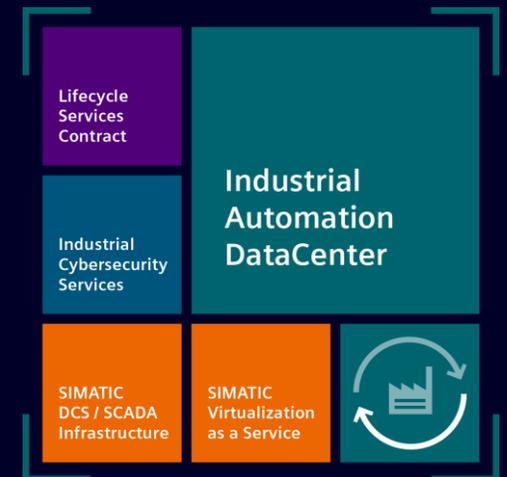




Industrial Automation DataCenter

Cross the digital chasm and modernize your IT/OT infrastructure



IT infrastructure in OT environments requires automation expertise

Operative challenges

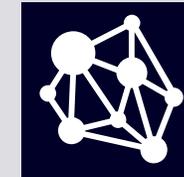
- Digital developments that have been common in office IT environment for years are now also becoming increasingly important in the automation environment, e.g. connectivity, virtualization.
- The environment of operational technology (OT) differs greatly from office IT, e.g. long asset lifecycles with discontinued systems and high system heterogeneity.
- The same applies for the requirements: While for IT systems data availability, integrity and confidentiality are most important, for OT systems equipment availability and safety have the highest priority.
- OT staff has a high expertise in mechanics, electrical & instrumentation, but usually lacks IT skills, while IT staff is lacking the OT jargon and understanding

Plant managers aim to take advantage of the benefits of digitalization – but the requirements of the automation environment have to be considered carefully.

Required solution



Combined expertise in automation, digitalization and cybersecurity



Turnkey comprehensive concepts for IT infrastructure in automation environment and Industry 4.0



Digitalization of industry while keeping high availability, reliability and security

How to solve the IT/OT dilemma?



Hyper-converged IT infrastructure for your Digital Enterprise with Industrial Automation DataCenter



Solution

- The Industrial Automation DataCenter is a custom-configured data center for all IT requirements in production, developed by Siemens experts with combined expertise in automation, digitalization and security. It facilitates entry into the forward-looking, digitalized infrastructure of the industrial environment of the future.

How does it work?

- All important core elements of a data center are included: high performance computing (with high availability), IT/OT networks, back-up and disaster recovery, process data archiving, uninterruptable power supply and IEC 62443 compliant security architecture.
- The holistic approach covers consulting, configuration and appropriate support services throughout the entire life cycle.
- The perfect symbiosis of hardware, software and services from a single source provides this ready-to-run hyper-converged IT infrastructure for industrial environments.



Pre-configured and tested state-of-the-art components

The core of the Industrial Automation DataCenter is a virtualization solution with virtual machines, supplemented by suitable hardware and software components for increased overall system availability and energy-efficiency.

Pre-configured and pre-tested hardware and software components

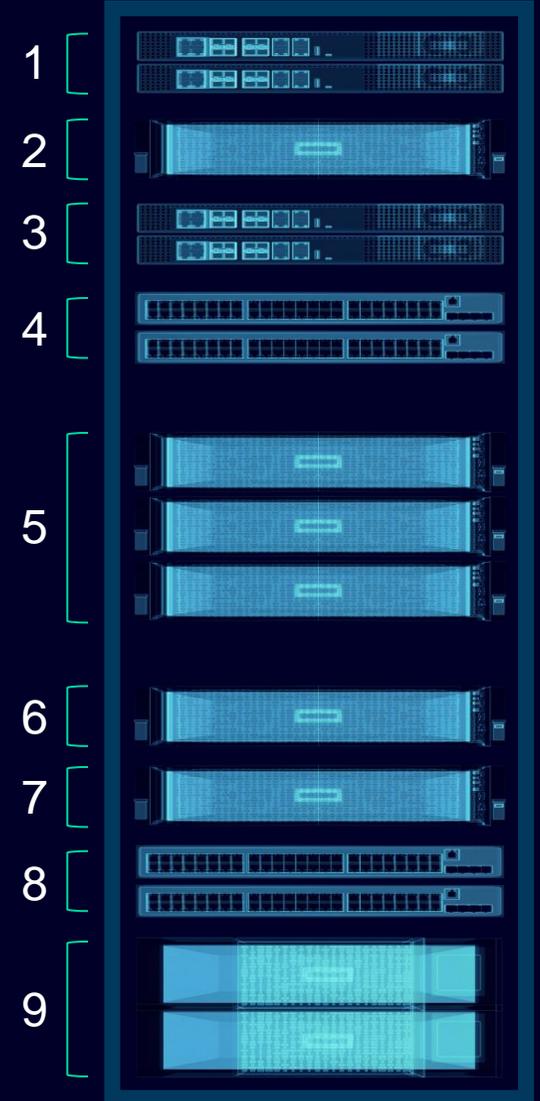
1. Front Firewalls
2. Industrial DMZ
3. Back Firewalls
4. IT Networking
5. Computing
6. Backup & Disaster Recovery
7. Process Historian
8. OT Networking
9. Uninterruptible Power Supply



Scalability:
resource upgrade
capability during runtime
to react quickly to
changing conditions

Central manufacturing ensures quality over the entire lifecycle

- Use of proven state-of-the-art technology from market leading companies
- All used hardware and software components are purchased, assembled, installed, configured and tested centrally at the manufacturing in Nuremberg according to strict quality requirements



Future of virtualization with SIMATIC Virtualization as a Service

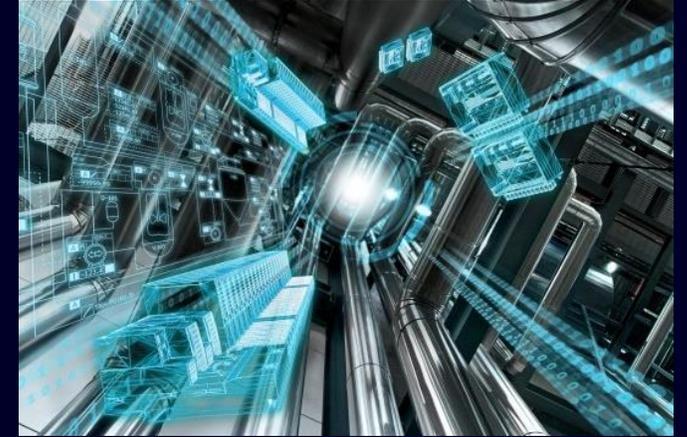
On the basis of the proven virtualization solution SIMATIC Virtualization as a Service, various applications can be integrated on the common hardware platform. The service includes the set-up of the virtualization server, the configuration of the virtual machines and the operating system, as well as the turnkey installation of the applications.

We have broad expertise in hosting the following applications:

- SIMATIC PCS neo
- SIMATIC PCS 7
- SIMATIC Step 7
- SIMATIC WinCC
- TIA Portal
- BRAUMAT
- SIMIT
- COMOS
- DESIGO CC

We are happy to advise you on the integration of your application.

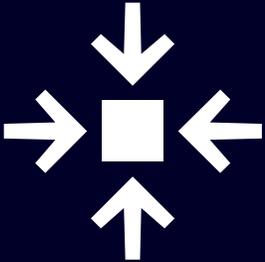
Even throughout the lifecycle of the virtualized system, we take care of comprehensive support for all technical questions about the function, use, and operation of the system components.



Hosting common DCS applications like SIMATIC PCS 7 and TIA portal



Contribution to a sustainable future



Up to **80%** less space required
due to a standardized overall system with
reduced number of communication interfaces

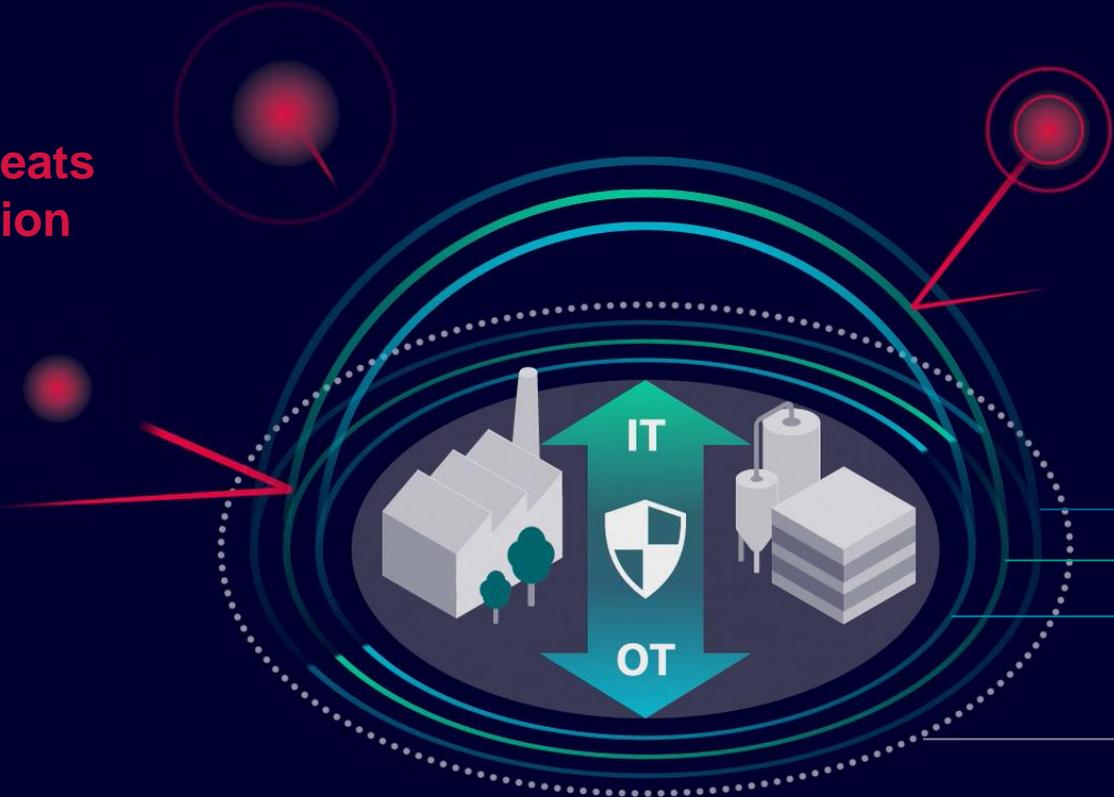


Up to **75%** energy savings
due to optimized use
of the IT resources deployed



Siemens holistic security concept: Defense in Depth based on IEC 62443

Security threats demand action



Defense in Depth based on IEC 62443

- Plant Security
- Network Security
- System Integrity
- Industrial Cybersecurity Services

Industrial Cybersecurity Services: End-to-end approach



Plant Security Services

- Security Assessments
- Scanning Services
- Industrial Security Consulting

Transparency about the current security status

Network Security Services

- Industrial Next Generation Firewall
- Industrial DMZ Infrastructure
- Industrial Anomaly Detection

Increased security level by closing security gaps

System Integrity Services

- Endpoint Protection
- Vilocify Vulnerability Services
- Patch Management
- SIMATIC DCS / SCADA Infrastructure
- SIMATIC Security Service Packages

Long-term protection through continuous security management

Industrial Cybersecurity Services @ Industrial Automation DataCenter



Siemens as reliable partner for IT infrastructure in OT environments

<p>We are the automation experts</p> 	<p>We drive digitalization</p> 	<p>We understand industrial security</p> 	<p>We have specific industry know-how</p> 	<p>We offer state-of-the-art technology and end-to-end services from a single source</p> 
--	--	--	---	--

“We make sure that you can focus on your core business.”

Reference: Bayer CropScience AG, Germany

Digital transformation of the production plants

Customer profile	<p>Bayer CropScience researches, develops and markets highly effective and innovative insecticides, fungicides, herbicides and seed treatment products. Around 2,000 different chemical products are manufactured at the CHEMPARK in Dormagen. Production focuses on the development and manufacture of crop protection products, polymers, plastics and rubber.</p>
Customer objectives	<p>As a result of the modernization, several production plants are to meet the latest requirements of a digital company. All necessary supplies and services are to be designed, offered, implemented and provided with the associated services from a single source.</p>
Siemens solution	<p>Seven production plants were each equipped with an Industrial Automation DataCenter as part of the modernization</p> <ul style="list-style-type: none">• Through intensive cooperation between Siemens and Bayer CropScience AG, the requirements with regard to the special features of production, the network architecture and the existing automation systems were determined and measures for conversion and preparation were developed.• In order to meet the requirements for the availability of the overall system, the system platform was designed on the basis of VMware vSAN technology.• A security workshop, a factory acceptance test and the implementation of specific customer requirements were successfully implemented within the scope of the project.
Customer value	<ul style="list-style-type: none">• Up to 80% less space required due to a standardized overall system with the aim of reducing the number of communication interfaces• Flexible system expansion through preconfigured and ready-to-use individual components• Up to 75% energy savings due to optimized use of the IT resources deployed• Essential IT security measures were already implemented upon delivery

Reference ID: [22382](#)





*Engineered solutions like Siemens' **Industrial Automation DataCenter** are designed to help users **cross the digital chasm** and modernize their automation architectures to **reap the benefits of digitalization.***

(ARC Advisory Group, 2022)

Why should you choose Industrial Automation DataCenter?



Ready-to-run high available IT infrastructure with system-tested and pre-configured components – tailor-made for your plant



High energy efficiency and **space savings** through virtualization platform and optimized use of IT resources



Cybersecurity by design thanks to integrated solutions like industrial DMZ, Next Generation firewalls and backup solution

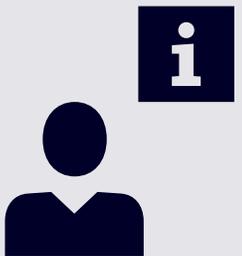
Let us know if there is anything we can support you with!



You want to find out more?

Contact the Siemens partner near you

[Siemens Contact Database](#)



Disclaimer

© Siemens 2023

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity>