

# DCS Modernization à la carte with Upgrade Factory



**“Innovation is change that  
unlocks new value.”**

**Jamie Notter**

Published author and business consultant

# Megatrends raise the need for efficiency, flexibility and more security

## DISRUPTIVE CHANGES



The rise of new technologies, climatic and demographic change are current megatrends which are changing values of our society and influencing consumer behavior.

## CUSTOMER EXPECTATIONS



Customers expect manufacturers to produce tailored goods on demand and just-in-time.

## CYBERCRIME



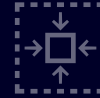
Increasing network of machines and industrial plants increase the risk of cyber-attacks.

# Your dilemma

Your  
**challenges ...**



Faster time-  
to market



Demographic  
changes



New  
technologies



Cybercrime

**While ...**



Meet your  
production plan  
to stay efficient



Being flexible to  
meet customers'  
expectations



Continuously  
improve  
cybersecurity

Megatrends raise the need for mass customization, flexibility and more security

MEGATRENDS

CUSTOMER EXPECTATIONS

CYBERSECURITY

**Gain maximum efficiency, flexibility and security with the timely modernization of your system.**

The rise of new technologies, climatic and demographic change are current megatrends which are changing values of our society and influencing consumer behavior

Customers expect manufacturers to produce tailored goods on demand and just-in-time

Increasing network of machines and industrial plants increase the risk of cyber-attacks

# Manufacturers know the benefits of a future-oriented system/plant in theory ...

## Efficiency

Maximum efficiency



Avoiding unwanted downtime



## Flexibility

Individual Upgrade



Industry 4.0



## Security

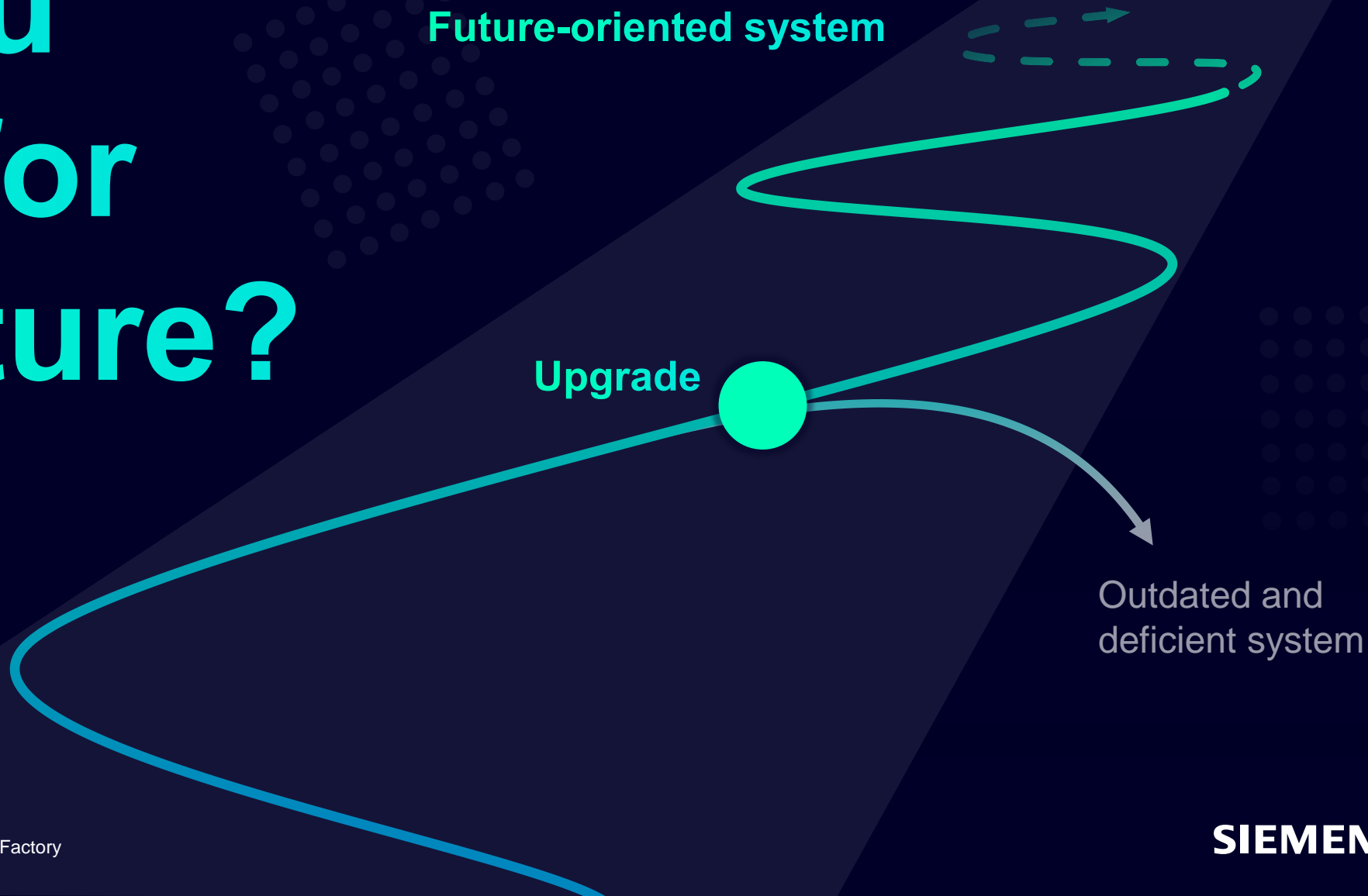
Up-to-date security standards



Plant availability



# Are you ready for the future?



# But what happens when components become obsolete and are not replaced in time?

Unplanned downtimes cause **production line shutdowns**

---

**Accidents** and personnel **injuries**

---

Unplanned and increased costs resulting in a **reduction of the annual production volume**

---

Growing **shortage of qualified workers**

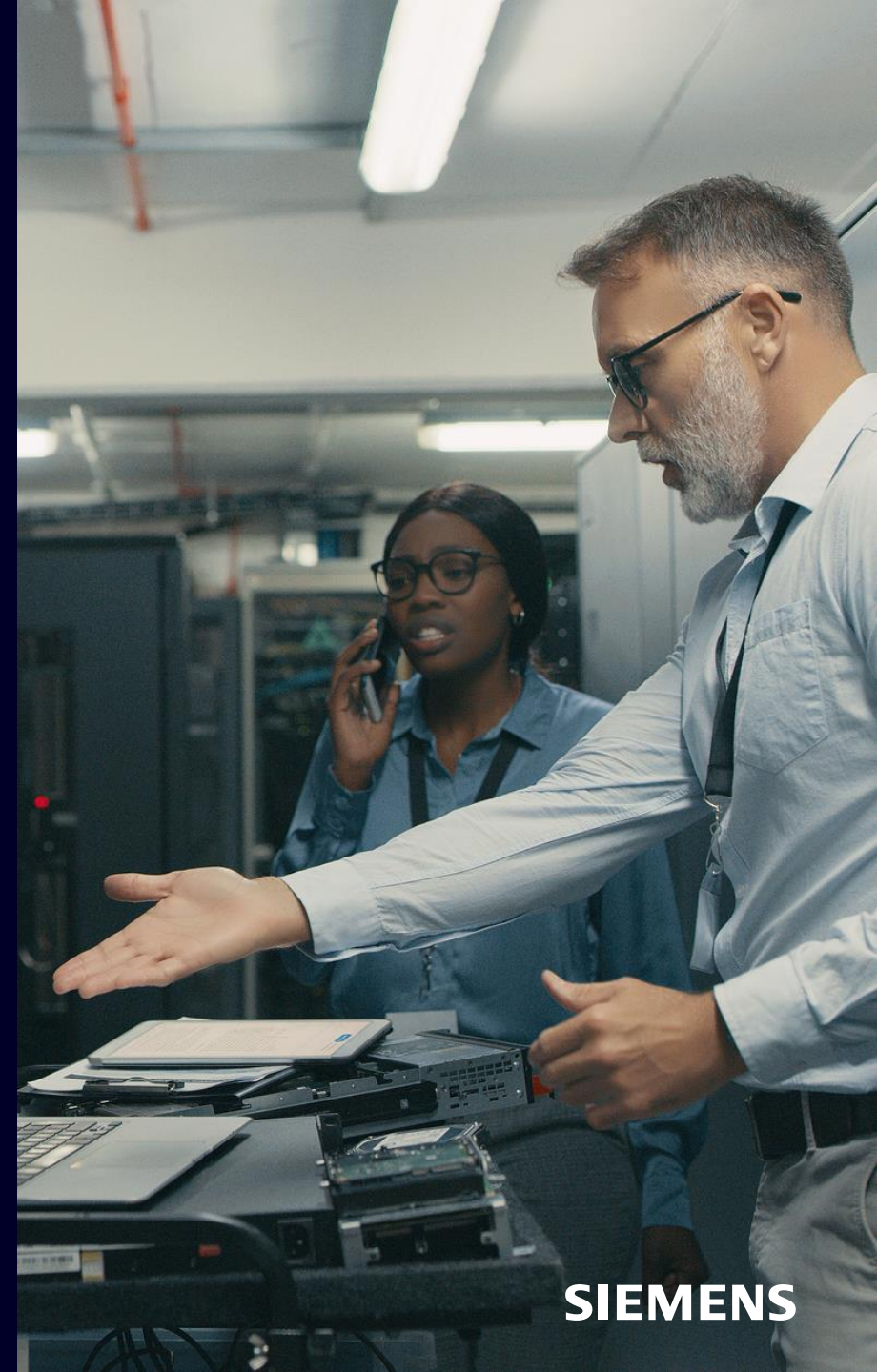
---

**Personnel difficulties** and unscheduled trainings

---

**Increased risk of cyber-attacks**

---



**SIEMENS**

**€ ~70.450**

per year cost for a company in the manufacturing industry for

**unplanned downtimes**

because of obsolete components or systems.

Source: Sewtec Automation, Why obsolescence is not the end for your automation system, 2019

**Outdated equipment don't meet the latest safety standards**

**Safety standards change and replacement parts do not perform as well**



**Lead to accidents and personnel injuries**

## **Consequence**

Accidents lead to failure of machines and staff

Enormous costs



## Better management of shutdowns and turnarounds ...

... can yield schedule and cost improvements of up to ...

# 30%

The teams managing STO (shutdowns, turnarounds, and outages) events at top-performing companies aim to maximize the overall value of turnarounds by **continuously optimizing across four areas**

The cost of the turnaround event

The duration of lost production during the event

The reliability of the plant after the event

The interval between events

Source: McKinsey & Company, the upside of downtime, 2016

## Consequence

For energy and materials players, outages typically consume between a 1/3 and 1/2 of the overall maintenance budget and can reduce annual production volume by **5 to 10%**.



## Manufacturers have difficulties to find experts who can support the old systems

Most skilled workers are retiring soon. Young operators are trained on recent systems.

**Outdated systems are no longer supported in universities and training centers.**



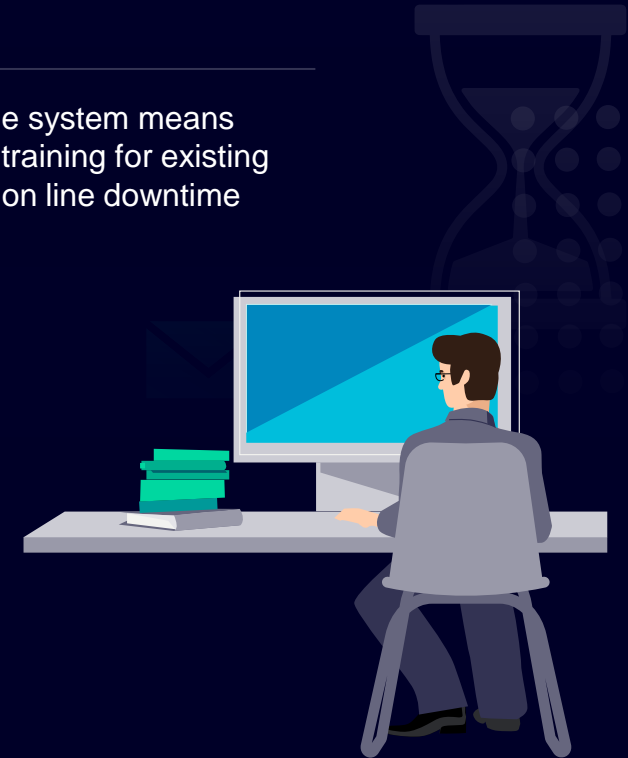
**New employees** cannot handle the old systems **and must first be trained.** Existing staff must be trained for the new technology in advance to avoid downtime in the event of an unplanned upgrade.

## Consequence

Extensive operator training

Employee absence

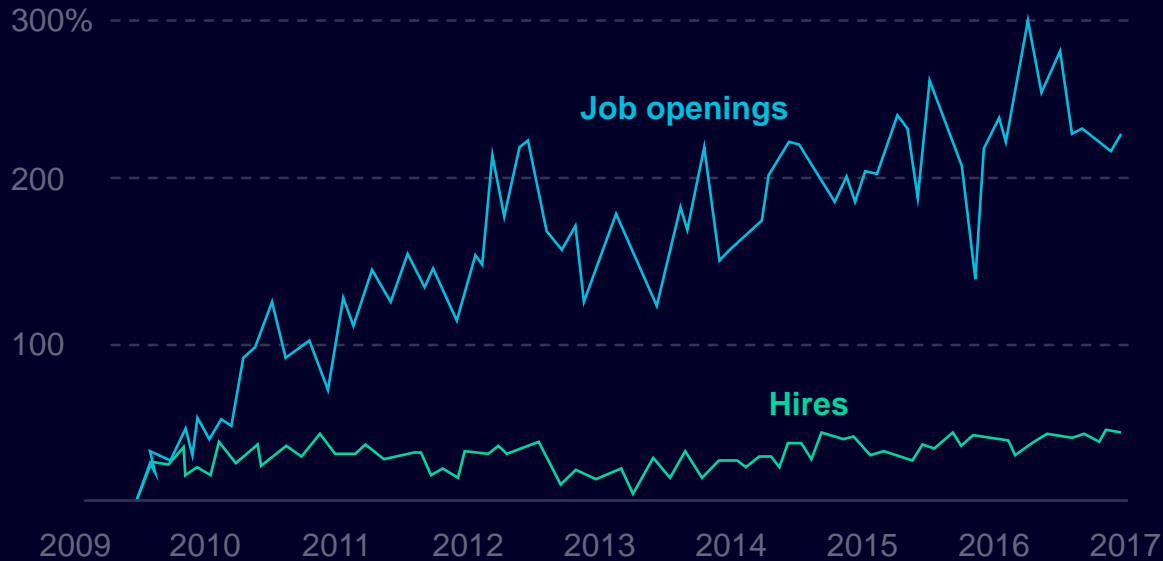
Unplanned replace of the system means also extensive operator training for existing employees and production line downtime



## Skilled labor is hard to find nowadays

### The Growing Shortage of Skilled Manufacturing Workers

Percentage change in U.S. manufacturing job openings and hires, seasonally adjusted



Source: [Harvard Business Review](#) | [1 Deloitte](#)

“... **3.5 million** manufacturing jobs will be available over the next decade in the US, 2 million of which will go unfilled.”<sup>1</sup>

## Lack of expertise in IT and cybersecurity for OT environments ...

... leads to an inadequate protection of the asset



## Increased risk of cyber-attacks

Attacks on the oil and gas sector increased by 1,6

In 2020 the percentage of industrial control systems on which malicious assets were blocked decreased by 6,6 %

A leading security company blocked 19,700 malware modifications from 4,119 groups on industrial automation systems.

Source: McKinsey & Company, Strengthening the IT security posture in corporates and industrials, 2021

## Consequence

Disruption

Unplanned downtimes

Data theft and extortion

Sabotage and product harm

Significant financial loss and reputational damage



# Untimely or no modernization of the plant leads to many difficulties in the entire production chain

## Unplanned downtimes/ accidents



Unplanned downtimes caused by obsolete or damaged assets increase the risk of accidents and injury to personnel.

## Unplanned and increased expenses



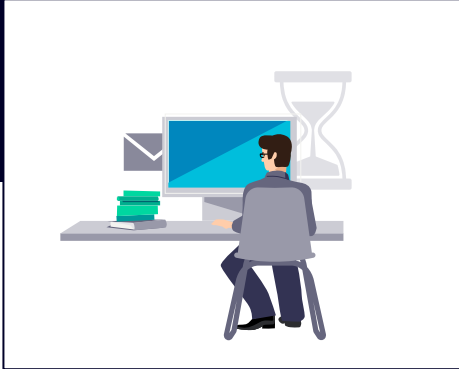
Unexpected downtimes typically consume between 1/3 to half of the total maintenance budget and can reduce annual production volume by up to 10%.

## Personnel difficulties and unscheduled trainings



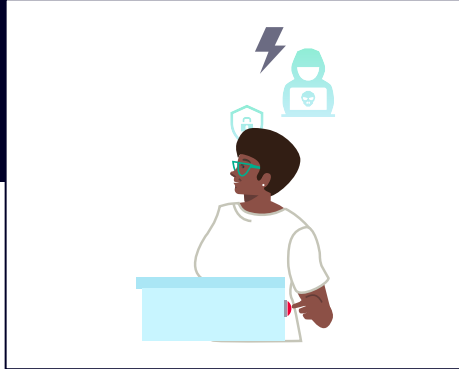
Unplanned system upgrades mean extensive operator training and production line downtime and must therefore be planned and prepared in good time.

## Growing shortage of qualified workers



The demand of skilled workers will increase as well as the difficulties of hiring them.

## Increased risk of cyber-attacks



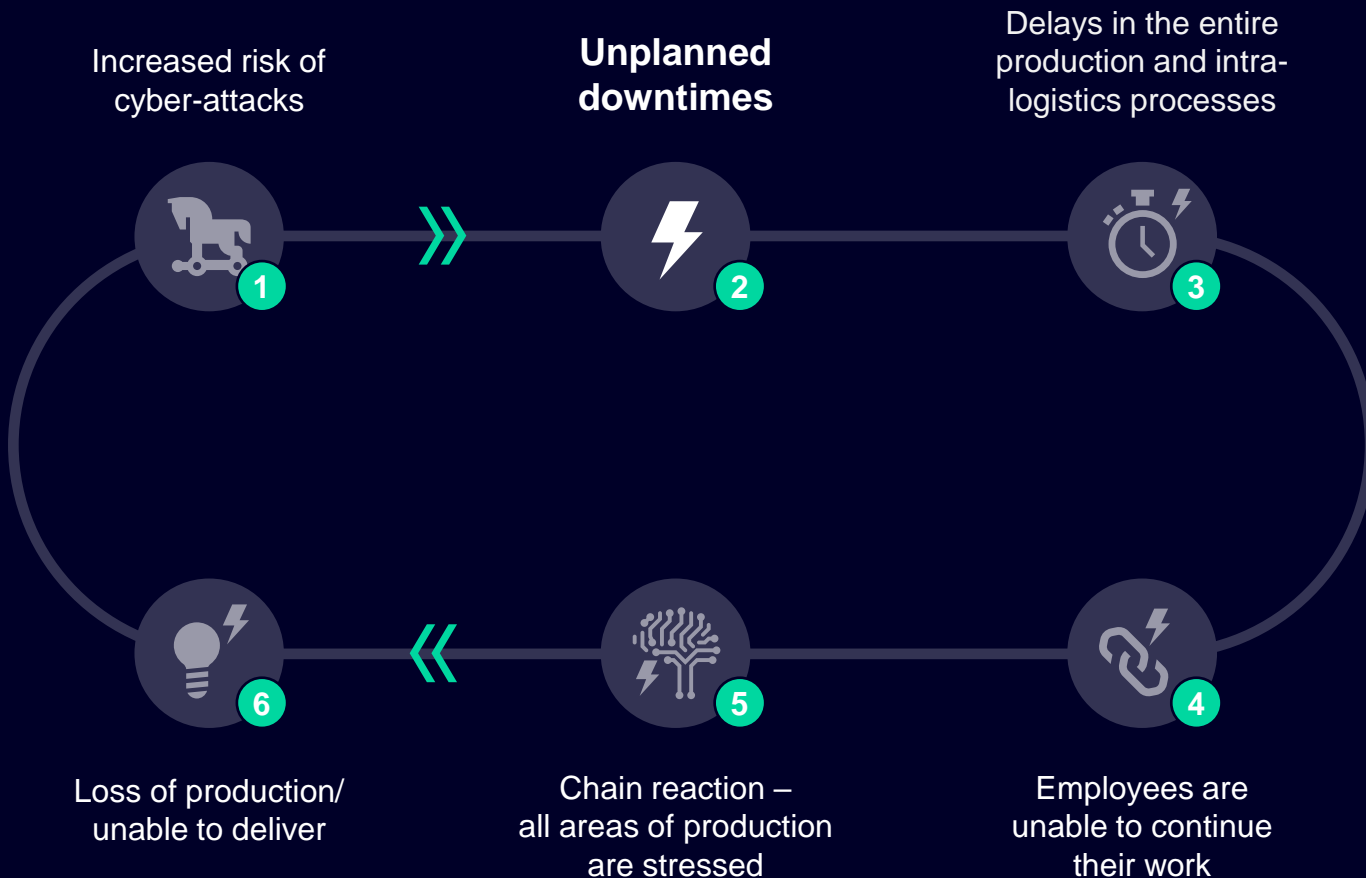
The lack of expertise in IT/OT cybersecurity leads to a lack of transparency about potential risks and inadequate protection of the assets.



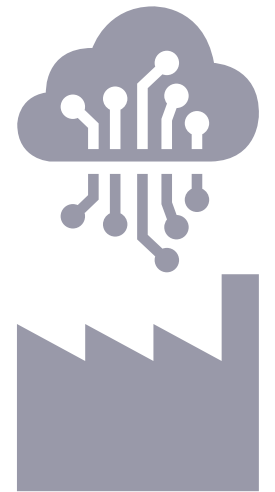
“What new technology does is  
**create new opportunities**  
to do a job that customers want done.”

Tim O'Reilly

# Imagine the impact of unplanned downtimes for your efficiency, flexibility and security



Zero unplanned downtime is now the **No. 1 priority** or a high priority **for 72%** of organizations



Source: <https://www.intechww.com/some-interesting-statistics-about-unplanned-downtime/>

## You need a partner who ...



An original manufacturer who combines security and automation know-how



Offers long-term lifecycle service contracts with third parties' systems



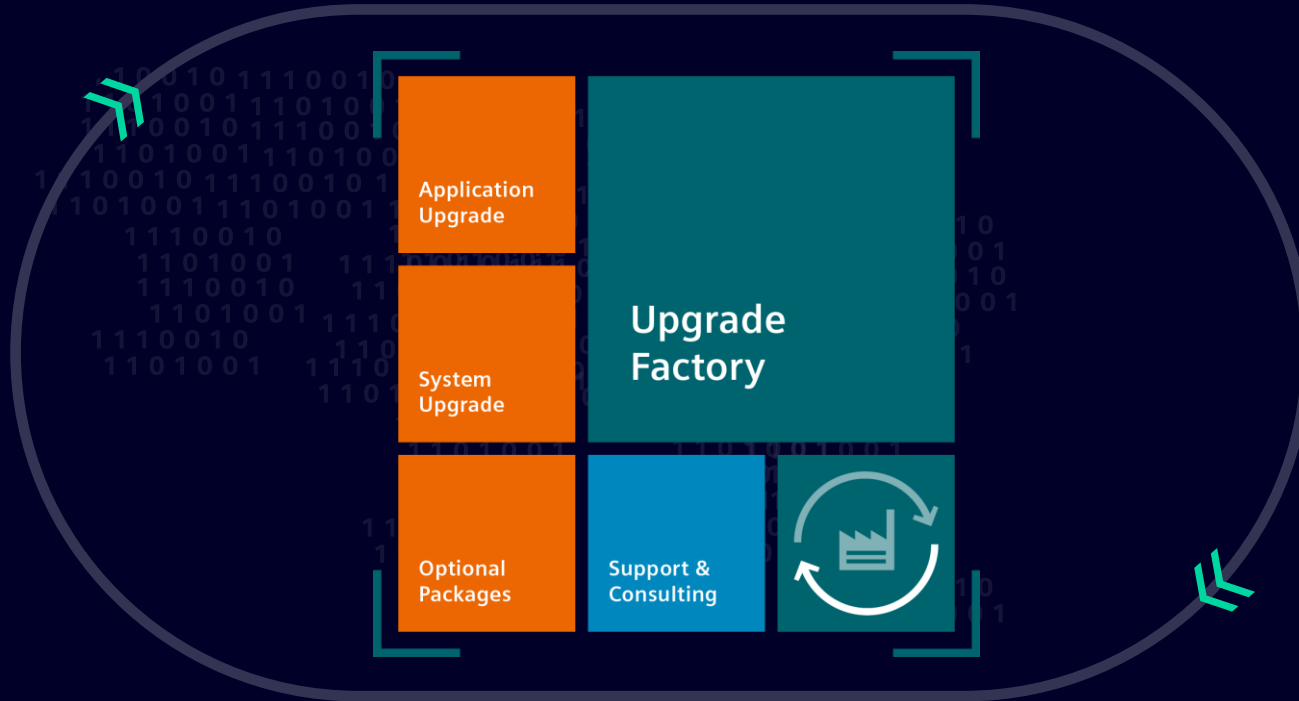
Provides pre-configured and tested state-of-the-art components for SW and HW



Offers turn-key solution incl. commissioning and SAT (site acceptance)

... offers DCS modernization à la carte to **help you meet your market** requirements and customer needs while ensuring security standards

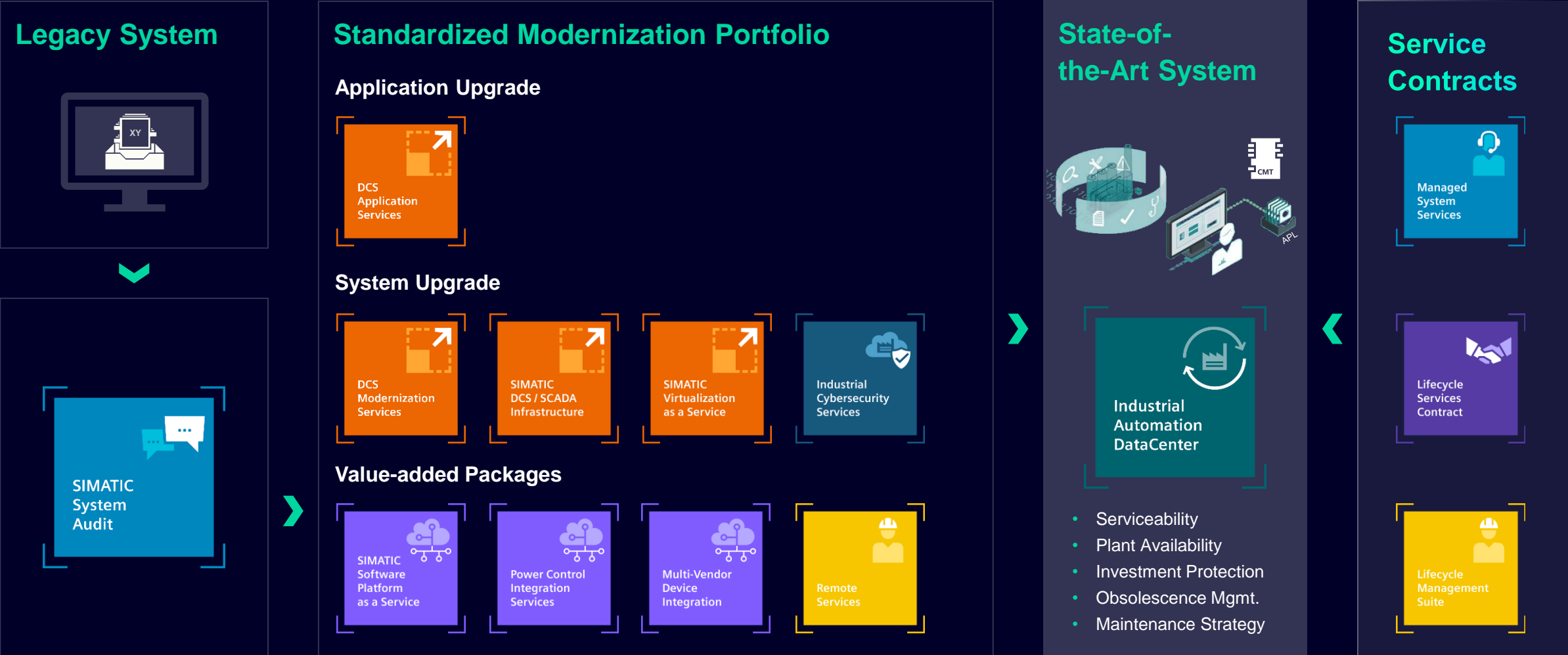
**Always be up-to-date with your factory  
with a holistic and customized upgrade approach**



Upgrade Factory offers DCS modernization à la carte to help you meet your market requirements and customer needs

**A trusted partner  
and advisor for  
state-of-the-art  
technologies and  
end-to-end  
services from a  
single source**

# Always keep your plant up-to-date with a holistic and customized upgrade approach



# Addressing your challenges with Siemens as a trusted partner



Faster time-to market



- SIPaaS (engineering before delivery)
- DCS Application Services (less engineering costs)
- DCS Modernization Services



Demographic changes



- SIVaaS
- MVDI
- PCIS (Reduction of HW & maintenance costs)



New technologies



- SIVaaS (Less Hardware)
- Remote Services (SIPIX)
- SIPaaS (Cloud based engineering)



Cybercrime



- Industrial Cybersecurity Services
- Managed Security (Assessment, Implementation, Monitoring)

# Tratolixo waste plant, Portugal

## Higher reliability level with DCS Modernization Services

<b>Customer profile</b>	<ul style="list-style-type: none"><li>• <a href="#">Tratolixo</a> is a certified intermunicipal company, 100% owned by - Association of Municipalities of Cascais, Mafra, Oeiras and Sintra for the Treatment of Solid Waste and responsible for the treatment of Urban Waste produced by more than 800,000 inhabitants this Urban Waste Management System. Transform Urban Waste in recyclable products - which are sent to valorization - electric and composite energy result.</li></ul>
<b>Customer objectives</b>	<ul style="list-style-type: none"><li>• Tratolixo was searching for a partner to upgrade their existing SIMATIC PCS7 V7.1 (discontinued) to the current version V9.0. In order to avoid future technical support and system compatibility difficulties for these SIMATIC PCS7 equipment, several on-site visits from Siemens Service experts have already occurred. There are damaged components and Microsoft Windows XP operating system is obsolete.</li></ul>
<b>Siemens solution</b>	<ul style="list-style-type: none"><li>• Siemens provided a suitable upgrade solution based on the DCS Modernization Services portfolio:</li><li>• Installation of new PCs / Servers with PCS7 V9.0 software and licenses</li><li>• Conversion of software applications from the existing version PCS7 V7.1 to version V9.0</li><li>• Update of automation software and supervision system</li></ul>
<b>Customer value</b>	<ul style="list-style-type: none"><li>• Higher level of reliability and software development based on an state-of-the-art system</li><li>• PCS directly from the manufacturer guarantees the authenticity of licenses</li></ul>
<b>Why Siemens?</b>	<ul style="list-style-type: none"><li>• All SIMATIC PCS 7 Services from a single source, including clearly defined responsibilities and long-standing modernization know-how from analysis via PCS 7 upgrades.</li><li>• Innovative through the use of current and future DCS technologies with simultaneous reduction of the maintenance costs by using state-of-the-art systems.</li></ul>

Reference ID: [24109](#)



# Evonik Industries AG, Germany

## Chemie, SIMATIC PCS 7 - Danfoss FC300 Integration with MVDI

<b>Customer profile</b>	<p>Over an area of 40 hectares, some 1,200 employees in the Advanced Intermediates and Inorganic Materials Business Units produce raw materials for various applications. Production includes silanes, fillers, matting agents, bleaching and oxidizing agents, and detergent raw materials, from which our industrial customers manufacture detergents, solar cells, paints and coatings, building protection materials, adhesives, sealing compounds, silicone rubber, paper, and textiles.</p> <p><a href="http://www.evonik.com">www.evonik.com</a></p>
<b>Customer objectives</b>	<p>In a plant upgrade, several Danfoss FC300 inverters need to be integrated into SIMATIC PCS 7 in the production environment. The integration should be based on a proven standard solution that offers full system conformity.</p>
<b>Siemens solution</b>	<p><b>MVDI- Multi Vendor Device Integration</b></p> <ul style="list-style-type: none"><li>• Consulting regarding 3<sup>rd</sup> party integration</li><li>• Delivery of driver module libraries</li><li>• System-compliant integration of the 3<sup>rd</sup> party inverter into PCS 7</li><li>• 5-year service agreement for technical questions and free updates</li><li>• Library can be combined with Siemens LCS</li></ul>
<b>Customer value</b>	<ul style="list-style-type: none"><li>• Use of a proven product from the hand of the long-standing system supplier SIEMENS</li><li>• System-compliant and seamless integration of 3<sup>rd</sup> party hardware into SIMATIC PCS 7</li></ul>
<b>Why Siemens?</b>	<ul style="list-style-type: none"><li>• Existing plant with SIMATIC PCS 7 supported by Siemens RC-DE, since many years</li><li>• In the past, the customer had already integrated 3<sup>rd</sup> party devices via drivers into SIMATIC PCS 7</li></ul>

Reference ID: ???



# Stadtwerke Flensburg plant, Germany

## Power Control Integration Services connect two worlds

<b>Customer profile</b>	<a href="http://www.stadtwerke-flensburg.de">www.stadtwerke-flensburg.de</a> is a utility company of the city of Flensburg, Business divisions electricity district heating, drinking water, industrial gas supply and telecommunications
<b>Customer Objectives</b>	<p>The customer reached out to Siemens for a modernization of their plant since the PCS 7 control system was already successfully implemented. Customer would like to purchase additional services from Siemens such as</p> <ul style="list-style-type: none"><li>• Integration of the medium-voltage system in PCS 7</li><li>• One control system for both systems</li><li>• High-availability system was important</li><li>• No external expertise required for the heavy-current side</li><li>• Use own existing PCS 7 expertise</li></ul>
<b>Siemens Solution</b>	<p><b>SIMATIC PCS 7 Station Gateway</b></p> <ul style="list-style-type: none"><li>• Integration of an existing SIPROTEC medium-voltage switchgear with IEC61850-capable field devices in SIMATIC PCS 7 via Station Gateway</li><li>• Use of a control system for joint monitoring and control of the process and the switchgear</li></ul>
<b>Customer value</b>	<ul style="list-style-type: none"><li>• The switchgear is integrated into PCS 7 AS/OS. Uniform control system for automation and switchgear</li><li>• Customer-specific adaptations for the display ability of fast trip signals</li><li>• High-availability connection between the PCS 7 control system and the heavy-current side</li></ul>
<b>Why Siemens?</b>	<ul style="list-style-type: none"><li>• The PCS 7 control system was already successfully implemented</li><li>• Standardized project handling according to the PCS 7 project planning guidelines</li><li>• The station gateway was easy to integrate into the existing plant</li></ul>

Reference ID: [24111](#)



# BMW Group, Germany

## Protection against malware thanks to whitelisting implementation by experts

<b>Customer profile</b>	<ul style="list-style-type: none"><li>With 31 production and assembly plants in 15 countries, as well as a global sales network, the <a href="#">BMW Group</a> is the world's leading premium manufacturer of automobiles and motorcycles, and a provider of premium financial and mobility services.</li></ul>
<b>Customer objectives</b>	<ul style="list-style-type: none"><li>The need for maximum availability and the heterogeneous deployment of software in the automation environment makes the use of anti-malware software a challenge. A partner with experience in the development and implementation of the solution should provide support.</li></ul>
<b>Siemens solution</b>	<p><b>Endpoint Protection: Application Whitelisting</b></p> <ul style="list-style-type: none"><li>Consulting and development of a method for implementing a suitable anti-malware software, including successful Proof of Concept at the Regensburg plant.</li><li>Development and implementation of whitelisting guidelines on the shop floor for 50,000 machines in all vehicle, engine and component plants.</li><li>The whitelisting solution deployed allows only pre-defined trusted applications to run, protecting both current and legacy operating systems from known and unknown threats.</li><li>Support during rollout as well as during operation.</li></ul>
<b>Customer value</b>	<ul style="list-style-type: none"><li>Protection against malware thanks to customized whitelisting solution.</li><li>Convenient operation and administration through central management system.</li><li>Time and resource savings thanks to professional planning and processing by experienced Siemens security experts.</li></ul>
<b>Why Siemens?</b>	<ul style="list-style-type: none"><li>Siemens impressed the customer with its wide range of experience in customizing industrial security, developing policies, and rolling out solutions in OT environments.</li><li>In addition, an excellent customer relationship already exists with the BMW Group, based on very positive experiences in the past.</li></ul>

Referenz ID: [23763](#)



# Bayer CropScience plants, Germany

## Digital transformation of the production plants

<b>Customer profile</b>	<ul style="list-style-type: none"><li>• Around 2000 different chemical products are manufactured at Chempark in Dormagen.</li><li>• The production focuses on the development and manufacture of crop protection products, polymers, plastics and rubber.</li></ul>
<b>Customer objectives</b>	<ul style="list-style-type: none"><li>• As a result of the a modernization project at Bayer CropScience in Dormagen, several production plants were identified to which need to be upgraded to the latest requirements of a digital company.</li><li>• All necessary supplies and services which need to be be designed, offered, implemented and provided should come from a single source.</li></ul>
<b>Siemens solution</b>	<ul style="list-style-type: none"><li>• As part of the modernization for the seven production plants, Siemens Service experts equipped each of the plant with the <b>Industrial Automation DataCenter</b>.</li><li>• The Industrial Automation DataCenter is an individually configurable, local cloud solution for a plant (on-premise).</li><li>• It uses virtualization to integrate a wide range of applications on a common hardware platform.</li><li>• Various hardware variants enable individual scaling of the data center including all necessary lifecycle services. The offer is rounded off by systems and functions for data archiving, backup and restore, IT security and increased availability.</li><li>• 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.</li></ul>
<b>Customer value</b>	<ul style="list-style-type: none"><li>• Up to 80% less space required due to a standardized overall system with the aim of reducing the number of communication interfaces</li><li>• Flexible system expansion through preconfigured and ready-to-use individual components</li><li>• Up to 75% energy savings due to optimized use of the IT resources deployed</li><li>• Essential IT security measures required by Bayer CropScience AG were already implemented upon delivery</li></ul>
<b>Why Siemens?</b>	<ul style="list-style-type: none"><li>• Implementation of an innovative control technology concept as part of a comprehensive Industry 4.0 project</li><li>• Holistic concept from consulting, implementation and subsequent testing to optimization and long-term support (lifecycle services for all installed components directly from the manufacturer)</li></ul>

Reference ID: [22382](#)



# Dow Middle East - Kingdom of Saudi Arabia

## Securing PCS 7 with Implementation of McAfee Antivirus and Application Whitelisting

<b>Customer profile</b>	<ul style="list-style-type: none"><li>• The Dow Chemical Company (TDCC) is a leader in specialty chemicals delivering products and solutions to markets such as electronics, water, packaging, energy, and coatings.</li><li>• TDCC via subsidiaries has been present in the Middle East for more than 50 years and delivering a broad range of technologies to their local customers across many industries, including water, energy, packaging, building and construction.</li></ul>
<b>Customer Objectives</b>	<ul style="list-style-type: none"><li>• Need for protection of the PCS 7 systems (Engineering and Client stations) and the associated database used globally for analysis and R&amp;D against incoming cyber threats aligned to cyber standards and legislation</li><li>• Distributed systems demanding a central administration console for managing security measures</li></ul>
<b>Siemens Solution</b>	<ul style="list-style-type: none"><li>• Deployment of a central management server to distribute and manage approved Antivirus and Whitelisting software from Siemens strategic security partner McAfee</li><li>• Installation of server on Siemens IPC 547E</li><li>• Rollout of Antivirus and Whitelisting for broad endpoint protection on PCS 7 systems</li></ul>
<b>Customer value</b>	<ul style="list-style-type: none"><li>• Usage of approved security software for PCS 7 minimizing the risk of operational issues in accordance with the Compendium F</li><li>• Standardized policies and installation procedures from Siemens automation experts ensuring fast installation with minimal downtime of the systems.</li><li>• Broad protection from malicious software and programs based on combination of Antivirus and Whitelisting functionality on PCS 7 systems.</li></ul>
<b>Project information</b>	<ul style="list-style-type: none"><li>• Dow Middle East R&amp;D Center KAUST, KSA utilizes state-of-the-art technologies such as reverse osmosis, ultra filtration, energy efficient systems and infrastructure, and roofing systems in the Kingdom and help to solve some of the world's biggest global challenges.</li></ul>

Reference ID: Ref+6891



„The last few years have shown a substantial increase in cyberattacks globally.“

Kamran Hashmi, Middle East R&D center at Dow  
Chemical

# Koehler Paper Group

## Implementation of Risk & Vulnerability Assessments and implementation of security measures at the papermills



<b>Customer profile</b>	<ul style="list-style-type: none"><li>• Koehler Paper Group, headquarters in Oberkirch Baden-Württemberg, paper manufacturer with mills in Oberkirch, Kehl and Greiz</li><li>• Koehler Paper Group employs around 1,800 people</li><li>• Production output of more than 500,000 tons of special paper and cardboard with state-of-the-art technology and an annual turnover of approx., 700 million euros</li></ul>
<b>Customer Objectives</b>	<ul style="list-style-type: none"><li>• Development of a security concept for the papermills and an increase of the security level</li><li>• Basis for further development of the infrastructure towards 4.0 through implementation of a security concept and operation</li><li>• Implementation of the security measures should be carried out without interruption if possible</li></ul>
<b>Siemens Solution</b>	<p><b>Security Assessment and implementation of security measures</b></p> <ul style="list-style-type: none"><li>• Comprehensive consulting and implementation support for cyber security for papermills</li><li>• Support of Siemens, as well as 3<sup>rd</sup> party products and solutions</li><li>• Expansion and segmentation of networks in papermills</li><li>• Implementation of solutions such as Industrial Next Generation Firewall as perimeter protection for papermills</li></ul>
<b>Customer value</b>	<ul style="list-style-type: none"><li>• Koehler Paper Group received a clear, neutral and holistic picture of its level of maturity in terms of digitalization and security status.</li><li>• Through the implementation of technical and organizational security measures, the security level is increased.</li><li>• Subsequently, penetration tests were carried out by a neutral service provider to prove the effectiveness of the measures, which were successful.</li></ul>
<b>Project information</b>	<ul style="list-style-type: none"><li>• Implementations of Risk &amp; Vulnerability Assessment in the papermills Oberkirch and Kehl</li><li>• Subsequent support in implementation of security measures in the factories</li></ul>



Reference ID: Ref+6891

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



## You want to find out more?

Here you can find more information about Upgrade Factory:

[www.siemens.com/upgrade-factory](https://www.siemens.com/upgrade-factory)

or 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.