White paper

Prevent production downtime effectively by monitoring intelligently.

This free white paper is for plant managers facing the challenges of digital production processes.

AUVESY-MDT

TEASER

A guide for production managers – achieving transparency and security in complex digital production environments

How is the digitalization of production changing the role of the production manager? Its numerous advantages come with new challenges. Harness the full potential of digitalization in production, but without increasing operational complexity.

The guide tells you how to maintain constant control of machines, project files, and updates. Operate any number of different systems and control layers reliably in unison. Accelerate product cycles and reduce batch sizes, without jeopardizing traceability. This white paper shows how automation, protection, project data version management and software versions take the operative complexity out of digitalization. It provides production managers with simple ways of making modern manufacturing as clear, reliable and well-structured as traditional production.

Our guide provides answers to these questions:

- How can production managers prevent interruptions in complex environments?
- How does octoplant help to automate, monitor, and protect modern production systems?
- What modern software features can help to prevent or quickly eliminate data loss, downtime, and misconfigurations?
- How does documenting assets and processes centrally for everyone involved speed up onboarding and problem-solving?

Our guide provides detailed information as well as a concise graphical overview of the various aspects of digitization.

Preventing production downtime through intelligent IoT monitoring

For those responsible for managing production facilities, it is paramount that machines continue to run. Continuity and reliability are the highest priority when it comes to operations. The ongoing trend towards digitalization promises companies enormous potential when it comes to increasing flexibility and efficiency. It offers them the ability to automate, manage, monitor, and map their production facilities digitally; and it also helps them to optimize maintenance plans and automatically manage project data. Production disruptions can be detected in real-time and manual errors are avoided due to automation. Plus, there is also the added benefit of smaller batch sizes, improved utilization, and reduced interruptions.

While the benefits are numerous, the implementation of digitalized software-driven machinery also brings about its own set of unique challenges and vulnerabilities, which in turn, require new solutions. Cyberattacks and deliberate sabotage are frequently responsible for production downtime. Safeguarding against such attacks is imperative when it comes to protecting and ensuring the continuity of production. In addition to the dangers posed by cyber threats, the overall increasing complexity of operational technology only adds to the many well-established risks to production, including defects and supply chain disruption. When machine shutdown occurs, the number of parts a machine handles per hour, as well as unit costs, and contractual penalties may impact the overall cost of downtime

Facilitating better continuity, transparency, and management of technical know-how in automated production.

A 2021 study of 72 major multinational industrial and manufacturing companies reveals that, on average, large plants incur 323 hours of downtime a year. The average cost of lost revenue, financial penalties, idle staff time and restarting lines is $532,000 per hour, amounting to $172 million per plant annually[1] . It is clear that downtime is both a financial and organizational disaster. Disruptions can cause losses to sales, decrease customer confidence, and can even cause the public image of a company to suffer.

Companies who have not implemented routine data backups, data recovery, and/or who lack an effective cyber defense strategy are vulnerable to production downtime. Damage caused by cyberattacks continues to increase dramatically. Global cybercrime costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015[2].

But it's only the start. Secondary costs start to roll in almost immediately, including:

- Customer disruptions, including churn
- Fines due to hacking incidents
- Productivity losses
- Overtime and extra staffing (source)

1 (reference: Senseye 2021 industry report „The True Cost of Downtime")

2 https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

In the event that downtime occurs, those in positions of responsibility need to ask themselves two questions: how can the system be brought back into operation as quickly as possible and why weren't we better equipped? In this whitepaper, we will explore various approaches you can take in order to minimize outages, and their consequences, and how you can optimize the resiliency of your operations.

Learning from the mistakes of the past so as to not repeat them

At the beginning of the 20th century, it was the production managers who drove the transition from the steam engine to the electric motor as the preferred power in production environments. However, there remained a flaw: the large steam engine, which operated as a central machine, drove entire production lines via a system of belts and pulleys. As such, it comes as no surprise that it would seem logical to that generation of production experts to view and use electric motors in the same way – as massive, centralized power machines.

It wasn't until a few years later that the next generation of engineering and manufacturing experts would replace the large, centralized machines – with their vulnerable belts and idlers – with effective, decentralized motors that directly drove those machines and conveyors. It was this step that revolutionized efficiency and productivity in factories. Now, a century later, it is once more the production managers who are driving networking, IoT and automation. These trends require people with vision, who do not see innovations as simple replacements for previous processes, but who recognize new technologies as new opportunities to optimize already existing technology. Replacing punch cards with floppy disks, then replacing floppy disks with USB sticks, only to then trade in USB sticks for controls that are not fully networked, is a start, but even that does not fully encompass nor yet achieve the pinnacle of what is possible today.

The new role of production management in the digital world

As the digitization of the factory floor, production planning, and customer ordering processes continues to increase so do the responsibilities shared by production management with regard to these areas and processes. While technology and processes have evolved significantly, so have the security risks. What's more, there are now new operational vulnerabilities that have the potential to bring an assembly line to a standstill. New automation solutions, complex networking structures, and new software are also the responsibility of management. They can make operations more efficient, however, they also come with their own complexities and potential sources of error, which could disrupt production flow. If that weren't enough, there is also the fact that data-driven production no longer functions by the rules that so many companies have used to operate successfully for the past few decades.

Familiar patterns and principles therefore need to be reexamined. Ensuring that operations run smoothly doesn't just require machines that function, available personnel, or a reliable power supply. Production environments must also consist of well-integrated and maintained electronic controls, controllers, sensors, and their programs and parameters.

Taking charge when presented with the challenges of digitalization

Automation solutions help to increase efficiency and simplify processes. This aspect of digitalization not only impacts production processes, but also influences purchasing and ordering. Thanks to digitalization, batch sizes are changing. In many cases, they are becoming smaller and smaller. Product life is also becoming shorter, while expectations of short-term delivery times are becoming greater and greater. Digitalization in sales causes orders placed in the industry to increasingly resemble consumer buying behavior shown in e-commerce. Networking and short-term production planning enable for this kind of marketing to happen. This increases the effort required to ensure business continuity in the face of increasing complexity and demand.

Important terms: Disaster Recovery

In the event that everything that could go wrong, does go wrong, having a functioning disaster recovery process in place can help ensure that all data and projects are quickly restored. Such a strategy can be carried out in the event of a cyberattack, sudden system or machine failure, or operator error. Disaster recovery encompasses performing regular data backups, having transparent documentation for all program versions, and being able to restore software states easily and reliably (even when carried out remotely) using a centralized solution.

Important terms: Device management in the industry

It is important that the numerous systems and levels present in production facilities are managed in a way that they work together seamlessly. Physical machines, IoT devices, control systems, communication modules, and many other hardware and software assets, all need to be monitored and managed. This is no small task given that managing these assets often requires different solutions due to the wide range of asset manufacturers. The advantage of unified device management means that there is no digital gap, and that all relevant assets are connected in one centralized system.

Short product cycles require more flexibility

The demand for „I need this product variation – now", is another growing trend displayed by customers across all kinds of industries. Suppliers are having to work with a shorter planning horizon. This increasingly leads to the parallel production of various products, and more and more product variants. Frequent changes to recipes and formulas in production is becoming commonplace, which increases the risk of errors occurring. More changes and greater speed not only increase the potential for errors, but also the effort required to document and manage all program versions. A clear change history (who changed what, when, where, and why) helps to ensure that changes made to device data are intentional; and that any unauthorized/unintentional changes are reported automatically.

In order to ensure the security of their systems - and to keep track of the complex array of controllers, machines, production parameters, recipes, software, and employees – management needs to work closely with IT. Quality assurance, compliance, and error traceability are major challenges in any production environment, but they are especially tricky in an environment that consists of fast-moving product changes and complex controls.

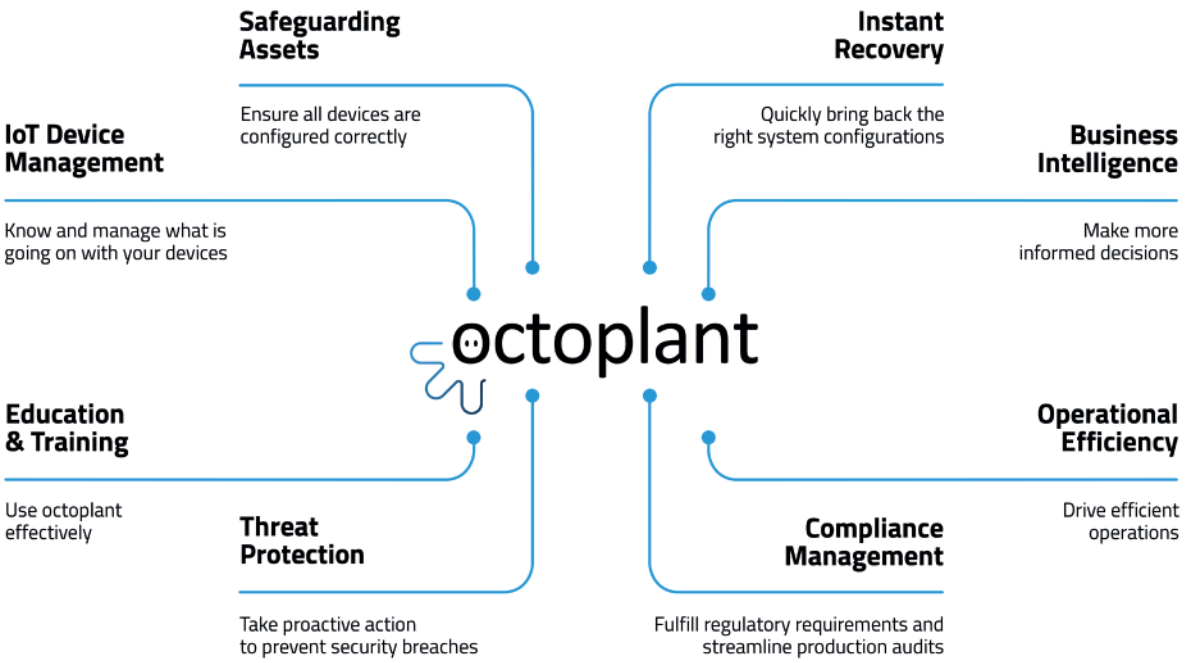
What happens when a component breaks down?

When a machine goes into standstill – due to a PLC malfunction and/or the machine having its memory wiped - speed is of the essence. Physically replacing the failed component can be done relatively quickly, however, the machine must also be brought back online. If the PLC program currently required for that machine can be restored in a few seconds (once the defective machine is replaced) the mean time to repair (MTTR) is significantly reduced. Manual effort is minimized and the potential for new sources of error – brought about by manually researching, checking, and restoring the needed program state – is avoided.

Your go-to solution | Gain complete transparency with AUVESY-MDT's octoplant

Automating your production environment only helps you win half the battle if control and data management continue to be carried out using manual processes. In networked production environments multiple software solutions interact with each other at different levels; providing support for controlling, safeguarding, and monitoring different components. This increases both the complexity and likelihood of errors occurring, and makes the task of effectively protecting all systems in a standardized manner much more difficult. One challenge in particular – when it comes to security architecture - is that of rights and access management. Employees must be assigned appropriate access to components and functions in the system, so that they can carry out the tasks they have been contracted to do. Another common problem in heterogeneous environments is the creation and management of program versions, data, and documentation. It is not always possible to create backups of all data and programs (so that changes and losses can be reversed at any time) across the board.

The AUVESY-MDT octoplant solution is capable of analyzing the data and programs of numerous manufacturers, and automates the processes involved in creating and saving versions, documentation, backups, and numerous other processes that can lead to errors when managed manually.



octoplant enables you to create backups, safeguard assets, and optimize operations in your production environment.

octoplant provides production managers with an integrated solution that meets all requirements needed for facilitating transparency and traceability in production facilities and the systems they contain. In a 2021 survey, 75% of all customers said that they have been able to sustainably increase production quality thanks to the software, and described it as being indispensable; 94% said that they would recommend it to others.

All of your assets managed in one system

The octoplant solution is a manufacturer-independent, centralized data management platform that supports a wide range of bus systems, standards, and manufacturers. The aim of this centralized approach – which details everything from sensors, field devices, SCADA systems, PLCs, HMI devices, industrial PCs, and switches – is to provide comprehensive visibility for all stakeholders, enable preventive maintenance, and minimize technical failures.

Ensuring traceability

When it comes to multi-shift operations - in fast-moving production environments - personnel, products, and project programs are all subject to frequent changes. Long-established processes with manual steps do not allow for an all-encompassing picture of which parameters (or documents) were changed, when, and by whom.

What's more, traditional methods cannot ensure that project data is correctly assigned to the current product at all times. This is essential when faulty batches need to be tracked. Plant management requires a complete overview and a central platform that consistently maps all assets. In the world of IT, this is referred to as a Single Source of Truth. A centralized point where all relevant sources of data converge and are collected.

Automatic backups

octoplant's safeguarding assets module backs up all production system data, projects, and programs. It also enables the automatic creation of program versions. Changes can be automatically detected and identified so that discrepancies can be easily fixed. This enables the last functioning software status – and as a direct result, production - to be restored at any time.

Training, documentation and onboarding

Assisting employees is yet another key benefit of implementing octoplant. The AUVESY-MDT Academy assists employees in learning how to use octoplant by providing personal feedback and ongoing support. This ensures that all users understand how to best use the solution's features. Just like octoplant is a centralized point for all plant and process documentation, having access to our central academy makes it easier than ever to train new employees and retain their expertise in your workforce.

More than 2,500 customers already rely on AUVESY-MDT solutions for their maintenance and production management.

Find out more about the free trial version.

TEST NOW

AUVESY-MDT

The world market leader in version control for automated production environments.

With over 150 employees and our own subsidiaries in Germany, USA and China, we support our customers with over 3,200 installations in more than 50 countries worldwide together with our partners. These come from various industries and use our solutions to manage and safeguard their automated production environments. Use cases range from managing IoT devices and enabling disaster recovery, to increasing operational efficiency or preventing cyber security breaches.

GERMANY

AUVESY GmbH
Fichtenstraße 38 B
76829 Landau in der Pfalz

+49 6341 6810-300
info@auvesy-mdt.com
www.auvesy-mdt.com

OFFICE USA NORTH

AUVESY Inc
146 Monroe Center St NW / Suite 1210
MI 49503 Grand Rapids

+1-616.888.3770
info@auvesy-mdt.com
www.auvesy-mdt.com

OFFICE USA SOUTH

MDT Software
3480 Preston Ridge Road
Alpharetta, GA 30005

+1.678.297.1000
info@auvesy-mdt.com
www.auvesy-mdt.com

OFFICE CHINA

AUVESY Data Management Solutions Co., Ltd.
Jinma Lu 3, Maqun, Qixia District, Nanjing

+86 25 52235097
info@auvesy-mdt.com
www.auvesy-mdt.cn