt
Whitepaper Cybersecurity in der vernetzten Produktion. 2020.
URL: https://www.ipt.fraunhofer.de/content/dam/ipt/de/documents/whitepaper/whitepaper-cybersecurity-in-der-vernetzten-produktion.pdf

ads-tec Industrial IT GmbH
Heinrich-Hertz-Straße 1
D-72622 Nürtingen
Phone +49 70 22 25 22-200
Fax +49 70 22 25 22-402
sales@ads-tec.de
www.ads-tec.de

TECHNOLOGY
MADE IN GERMANY

adstec
Industrial IT