AUVESY-MDT
We secure the world's automation

NIS2 – Stricter Cyber-security Regulations for Production

Harsh penalties starting in 2024: Is your company compliant?

white paper

PREFERRED octoplant partner
powered by AUVESY-MDT

INTRODUCTION

An overview of actions and solutions for the new EU directive

Ten million euros or two percent of the previous year's turnover: the EU's maximum penalty is designed to persuade major facilities to comply with new cybersecurity standards. Its new cybersecurity directive aims to thwart attacks and minimize damage in order to shield the economy and society against outages.

Its new regulations don't just affect the operators of critical infrastructure; they extend to industry and indirectly increase the security demands faced by any business that could be a target of attacks.

At a glance: how the EU is forcing industry and suppliers to act

- Stricter mandatory, preventative security management and a duty to report security incidents.
- NIS2 affects any enterprise belonging to what it defines as a 'critical' or 'important' sector and providing services or products to people and businesses in the EU—even if the supplier itself is **based outside the EU**, such as in the USA.
- Risks: fines for a breach of the rules can be between seven and ten million euros or up to two percent of annual global turnover, depending on the sector and the severity of the violation.

For operators of critical infrastructure seeking to strengthen their security requirements in compliance with the new EU directive, these recommendations aim to safeguard the economy and society from potential failures and their repercussions.

Background: digitalization and security in OT

By digitizing and automating their infrastructure and production, businesses and organizations can make themselves more efficient and tap into new potential. The transformation of IT and OT (operational technology) has accelerated significantly in recent times, not least on account of the pandemic.

As digitization has progressed over the past few years, attacks on production and infrastructure have intensified. Examples include the targeted manipulation of a drinking water treatment plant in the USA and attacks on parts of the energy grid in Europe.

At the same time, events in recent years have highlighted how profound the impact of disrupted supply chains and compromised basic services can be. The supply of energy and healthcare and the production of important basic materials and intermediate products together represent a major pillar of our society, and every defect, interruption, and disruption can damage society as a whole.

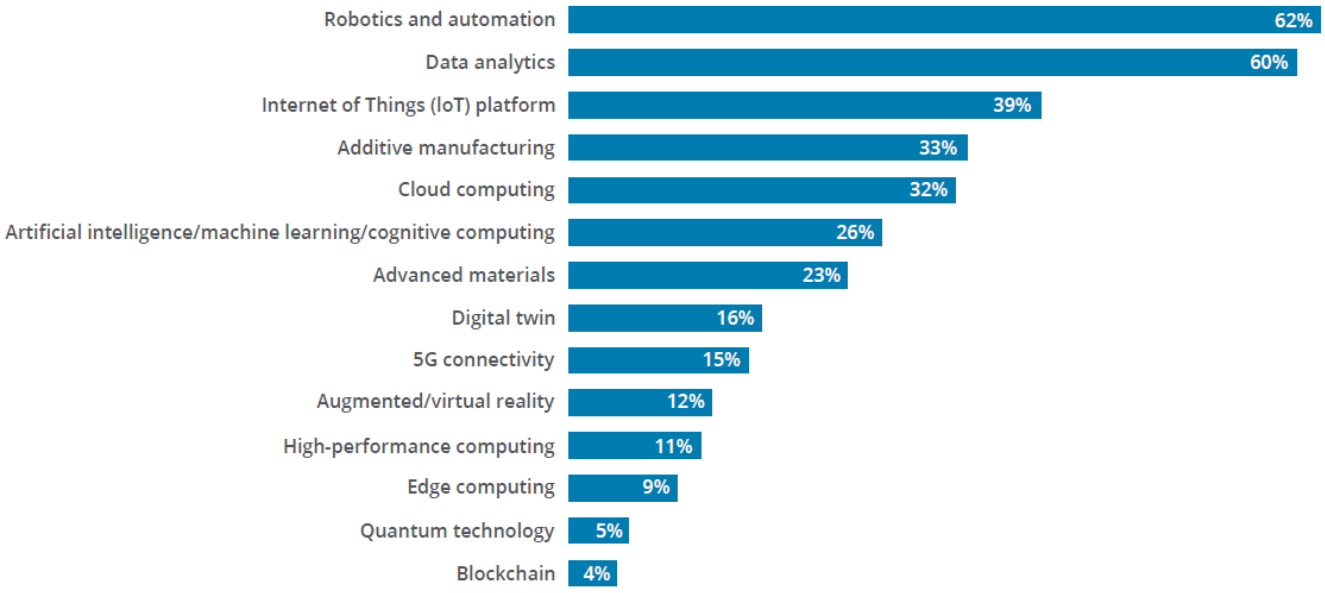
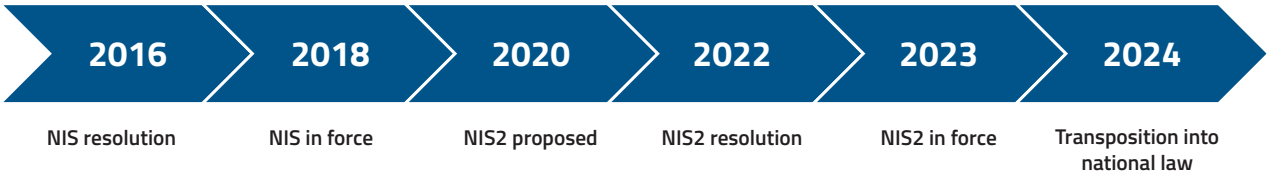


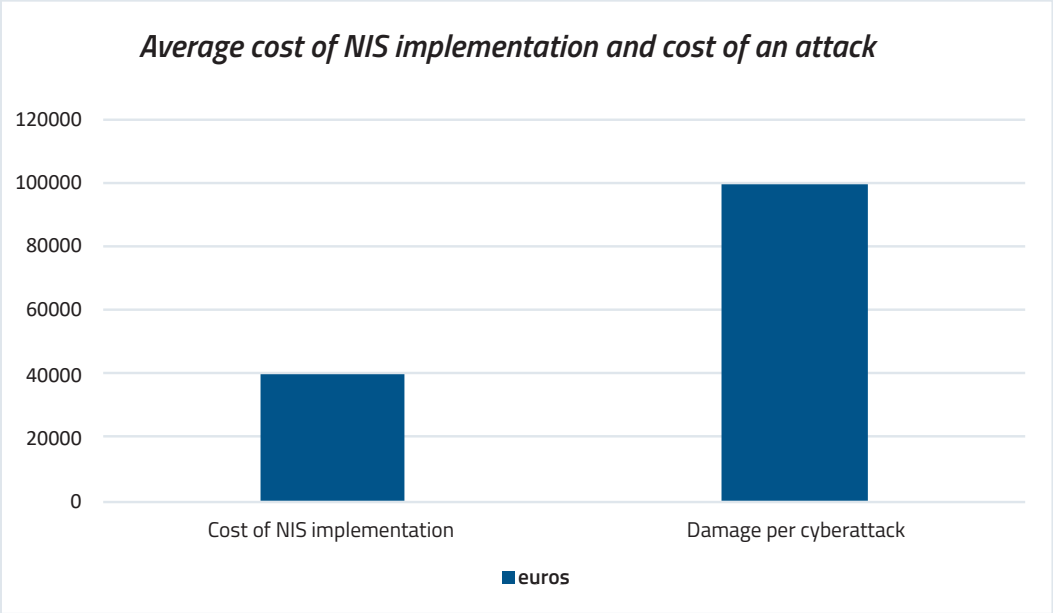
Fig. 1: According to the 2023 Manufacturing Industry Outlook | Deloitte US has shown that companies that embrace a higher level of digitalization demonstrate greater resilience. According to the survey results, their planned digitalization investments for the next 12 months will revolve around leveraging a range of technologies to maximize operational efficiency. Source: 2023 Deloitte manufacturing outlook survey.

NIS and NIS2—the Timeline

The businesses surveyed spent an average of €40,000 on implementing the requirements, while the European Union Agency for Cybersecurity (ENISA) estimates the average cost of an attack at €100,000. In its report entitled The State of Ransomware in Manufacturing and Production 2021, security company Sophos says the average cost of an attack on manufacturing companies specifically is as much as USD 1.5 million.



THREE YEARS AFTER NIS CAME INTO FORCE, ONLY FOUR OUT OF FIVE BUSINESSES HAD MET THE REQUIREMENTS.



Sources: ENISA and Sophos

Under NIS2, serious breaches could result in penalties of up to ten million euros or two percent of a company's global turnover. Under the previous Directive, the penalty for violations was only €150,000. According to EU cybersecurity authority ENISA, just 82% of companies asked had implemented the requirements of NIS by the end of 2021, despite the first version of the Directive having been in force for years.

Two-thirds of them had to allocate an additional budget to implement the Directive. **Half of the companies say the new measures have improved their threat detection** and a quarter that their recovery capabilities have improved as a result. That's a big step in the right direction, but there's still room for improvement, especially in recovery. With greatly increased fines in sight, investments in cybersecurity are now distributed as follows:

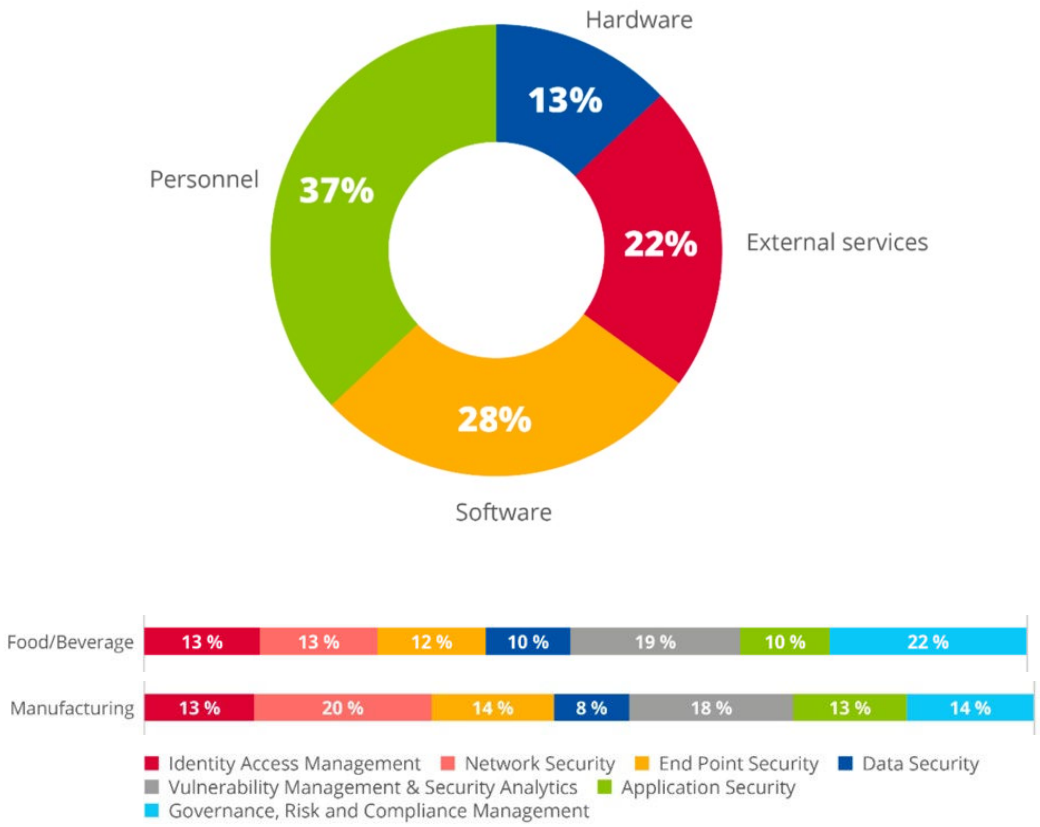


Fig. 2: Distribution of spending and measures for IT security—overall and in different industries.
Source: Gartner, IT Key Metrics Data 202: IT Security Measures

NIS2—Only for KRITIS Companies?

To whom does NIS2 apply in practice? Its definition expands on the previous version's 'critical' infrastructure (NIS) to include 'important' infrastructure, thus encompassing a great many industries. Up until now (i.e., under the first version of the NIS Directive), EU Member States could decide for themselves which industries and companies they classified as critical infrastructure. Now the EU is setting out universally applicable sectors and criteria.

Importance of the sectors

The criteria and sectors are similar to those of Germany's KRITIS regulation, but now the EU Resilience of Critical Entities Directive (RCE) applies. In its definition, the EU distinguishes between 'critical' and 'important' industries and sectors. Eleven industries fall into the 'critical infrastructure' category, another seven are classed as 'important infrastructure'. That's more than under the first NIS Directive in Germany. The regulation addresses every industry in which a failure could pose a risk to public safety or health, or systematic risks. **Manufacturing enterprises** are now counted as 'important entities' under NIS2, which places them in the 'important companies' category. The NIS Directive did not cover the **production** of food or industrial and chemical goods, but **NIS2 impacts it directly.**

Sectors directly affected by NIS2:

Essential sectors	**Subsectors/examples**
Wastewater and drinking water	-
Banks	-
Digital infrastructure	*Providers, data centers, registrars, etc.*
Energy	*Electricity, gas, oil, etc.*
Finance	*Stock exchanges etc.*
Health	*Research, medical devices, healthcare providers, etc.*
IT providers	*Service providers, security providers, etc.*
Aerospace	-
Transport	*Rail, road, etc.*
Administration	*Local to national administration*
Major sectors	**Subsectors/examples**
Waste disposal	
Chemicals	
Digital services	*Social media providers, search engines, etc.*
Food	
Research	
Industry	*Automotives, electricals, computers, mechanical engineering, etc.*
Post	

Fig. 3: Manufacturing industries are now covered by NIS2 and are highlighted here in color

Company size

The EU draws a further distinction relating to the size of companies. Medium-sized (50–250 employees) and larger companies (> 250 employees) are directly affected. Digital infrastructure businesses are all affected, regardless of size. Other exceptions: public entities and providers with a cross-border impact fall within the planned legislation—regardless of size. Federal and Land agencies are now all affected. Legislating Länder can decide for themselves whether regional and local authorities will also be included.

NIS2 no longer affects critical infrastructure alone

Chemicals, food, and industry (including mechanical engineering, transport, automotives, and electricals) are all 'important sectors' under NIS2 and are therefore directly affected by the Directive.

NIS and NIS2 have an impact beyond the industries directly addressed. Firstly, the Directive defines minimum standards and best practices that businesses from non-essential industries have to follow. Not because they're worried about compliance breaches or fines—purely pragmatically. For example, premiums for insurance against business interruption or damage caused by cyberattacks are partially based on the presence of safeguards, the probability of damage, and past incidents.

Furthermore, rising levels of protection in regulated critical industries potentially mean that attackers will turn their attention to other sectors which they consider less protected and thus easier targets. According to Europe's ENISA, only half of companies currently have cyber insurance.

What businesses have to implement

NIS2's specific requirements require critical infrastructure providers to implement effective cybersecurity measures in contexts such as risk management. The Directive makes it especially clear that companies should put structural measures in place. They should assess risks, establish rules, and proceed on that basis or implement solutions. What is required of policymakers is that they establish a culture of security by example, instead of prescribing particular security mechanisms, because solutions alone only help up to a point. To cite one example, in its survey of NIS implementation, security agency ENISA found that businesses overestimate the impact of the mere presence of security solutions while underestimating the actual effectiveness of such solutions as a variable.

HALF OF BUSINESSES SAY THE NEW (NIS) MEASURES HAVE IMPROVED THEIR THREAT DETECTION.

Risk Management and Incident Response in OT

The Directive deals with some cybersecurity aspects and precautions, focusing mainly on two areas: risk management and incident response. These two aspects of cybersecurity are especially relevant for OT executives. Risk management is about identifying vulnerabilities and potential points of attack before someone else does. It also includes assessing potential consequences.

Fig. 4: First steps to achieving NIS2 compliance.

What businesses have to do in practice

NIS2 is now compelling businesses in the manufacturing industry that are not encompassed by the previous KRITIS regulation to implement appropriate rules, processes, and structures, so as to deal systematically with potential security risks. Here's an overview of the fundamentally necessary levels of action.

Management
Executives are responsible for establishing rules and processes and assessing how effective measures are. Cybersecurity is now business-critical, even for non-regulated industries.

Risk management
Companies have to identify, understand, and evaluate risks.

Asset management
All of the components needed to run elementary services have to be covered. This starts with personnel, continues through every device and system, and includes critical data.

Training and personnel
Hire cybersecurity staff, train employees,
and security in recruitment.

Implement protective measures
Establish security processes according to ISO 27001/IEC 62443, such as those described in the Basic IT Protection Profiles.
Implement monitoring, defense, and instant recovery solutions to prevent or minimize failures.

Incident management
Incidents have to be prevented, detected and handled professionally.

Encryption
Communications, data, and systems have to be cryptographically secured.

Suppliers
Supply chains and their potential security risks also have to be recorded, assessed and managed in compliance with the Directive.

Implementing with the aid of data and OT endpoint

management

Important companies are required to prevent outages and, should they occur, minimize their duration. To do this they need effective solutions for their data and backup strategies and must begin by inventorying their endpoints fully.

1. Firstly, businesses need to catalog and monitor all of their assets in production through **asset management**. Every PLC, every automation component, and every machine has to be recorded and monitored digitally. This provides the basis for each subsequent step.
2. Secondly, **versioning** every software status and change (change management) is part of every security strategy. Who made which change? This is also the basis on which to re-store the last functioning state after an error or attack (recovery).
3. **Access control** defines who is allowed to change which data.
4. **Monitoring** every inventoried system reveals every change and deviation from the target state and is crucial when responding to incidents.
5. A **backup strategy** defines which data is stored redundantly, where, and for how long so that a secure copy of every production program and software status can be accessed at any time.

By taking these steps, manufacturing companies can create a basis from which to satisfy all the legal requirements of NIS, KRITIS, and other security laws. Only by digitally recording and monitoring your production and systematically backing up your data can you meet the latest requirements and adapt your processes to even stricter requirements in the future.

How octoplant Can Secure Your Production

octoplant is a modular solution for endpoint and data management in production with which businesses can protect automation devices in production against risks and expensive production outages. It keeps users up to date with the latest technological advancements and allows them to fulfill compliance requirements. octoplant has modules designed around user benefits:

Threat Protection
With octoplant, businesses can monitor their assets and are automatically informed about vulnerabilities and risks. A separate risk score for each asset reveals potential threats. Other preventative features such as change and vulnerability detection actively help to eliminate outages. This makes octoplant an important part of the security architecture in production.

Safeguarding Assets
In complex production environments, versioning multiple projects and their changes can be a laborious task, as well as a critical one. Version management and automatic backups of all versions and changes ensure that the correct version is always running. Differences between data statuses can be displayed as graphics and tables. Automated backups save time, reduce errors, and make the programming and configuration of equipment more reliable.

Device Management
Different kinds of controllers and incompatible manufacturer solutions impede networked automation and can hamper effective security solutions. octoplant integrates all common IoT devices, manages and monitors all of the configuration data associated with different manufacturers, and reveals who made which changes, and when. This makes octoplant the ideal platform for OT data management.

Instant Recovery
If something really serious does happen, instant recovery enables all of the necessary programs and data to be restored to their most recent state in the shortest possible time. This means that octoplant enables individual devices or the entire production facility to be restored to a valid status at any time. It minimizes outages and disruptions and allows errors and manipulations to be reversed.

Compliance einhalten
octoplant offers integrated documentation for compliant processes and compliance management in order to ensure that everyday processes are legally compliant. All of the production processes are then fully traceable in the event of an audit.

USE CASES IN PRODUCTION & WATER SUPPLY

Use case—water supply

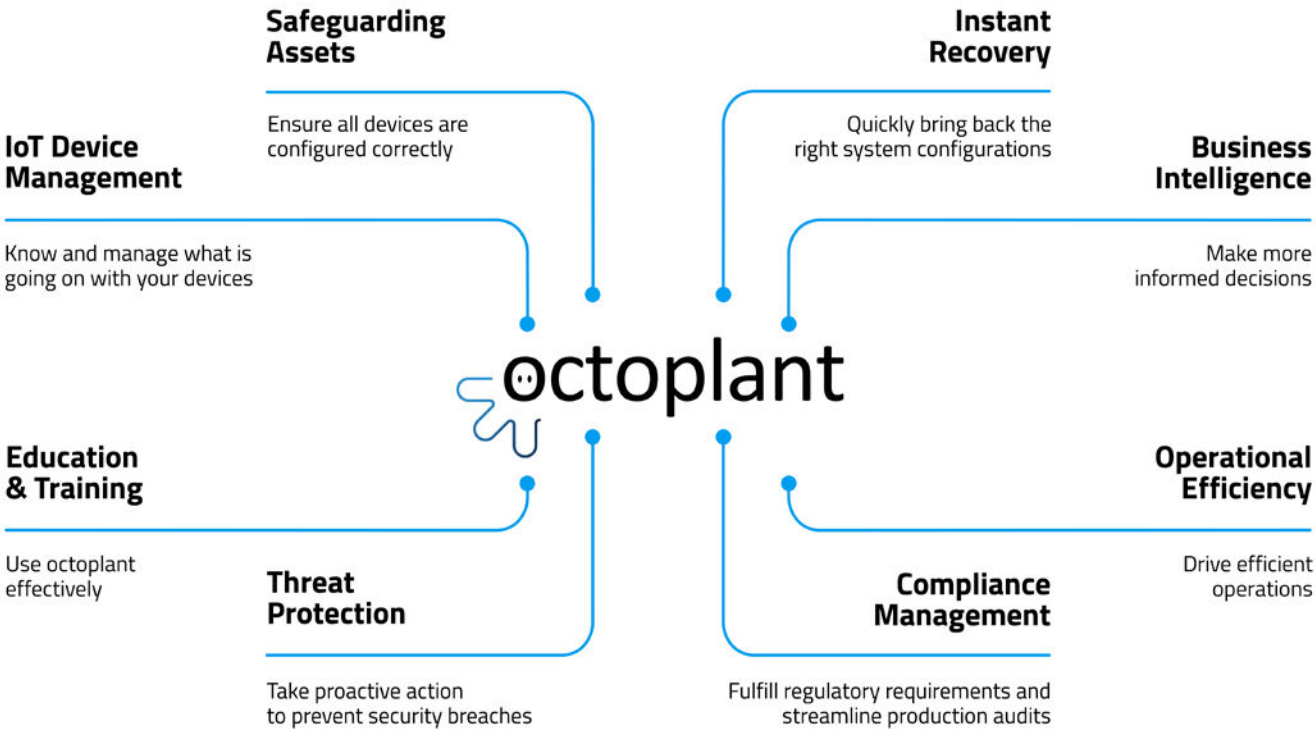
Water is an essential utility and is therefore subject to the KRITIS Regulation, and now the NIS2 Directive as well. Water supplier Canal de Isabel II is the Madrid region's central water utility. The 600 monitoring stations and 250,000 measurement variables belonging to all of its water plants had to be consolidated into one unified monitoring system. This platform displays status information belonging to the stations, the processes, and the equipment in real time. AUVESY-MDT's data and endpoint management safeguards this system network, managing backups and restoring previous versions of monitored equipment.

Canal de Isabel II, Spaine

Use case—production

Nanostone: ceramic membrane filters for water treatment, manufactured at an increasingly automated production plant in Germany. The products are used for desalination, industry, and the public water supply. The production of these ceramic filters is highly critical. Nanostone uses numerous different Siemens PLCs for its various production processes. Robots, CNC machines, lasers, and transport in manufacturing. AUVESY-MDT has been used for access control and versioning since 2018. Its data and endpoint management administrates file versions, makes changes transparent, and safeguards production. Access is given to internal C&I automation and maintenance, and an external service provider. This allows the company to track any changes made to versions and recipes. All of their documentation is located in a dedicated folder which provides a central location for current documentation. Implementing AUVESY-MDT was "surprisingly" fast and smooth.

Nanostone Water GmbH, Germany



Conclusion: Secure, Legally Compliant Production with octoplant

octoplant enables company managers to monitor and control the entire production process using one centralized standard solution. It manages all of the assets and devices centrally, whoever they are manufactured by. Central device monitoring assures an overview, while asset safeguarding through backups and version management provides a complete picture of all the production facility's data. Also, in an emergency, the instant recovery of software versions and program data puts all the data back the way it should be. And octoplant proactively detects vulnerabilities, changes, and risks to protect production processes against attacks and eliminate damage and downtime.

MORE THAN 2,800 CUSTOMERS ALREADY RELY ON AUVESY-MDT SOLUTIONS FOR THEIR MAINTENANCE AND PRODUCTION MANAGEMENT.

Discover the free trial version now!

Click here: octoplant Web-Demo

*https://auvesy-mdt.com/en/web-demo-live

AUVESY-MDT

AUVESY-MDT is the global market and technology leader for versioning and backup solutions in industrial automation. With its octoplant software platform, the company secures the automation of production processes through strong end-point management, where it consistently records and monitors changes to configurations, programming and project statuses in production. This minimizes downtime, increases efficiency, quality and safety standards, and saves costs as well as resources. As a modular solution, octoplant can be linked to different automation technologies and devices, regardless of the manufacturer.

AUVESY-MDT was formed in 2022 from the merger of the two established market leaders AUVESY GmbH and MDT Software Inc. The company is headquartered in Landau, Pfalz, Germany, with additional locations in the USA and China. The company works with more than 100 partners on all continents and serves over 2,800 customers worldwide.

More Information at: auvesy-mdt.com

PREFERRED octoplant partner
powered by AUVESY-MDT

Novotek

Novotek Switzerland AG
Glutz-Blotzheim-Strasse 3
4500 Solothurn

info.switzerland@novotek.com
+41 58 255 32 32

www.novotek.ch