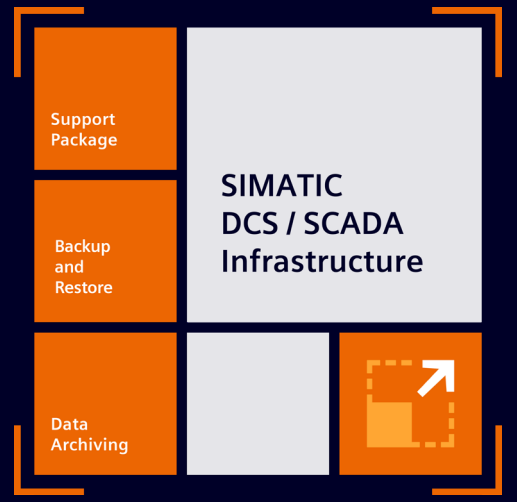
Backup and Restore
(part of SIMATIC DCS / SCADA Infrastructure)

Pre-configured IT infrastructure for backup and disaster recovery



SIEMENS

Complex IT systems require fully supported backup solution

Operative challenges

- Increasing cyberattacks arise awareness for data security and new security regulations (e.g. NIS 2 for EU) require operators to have a system for backup, disaster recovery and crisis management in place.
- In case of disaster - restarting the production after a breakdown or cybersecurity incident?
  - → Data loss should be prevented
  - → Fast and reliable disaster recovery strategy extremely important
  - → Fully supported backup solution needed
  - → Without a trusted partner who knows your production infrastructure you could face long production outage
- Simplifying the installation of complex IT solutions is key

A thoughtful backup and disaster recovery strategy increases the productivity and availability of the production infrastructure.

No backup? No mercy!

Possible consequences

Ignoring new regulations can lead to legal issues, fines and potential exclusion from public tender

Cyber attacks often force productions to downtimes and data loss can occur

Your vendors don’t feel responsible for your disaster incidents and the system can’t be restarted in time

SIEMENS

Pre-configured IT infrastructure for optimized disaster recovery with Backup and Restore (SIMATIC DCS / SCADA Infrastructure)

Solution

SIMATIC DCS/SCADA Infrastructure provides a powerful and pre-configured IT infrastructure for optimized data handling and disaster recovery in industrial environments.

A prefabricated complete system ensures that the engineering and commissioning phase can be carried out as efficient as possible. In addition, customized services cover the complete lifecycle.

How does it work?

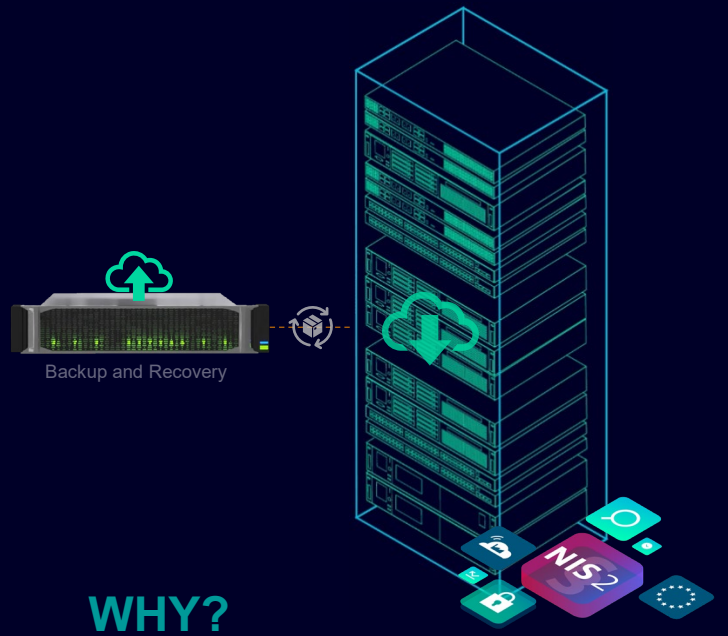
- **Backup and Restore:**
  Best in class disaster recovery backup solution, adapted to industrial environments.
- **Support Package:**
  3- or 5-year service agreement

SIEMENS

SIMATIC DCS / SCADA Infrastructure
Module „Backup and Restore“

Backup and Restore creates automatic backups during operation of the plant to keep all process steps as effective as possible and protect the archived data.

Even the increasing amount of cyber attacks and upcoming security standards (e.g. NIS 2) make it unavoidable to integrate a fully supported backup and restore solution.



WHY?

- prevent data loss
- increase availability
- deal with plant failures and
- restart production as fast as possible after critical downtimes

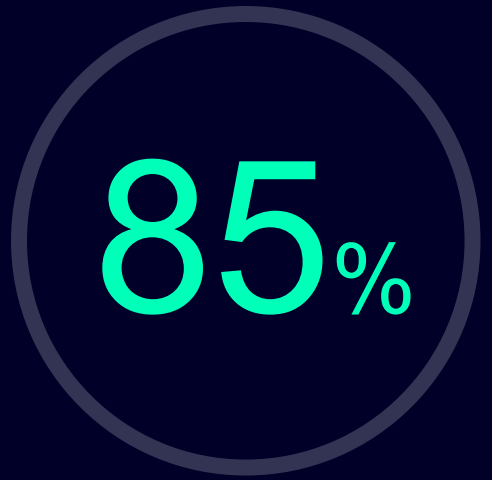
→ a holistic disaster recovery is needed.

No backup? No mercy!

SIEMENS

SIMATIC DCS / SCADA Infrastructure
Module „Backup and Restore“

Keep in mind…



..of organizations were hit by a ransomware attack in 2023

..of ransomware attacks targeted backups

..of the attacks on backups were at least partially successful

Source: Veeam Data Protection Trends Report 2023, Veeam Ransomware Trends Report 2023

SIEMENS

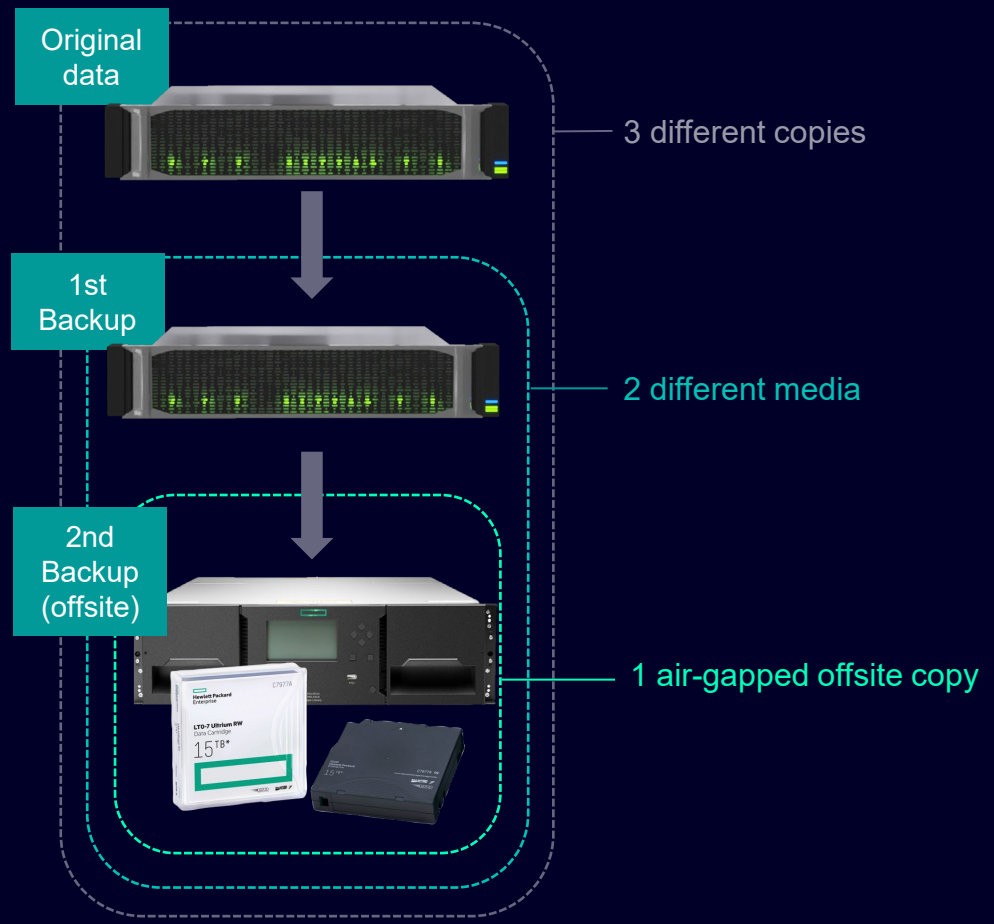
SIMATIC DCS / SCADA Infrastructure
Module „Backup and Restore“

Master the „3-2-1 Rule“!

The ready to run **Backup and Restore** solutions allow runtime backups from your operating system with just a few clicks!

The solution is defined by a fast backup repository with our Backup & Restore – Professional or Essential, for easy and fast backup and restore.

Additional offsite backup archives on SIDSI Tape storage, enable secure and durable backups of large capacity, at a low cost.



SIEMENS

SIMATIC DCS/ SCADA Infrastructure
Module “Backup and Restore”

<u>NEW standardized hardware for the Backup and Restore line based on Dell!</u>

Next to our established hardware based on HPE a new hardware variant from **Dell** is now available for the **SIDSI Backup and Restore** line to ensure an even higher compatibility for our customers regarding different manufacturer needs at their plants.

Based on years of experience, the Dell system was built identically to the HPE system and will countinously maintained in parallel to the well-known HPE hardware.

- Available as PowerEdge R760xs for optimized pricing
- 4th generation Intel XEON Scalable processors
- Supports DDR5 RAM with 5600 MT/s
- Integrated hot swapable BOSS device
- Energy efficient power supplies with 1100W

SIEMENS

SIMATIC DCS / SCADA Infrastructure
Module „Support Package“

Basic Support

Support of **all Siemens software components** is a crucial part

Spare Parts

Defected hardware components will be replaced on **next business day** basis*. All actions are coordinated by the SIMATIC Tech Support

Setup

Preinstallation and **configuration** by Siemens experts guarantee a perfectly matching IT-infrastructure system

Application Support

Our technical support team additionally covers the support of all included 3rd party hard- and software components

*after it has been ensured that it is indeed a hardware defect

SIEMENS

SIMATIC DCS / SCADA Infrastructure
IT/OT Asset Monitoring based on PRTG

What is it about?

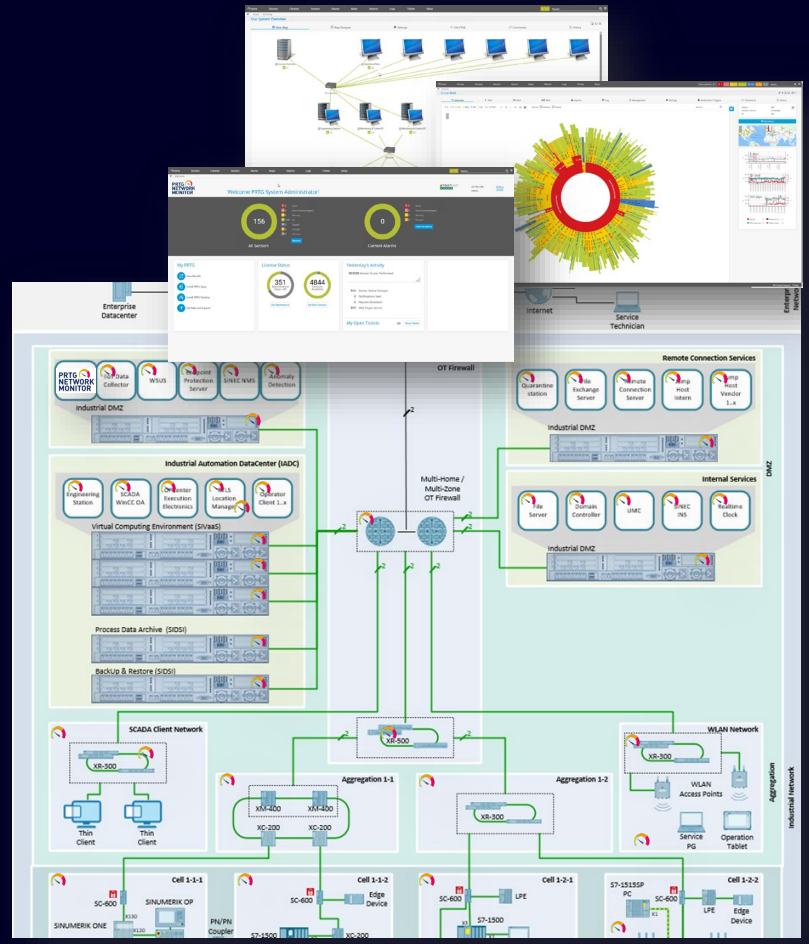
Your IT/OT infrastructure must function reliably to ensure the operational continuity of the entire system. Therefore, it is important to identify problems at an early stage before they cause a failure.

With IT/OT Asset Monitoring, we provide the perfect solution to monitor all critical hardware and software components of your OT environment.

This enables you to prevent downtime and thus boost the availability and reliability of your entire production.

How does it work?

- Asset monitoring by using standard protocols like WMI, SNMP, SSH, OPC UA, HTTPS and many more (an asset can be a hardware or software component).
- Get notified via email, SMS/pager, OPC UA.
- Create new value by combining acquired information, e.g. health status of all hard disks.
- Share all your data with your OT environment for monitoring and alerting purpose.
- Monitor many production sites even across continental borders. Ask our experts!
- Get creative visualizing your IT/OT environment with the map functionality of PRTG.



Deliverables

IT/OT Asset Monitoring based on PRTG

Software licenses and services

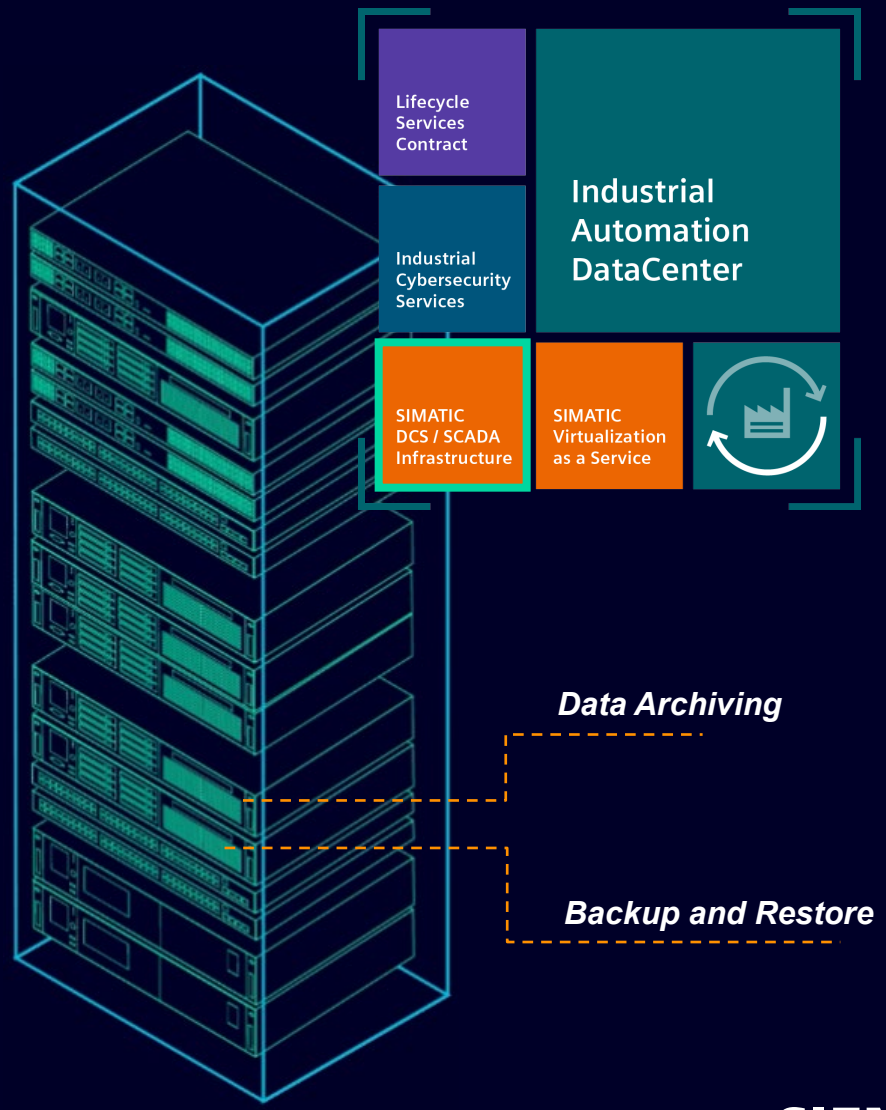
- Available in batches of 500, 1.000, 2000, 5.000, 10.000 asset sensors
- Including a half-day start-up consulting for commissioning and implementation
- Technical support for 3 or 5 years
- Software maintenance for 3 or 5 years
- Implementation and commissioning services (optional)

SIEMENS

SIMATIC DCS / SCADA Infrastructure
as part of the Industrial Automation DataCenter

The **Industrial Automation DataCenter** is an individually 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.

- All important core elements of a data center are included: high performance computing (with high availability), IT/OT networks, uninterruptable power supply and IEC 62443 compliant security architecture, ***back-up and disaster recovery*** and ***process data archiving***
- 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-convergent IT infrastructure for industrial environments.



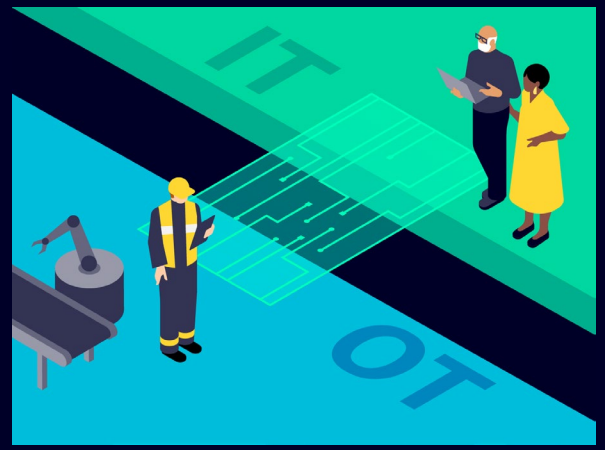
SIEMENS

Why not profiting from the industrial digitalization age and get Siemens on board for your IT/OT infrastructure?

Managed IT/OT Infrastructure

- includes a ready-to-run high-available IT infrastructure for OT environments.
- meets sustainability goals and the latest cybersecurity requirements.
- ensures operational continuity through remote management and monitoring by IT/OT experts.

➢ **bridges the gap between IT and OT.**

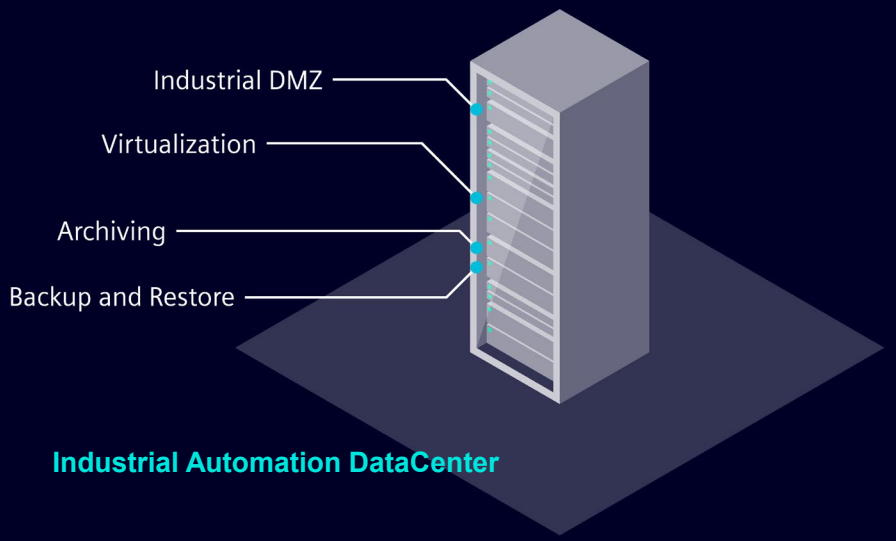


The perfect symbiosis of hardware, software and services

Secure data exchange between IT and OT based on IEC 62443 with industrial DMZ infrastructure

Future-proof modernization of control systems with a pre-configured virtualization platform

Pre-configured IT infrastructure for optimized data handling:
- Archiving
- Backup and Restore



Industrial Automation DataCenter

+

Remote monitoring and management of your IT/OT infrastructure by IT/OT experts through the entire life cycle

SIEMENS

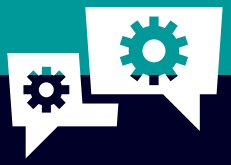
Siemens as reliable partner for IT infrastructure in OT environments

We are the automation experts

We drive digitalization

We understand industrial security

We have specific industry know-how

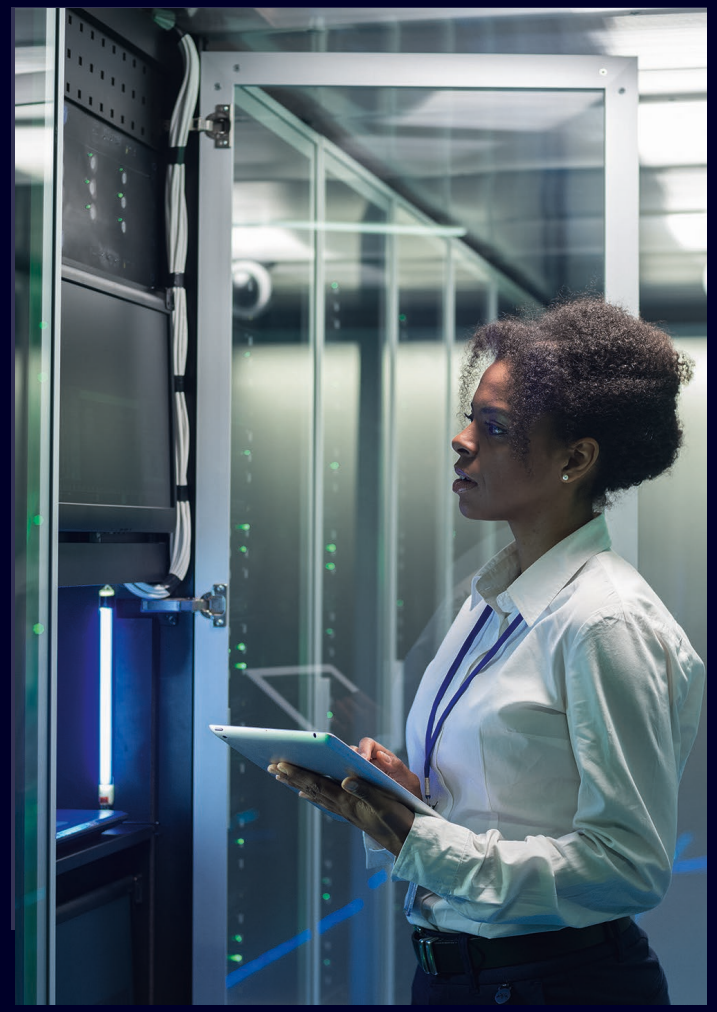


We offer state-of-the-art technology and end-to-end services from a single source

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

SIEMENS

Why should you choose SIMATIC DCS / SCADA Infrastructure?
Backup and Restore – Disaster Recovery



Increased availability thanks to fast disaster recovery and prevented data loss

Compliance with cybersecurity regulations (e.g. NIS 2) and **improved plant data security** in case of ransomware incidents

Ready-to-run infrastructure with system-tested, pre-configured components and 100% lifecycle services from a **single source**

SIEMENS

MP Hygiène, Davézieux, France
Full IT/OT Infrastructure with Industrial Automation DataCenter

Customer profile	MP Hygiène is France's leading manufacturer of pure cotton wiping paper with the Origine France Garantie® label, and also manufactures non-woven wipes, soaps and hand hygiene solutions. 56,700 m² of buildings on 4 sites and 12 production lines. https://www.mphygiene.com/en/accueil-english/
Customer objectives	As part of their industrial process, the customer wanted a virtualized infrastructure and strong cybersecurity packaged by Siemens
Siemens Solution / service Description	**Industrial Automation DataCenter – SIVaaS and SIDSI** • Redundant SIMATIC Virtualization as a Service (SIVaaS) and SIMATIC DCS / SCADA Infrastructure (SIDSI) / back up and restore solutions in the same infrastructure • Scalance based virtual network architecture including DMZ • Turnkey PCS7 migration • Technical support from a Siemens paper industry expert throughout the project
Customer Benefits	• A pre-configured redundant Siemens virtualized infrastructure ready to host the migration of its PCS7 project • A powerful backup and recovery solution and a security-oriented network to prevent cyber attacks • A service contract included with the infrastructure • Virtualized Resources, Less Hardware, Energy Savings, Obsolescence and Cybersecurity Management
Why Siemens?	• Siemens offers turnkey solutions for virtualized HW-based migration • Siemens combines IT & OT solutions • Siemens has a wide range of track records in the paper industry

MPH1865

Reference ID: 37510

SIEMENS

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

You want to find out more?

Here you can find more information:
www.siemens.com/sidsi
or contact the Siemens partner near you
Siemens Contact Database

SIEMENS

Disclaimer

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.

SIEMENS

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

SIEMENS