Is your OT safe from attacks?

This free guide is aimed at IT managers who wish to protect digital production processes against malware and other cyber threats.

white paper

AUVESY-MDT
We secure the world's automation

INTRODUCTION

The white paper for “Is your OT safe from attacks?“ Our guide for IT and OT managers – securing complex production environments

Targeted cyberattacks on industrial facilities are on the rise, as are the costs they incur. In recent years, plenty of well-known companies have fallen foul of trojans designed to extort and of cyberattacks targeting production facilities. Although IT and OT are gradually merging, familiar IT security mechanisms can’t always be applied to OT as they are. And OT systems are easy targets for professional attackers, because it’s far less common for their hardware to be abstracted by protective and monitoring software layers than in modern IT architectures. Instead, a multitude of different stand-alone software solutions often make system landscapes more complex.

Enjoy the transparency and efficiency of digitally networked production without exposing yourself to new risks. Cyber insurance can provide a safety net, but because a successful attack can have expensive repercussions, these policies are expensive, and they still require active protective measures that minimize risks.

This white paper shows you how you can connect up your IT and OT, regardless of the manufacturer, to create a transparent and secure overall system.

Our guide provides answers to these questions::

- How can IT managers achieve unified, secure asset management?
- What are the security needs of today’s networked production environments?
- How does octoplant help to secure OT in production and to avoid downtime?
- How are German businesses and organizations already protecting themselves against cyberattacks

Our guide contains detailed information as well as a summarizing graphical overview of the various aspects of security in production.

This free guide is aimed at IT managers who wish to protect digital production processes against malware and other cyber threats.

Avoid unwanted changes and data loss – increase uptime Better alternatives to expensive cyber insurance policies

According to the Forbes Magazine, a minute of downtime cost 22,000 US dollars. That adds up to 50 billion in costs caused by unplanned production downtime per year. High-profile production outages in recent years haven't just inflicted massive financial damage on the companies concerned, they damaged images too, because the attacks were so widely publicized.

Auto manufacturer Honda, for example, had its entire production immobilized by a ransomware attack in June 2020. This is just one of many attacks using the extortion trojan known as Ekans. Its mechanisms target ICS environments through vulnerabilities in IT infrastructure and reach OT machines via unpatched software. Just a few days later, European energy company Enel fell victim to an Ekans attack, as the company confirmed in news magazine BleepingComputer.

Cyberattacks are a growing threat to OT. As the Honda incident shows, cybercriminals are now developing malware aimed specially at ICS and SCADA systems. Examples of such malware, aside from the aforementioned ransomware, include LockerGoga and Doppel-Paymer. Complicating matters further, IoT search engines like Shodan make it easy to locate and identify networked devices that are connected directly to the Internet. This search engine is so sophisticated that it even displays the version of the operating system a device runs on, making it easy for hackers to spot vulnerable targets.

According to IBM Security, attacks on PLCs and SCADA-related attacks grew by more than 2,000 percent between January and September 2021. Analyzing data from 2021, IBM's Security Offensive X-Force observed a significant increase in activity targeting TCP port 502. This port uses Modbus and allows malicious players to control hardware connected to the Internet.

The maintenance and configuration of systems used to be the biggest reliability factors before digitization. Today, systems need protecting against outside vectors.

The differences between IT security and OT security

IT (Information Technology) traditionally becomes OT (Operational Technology) when machines and the processing of goods are added to the equation and it's no longer about planning and management alone.

Technology that touches factory floors falls within the industry definition of OT. But successful trends such as IIoT (Industrial Internet of Things) and general digitization in development, resource planning, and process control have led to the networking of machines and their control systems, and the boundaries between IT and OT are blurring fast. People today often try to achieve OT security and protection by means of logs, backups, and recovery. Solutions like firewalls and malware protection are not yet widely deployed. The main reason is that the two disciplines place different emphases in their protection goals: data confidentiality is top of the list in IT, whereas availability is given much more weight in OT.

Meanwhile, new systems and new tasks are finding their way into production. The management and support of PLC and machine data used to be a matter for maintenance alone, but nowadays, more and more IT and OT managers are working hand in hand.

Level 5: Company level
Strategic and operational management of the company (ERP)

Level 4: Production level
Planning and operational control of production (MES)

Level 3: Line level
Operational control of a production line (SCADA)

Level 2: Machine level
Real-time control of individual machines (NC)

Level 1: Sensor/actuator level
Processing and measurement in product manufacturing

Quelle: ANSI/ISA-95 Standard

Fig. 1: Layer model - distinction IT & OT

The ANSI/ISA-95 standard describes a layer model that clarifies the traditional distinction between IT and OT as well as networking as a whole.

Approaching IT security standards

When it comes to protecting its control systems and standalone solutions, operation technology (OT) is still very different from IT. In most companies, the process of abstracting different assets and software solutions to create one homogeneous overall system is still years behind what has been achieved in current IT setups. In a modern, self-healing IT platform, it no longer matters who makes the various servers and components. The task now is to achieve the same level of abstraction in OT, the same transparency through monitoring, and the same resilience through threat protection and instant recovery as has long been enjoyed in IT. So far, industry managers have lacked this kind of standard solution.

LOOKING AT UPTIME, 88 % OF MANUFACTURING COMPANIES SEE ROOM FOR IMPROVEMENT

With increasing complexity comes a rise in production failures

Those responsible for operations and infrastructure face the challenge of optimizing production efficiency and flexibility without introducing new vulnerabilities and bottlenecks into the way things are organized. Avoiding downtime is a high priority in 70 percent of manufacturing companies, and more than 80 percent of managers expect to achieve it using software.

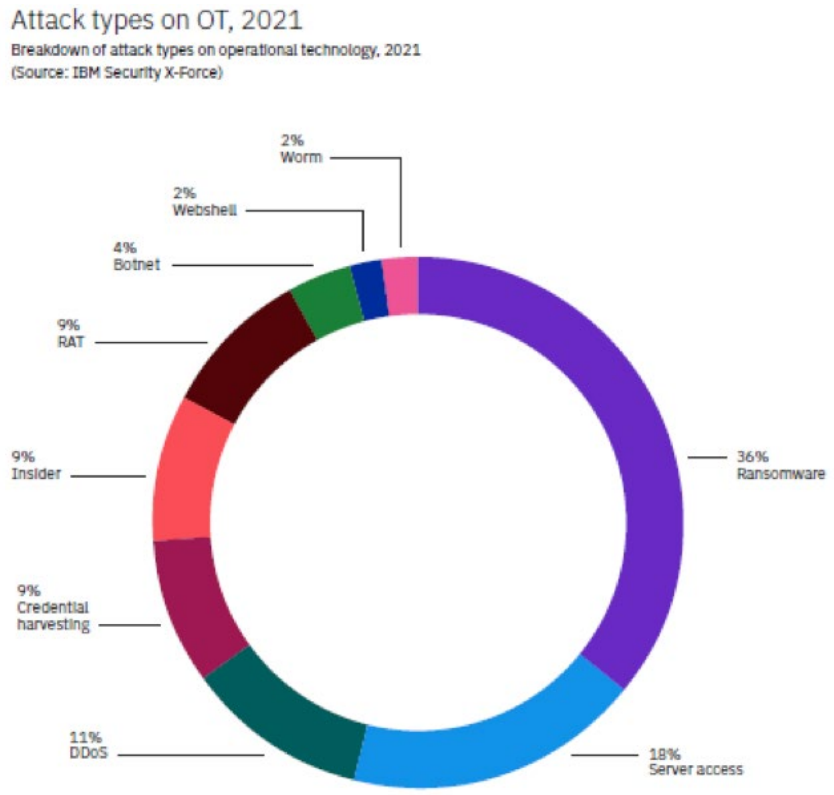

Fig. 2: Production downtime - attack types

Managers want:

- Greater transparency through daily insights into production
- To be able to deliver orders as contractually agreed
- Greater flexibility to accommodate ever smaller batch sizes and multiplying product variants
- Production resilience through threat protection and instant recovery

The causes of production downtime include cyberattacks, misconfigured machines and software, and human error. According to the study Costs, Causes and Consequences of Unplanned Downtime, 45 percent of unplanned interruptions are due to hardware failure, 39 percent to software error. The cost of this downtime is rising: average hourly outage costs rose from 160,000 to 260,000 US dollars between 2014 and 2016 alone. According to Sophos, more than a third of manufacturing companies complained of a ransomware attack in the past twelve months. In half of these, attackers succeeded in encrypting data. Two-thirds of the businesses were able to restore data from backups.

One-fifth paid the ransom instead. This means around ten percent of all of manufacturing companies surveyed paid blackmailers within a twelve month period. The average amount was $150,000. Despite doing this, more than a third of those businesses received less than half of their data back.

1.52 million US dollars

is the average amount of damage inflicted on manufacturing companies by a cyberattack. This includes downtime, labor, ransoms, equipment and lost opportunities. (Sophos)

IT and OT both offer doorways to attackers. According to the ICS Risk & Vulnerability Report, one-third of known vulnerabilities can be attributed to IT and IoT, two-thirds to OT. Companies can protect themselves against this risk, against the sudden onset of chaos and uncertainty. Insurance against operational failure, for instance, offers theoretical protection against financial consequences. But it is expensive and demanding and comes with complex settlement modalities and lots of liability exclusions.

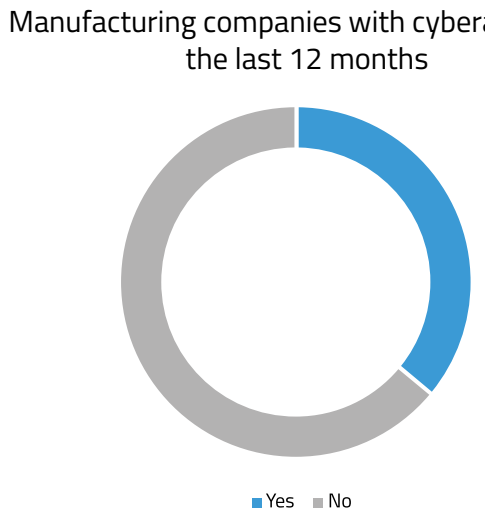

Fig. 3: Sophos-Studie („The State of Ransomware in Manufacturing and Production 2021") sophos-state-of-ransomware-manufacturing-production-2021-wp.pdf

As manufacturing becomes more complex and cybersecurity concerns grow, many manufacturing companies are contemplating major challenges and conflicting demands. Greater digitization has improved production flexibility and efficiency as had been hoped, but it has also ramped up complexity while creating new points of attack and disruption risks. For company managers, the problem is often not just the failure or malfunction of a component. It is how to identify and recover a system's most recent status, such as all of its project data. This is because diagnostics and data management, even in automated environments, are often still done exactly as they were 30 years ago: manually. There are too few methods available for things like monitoring changes and logging their sequence, and only allowing selected people to make adjustments.

Wanted: a simple, one-size-fits-all solution as a way of safeguarding production

Those tasked with technology, infrastructure, and operations are seeking a solution that is easy to implement and uniform across all automation devices, controllers, and even sites. In practice, complex patchwork systems consisting of multiple separate solutions demand constant adjustments and workarounds; they themselves can become a source of trouble requiring complex diagnostic input.

Insurance against downtime and loss due to cyberattack can provide a financial safety net against operational failure – in theory at least. But requirements have tightened a lot in recent years. Closures during the pandemic have had a major impact on policies of this kind. And insurance companies no longer consider themselves solely responsible for cover. While the insurance industry is optimistic that automation will reduce the level of conventional production losses, it warns of the new, systemic risks that this networking brings. Sadly, the days when downtime insurance was comparatively easy to come by are over, because there has been such a sharp rise in the number of incidents.

Insight: Minimizing cyber security risks will be the biggest challenge in reducing unplanned downtime in the coming years

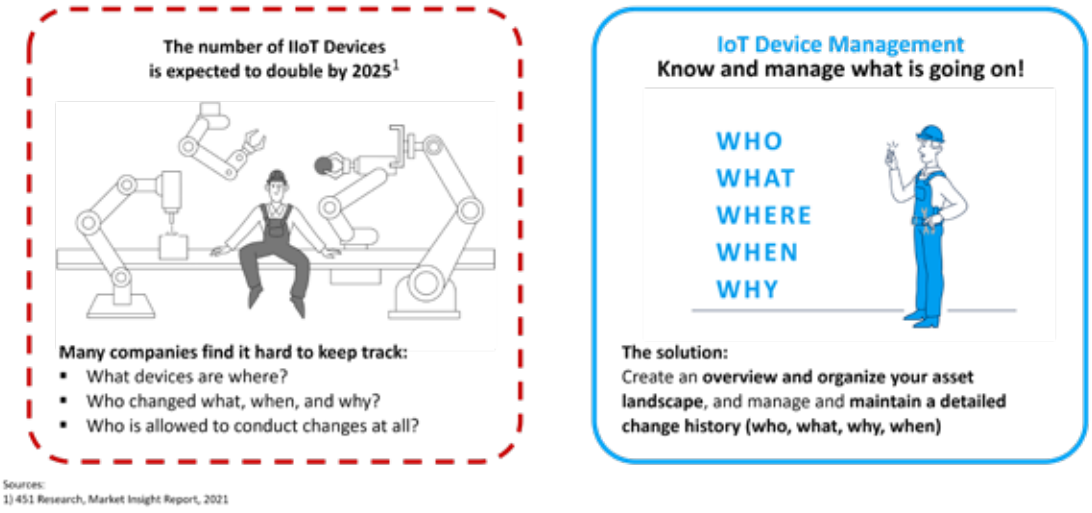

Fig. 4: Minimization of cyber security risks

U.S. insurance company Travelers, for example, posted losses in 2020 as it had to deal with so many costly cybersecurity claims. Because of these developments, it's now virtually impossible for a business to get a new policy without extensive auditing and far-reaching extra protections. All this means that today's manufacturing companies definitely have to be proactive about IT and OT security. Insurance companies will only provide cover if extensive measures are in place to actively minimize the risk of failure.

Businesses therefore have to invest heavily in active operational security if they want to enjoy attractive insurance terms. Specific threats (which might be determined on the basis of previous attacks) play just as important a role as a company's demonstrable security level. The scope of cover (first party? indirect customer damages?) also has a major impact on price. Cyber insurance can be configured very specifically, which means there can easily be gaps in cover.

Attacks and other catastrophic incidents aren't the only thing that can cause downtime. Normal day-to-day operations can too. Reports still persist about world-famous companies whose machine updates regularly cost millions, because technicians have to do them one by one using memory sticks.

THE BEST PRODUCTION INSURANCE IS TO BE CERTAIN YOU HAVE CONTROL – AND A PLAN B – AT ALL TIMES.

Attack on waterworks in Florida compared with Emschergenossenschaft in Germany

Expectations of reliability and robust operation are especially high in critical infrastructure. This goes for the law, of which the international standard IEC 62443 and EU NIS2 directive are but two examples. And it goes for the public too. Businesses that provide people with their basic daily needs have to meet the highest requirements when it comes to protection against attacks, as well as protection against mistakes and technical failures. A case in Florida shows just how vulnerable essential infrastructure can be. In 2021, unknown attackers succeeded in manipulating the control system of a water treatment plant remotely. They increased the amount of sodium hydroxide (lye) added to the water by a hundredfold. Only by chance did a technician notice the computer being controlled remotely; they were able to restore the normal water treatment parameters before things got dangerous.

The Emschergenossenschaft/Lippeverband waterways association (EGLV) has shown how critical infrastructure operators can safeguard essential processes such as process control. It is responsible for wastewater disposal and water maintenance affecting more than 3.5 million inhabitants of North Rhine-Westphalia. All of EGLV's water treatment controls and programs are digitally monitored and backed up using octoplant from AUVESY-MDT.

Monitoring complex industrial systems uniformly

No company, whether DAX or SME, can consider itself immune to today's cybercrime. An increasing number of such attacks – especially ransomware – are on operational technology (OT) in industrial plants, and by no means IT infrastructure alone.

To ensure that production keeps running efficiently, robustly, and transparently, managers need the right tools: solutions that allow fast, fact-based decisions to be made that are easy to actuate and implement. Lots of separate solutions make the overall system more complex and add potential breaking points and sources of trouble. The answer lies in unified plant management. octoplant by AUVESY-MDT provides a transparent, manufacturer-independent, 360-degree view of entire industrial plants, whatever industry standards are involved. The solution augments a well-thought-out cybersecurity strategy at every stage: preventing an attack, detecting an attack early, and minimizing damage through rapid disaster recovery.

It is compatible with a wide range of automation systems and, compared to competitors,supports an unparalleled number of devices within a system. This prevents downtime, data loss, and time-consuming diagnostics, because the system is managed centrally. And it gives you full control over all of your software versions, an overview and insight into all your production devices, and transparency in your automation.

An inventory of all the devices in your industrial facility improves your OT's cybersecurityand enables you to analyze risks. It shows you whether the machines and systems that are connected up are as secure and up-to-date as they can be. All this helps in day-to-day operations of course, and allows you to quickly upload the best backup of a previous version in the event of a cyberattack and get your system up and running again. This an area where up-front investment is money well spent, especially considering the rapidly rising costs of production downtime.

Recommendations for securing your production

As a manager, what do you need to do to enable your workforce to operate their OT reliably?

Assess your own risk

- Assess your own cybersecurity (Management of Cyber Risks manual, Appendix B)
- Develop and monitor cyber business metrics (Management of Cyber Risks manual, Appendix D)
- Self-assess the security requirements of the German Federal Office for Information Security's Basic IT Protection Compendium ("Process control and automation technology", for instance)

Protection against attacks

- Establish a security process using the templates offered by the Basic IT Protection Profiles
- Draw up a detailed inventory of your OT assets (firmware, model, rack slot, IP, manufacturer)
- Strategy for automatically backing up all your devices

Minimizing risks

- Monitor your security status (CVE: common vulnerabilities and exposures)
- Detect and close security gaps
- Document any changes clearly

In the event of an attack

- Detect unwanted changes quickly (alarm triggers)
- Quickly restore the most recent version before the attack

"Cyberattacks are a real threat to us. We would rather have too much protection against the outside world than too little. The fact that versiondog* tracks and timestamps every data access helped seal the decision."

Matthias Teitge
Head of Plant Management, Hofbrauhaus Wolters
*The predecessor of octoplant.

Hofbrauhaus Wolters is a traditional medium-sized business whose products demand consistent, controlled, auditable quality. Its machine and control system structure has evolved over a total of three decades. Hofbrauhaus Wolters therefore needed a solution that would uniformly monitor and safeguard older PLCs and modern robotics. The solution: octoplant monitors access, automation, and program versions.

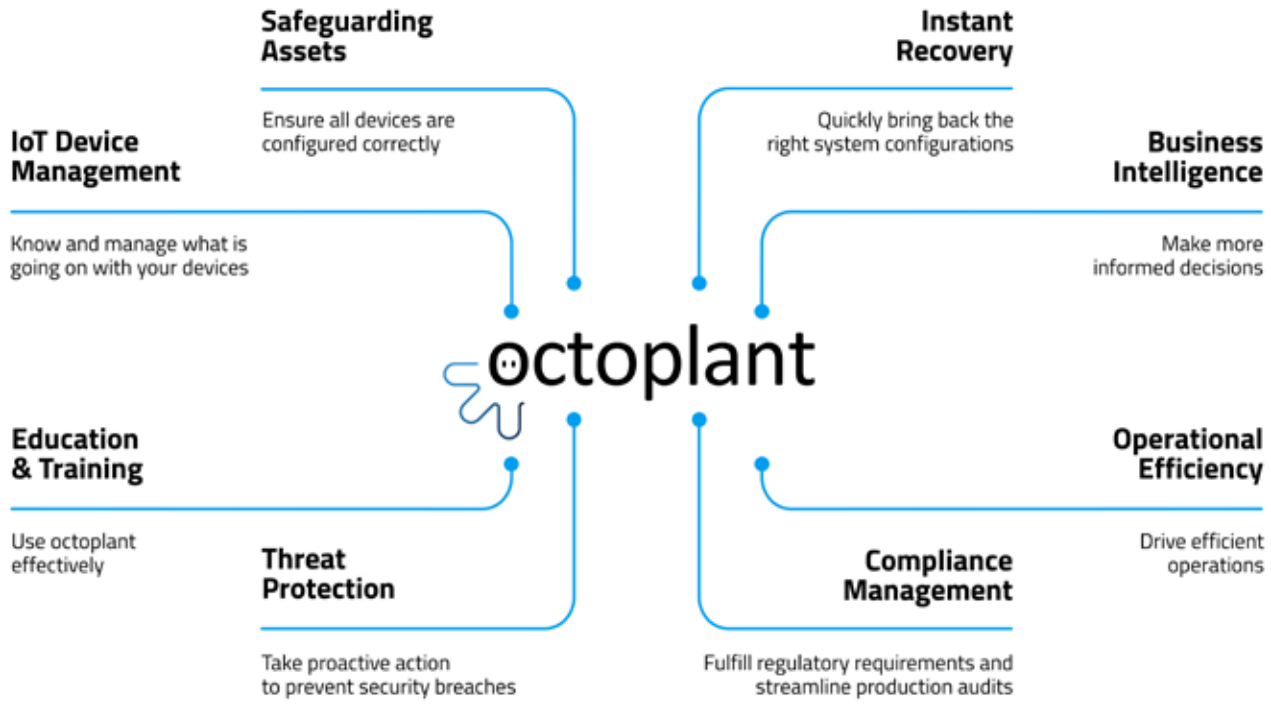

Fig. 5: octoplant Maintenance and production management solutions

Conclusion: uninterrupted 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 everything 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 2,400 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

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

AUVESY-MDT
3480 Preston Ridge Road / Suite 450
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