cecimo
European Association of the Machine Tool Industries
and related Manufacturing Technologies

CYBERSECURITY FOR THE MACHINE TOOLS INDUSTRY

www.cecimo.eu

1. Introduction & Legislative Updates

As digitalization becomes more prevalent across industries, there is a growing need for companies to increase the safety measures against cyber risks.

Like in other sectors, the machine tool industry perceives cybersecurity as a technical risk and a business risk. Equipment, uptime, trade secrets, brand value, intellectual property, and even personal safety must be protected from malicious network intrusions, employee sabotage, or accidental manipulation.

The EU policymakers have worked intensively to increase the level of cyber resilience of different sectors (including manufacturing) by strengthening cybersecurity requirements for companies and addressing the security of supply chains as well as safeguarding relationships with suppliers.

Given the relevance of this subject for the machine tool sector and the importance of highlighting the main challenges and actions to increase the sector's cybersecurity, this paper includes:

- A legislative overview
- Cybersecurity for machine tools
- Examples of vulnerabilities to cyberattacks
- Countermeasures: national actions
- CECIMO recommendations

2. Legislative Overview

The EU economy has grown more dependent on network and information systems and is open to cyber-attacks. To respond to these growing threats, the European Commission (EC) has undertaken different initiatives to strengthen the security of European economic actors that operate through digital systems.

The Directive on Security of Network and Information Systems (NIS Directive) has been adopted in 2016 with the objective to improve security requirements, tackle the cybersecurity of supply chains, implement tighter supervisory and enforcement measures and boost security levels across Europe in the long run. One of the pillars of this piece of legislation was the implementation of risk management and reporting obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP).

In 2019, the EC adopted the EU Cybersecurity Act (CSA) to define a cybersecurity standardised certification framework for IT products, services, and processes. This legislation gives the ENISA (EU Agency for Cybersecurity) the mandate to set up and maintain the mentioned framework fostering operational cooperation among the Member States on cybersecurity certificates.

In 2020, the Commission submitted a proposal for the Directive on measures for a high common level of cybersecurity across the EU (NIS2 Directive) to expand the scope of the NIS Directive strengthen supervisory and enforcement measures and fortify the strategic autonomy of the EU.

The NIS2 Directive is particularly important for the machine tools sector:

- There will be no longer a distinction between OES and digital service providers but, instead, will categorise entities between essential and important ones, with the manufacturing sector included in the second group.
- Essential and important categories will need to fulfil cybersecurity management and reporting requirements; however, the main difference stands in the supervisory and penalty regimes. The essential entities are subject to an ex-ante supervisory regime and penal responsibility, whereas the important entities are subject to lighter ex-post supervision in case of non-compliance.
- Important entities are deemed to be under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it should fall under the jurisdiction of each of these Member States.
- Member States are required to ensure compliance with the security and incident notification requirements. National competent authorities should act when provided with evidence or indication that an important entity does not meet the security and incident notification requirements.
- Member States should ensure that important entities, thus including machine tool builders, implement cybersecurity risk management measures and that they follow regular training to get the necessary skills for assessing cybersecurity threats.

In May 2022 the European Parliament and the Council of the EU reached a provisional political agreement on the NIS2 Directive. Member States will have 21 months from the entry into force of the NIS2 Directive in which to incorporate the provisions into their national law.

In 2022 is also expected the publication of the EC proposal for a Cyber Resilience Act (CRA). Such a proposal will address market needs and protect consumers from insecure products by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital and ancillary services.

3. Cybersecurity for machine tools

Machine tools (MT) are long-lasting capital goods that are often operated for decades, therefore a large part of the installed equipment in a typical production facility needs Operational Technology (OT) security solutions.

Furthermore, MT are complex technical systems that are:

- Made of several subsystems (e.g., HMI, connectivity gateways, etc),
- Connected to several units (e.g., loading magazines, coolant systems, hydraulic units, etc.).
- Regularly adapted by and with the customer and often supplemented with third-party enhancements (e.g., tool breakage monitoring)
- Modified over the years during their use.

This complexity leads to the fact that an isolated and single intervention to protect a machine (in the sense of OT Security) would not secure the entire system. A solution is to develop a machine that already incorporate high level of security standard: Security by design.

The phase of design of new machines presents the best starting conditions for efficiently achieving a high degree of protection. The effort and difficulties to secure the MT increases steadily along the use phases, which is why an initial effort represents the best possible basis to ensure the safety of the system.

Although the operator of the machine can make an initial and important contribution to safe machine operation, the plant and machine manufacturers can also invest in security of construction and operation of the machines.

The importance of security by design approach is even more evident if we consider that a machine tool operating system might need an update even before arriving to the customer. This is because the time of initial commissioning at the customer's premises, and the actual delivery and transport could be longer than the time between security patches.

Finally, another challenge for this sector is to protect machines during their long lifecycle and maintain a high level of security standard throughout the entire service life.

Therefore, it is important to find ways of protecting beyond the design phase and look for solutions for existing machinery to ensure that the benefits of digitization in production can be implemented while maintaining high safety standards.

Differences between OT and IT security

Although the attention of media and policymakers has been directed almost exclusively on IT security matters, it is of crucial importance for our sector to put the emphasis on the OT cybersecurity.

The OT is commonly used to indicate the technological and functional differences between traditional IT systems (available in an office) and the environment of industrial control systems, the so-called "IT in non-carpeted areas".

OT systems use many of the same tools as IT environments but are designed to be utilised in different ways. OT primarily refers to hardware and software for the control, regulation, monitoring, and surveillance of industrial plants, machines, assets, and systems.

Several experts have pointed out the growing convergence of the two sides of security when it comes to interconnected devices and machines, namely IT and OT as two sides of the same coin. However, even if there are different overlapping elements, there is a strong need to have a dedicated OT Cybersecurity Policy aimed at explicitly stressing the importance and supporting the actions undertaken by machine tools companies. If certain measures such as assets inventory, micro-segmentation of devices, role-based access control etc., are underestimated, every initiative strictly related to IT security would have very limited effectiveness in supporting our industries.

CECIMO highlights the importance of distinguishing between IT and OT security when discussing cybersecurity for the machine tool sector. Due to the significant differences between the "classical IT-Systems" and the IT-Systems used in the production environment, there are at least five major differences that separate machine tools (and other production equipment) from classic Office-IT equipment:

Differences in the requirements for IT (office environment) and OT (production environment)

	IT	OT
Lifespan	3 - 5 years	5 - 20 + years
Development cycle	Short	Adapted to the life cycle of the machine
Anti-virus	Used everywhere	Often difficult or impossible to use in (legacy) system
Vulnerability scanning	Active scan	An active scan can disrupt the operational production
Security testing	Used everywhere	Only after identifying the risks and careful assessment
Availability	Short delays – tolerated	Running 24/7 – No margin for delays IEC 62443 defines safety objectives in part 1-1, with availability defined as the highest protection objective
Reliability	Incidental failure is accepted	Failure is unacceptable
Time dependency	Not relevant – Delays are accepted	Critical – No margin for delays IEC 62443 defines in part 1-1 where real-time capability is specified as a millisecond range
Investment	~ 1.000 €	Up to million € - Depending on machinery

Sources: VDW; Dutch Security Cluster

4. Examples of cyber threats and cyber risks and the role of the operator

Industrial cybersecurity experts struggle with keeping operations of modernized manufacturing plants cyber-safe. Cyber-attacks have become more sophisticated combining different techniques and attacking multiple layers and technologies at the same time. Attacks can force complete shutdowns of certain facilities, corrupt information technology systems, force manufacturing plant closures, and impact the company's reputation. No less than any other sector, machine tool industries are vulnerable to cyber threats.

The digital optimization of a machine tool brings both opportunities and risks for a company's production processes. For this reason, the goal of each company must be to embrace the digital transition while ensuring the highest possible level of security.

It is of primary importance to clearly explain the difference between the concepts of cyber threat and cyber risk which are intertwined but many times can be confused. With the latter, we refer to the potential or the probability of loss, damage, impairment, or destruction of an asset within an IT/OT system because of a cyber threat that breaches an identified vulnerability. On the other hand, a cyber threat is anything that can exploit a system’s vulnerability and affect its assets or other parallel dimensions (e.g., reputation, financial gains, etc.). A company should identify all the potential threats in order to assess the cyber risk that its assets are subjected to.

Here is a table that summarizes the most common cyber threats (and the related cyber risk) that should be addressed by the operator of a machine tool.

Vulnerabilities	Cyber Threat	Cyber Risk
Data sharing via USB drives	Malware	Data leakage and system corruption
Insecure office IT environment	Malicious software intrusion	Impairing production machines
Outdated operating systems	Ransomware infestation	System corruption and corrupted storage devices on machine controllers
Incorrect operations due to the lack of basic training	Blackmail trojans or other phishing techniques (e.g., SQL injection)	Data loss, legal implications
Uncontrolled use of cellular devices for installation monitoring	DNS poisoning (or spoofing)	Operations or production impairment

Please note that this table is not exhaustive, it is aimed at highlighting the most common cyber threats and risks.

4. Countermeasures: National actions

Machine tools require precautions specific to their unique networking needs and immediate and long-term data use cases. More connectivity and more data sharing mean more opportunities but also enhanced risks. Considering that by 2025 there will be more than 37 billion Industrial IoT connections, the need to build a cybersafe industrial environment is a key priority.

Implementing a secure process in the machine tool companies is essential to increase the sector's resilience. Measures such as secured development, awareness and training, vulnerability management, application and network security, and incident management, amongst others, are fundamental to mitigate the cybersecurity risks for both manufacturers and products.

Improving cybersecurity awareness in the machine tool sector

Examples of cybersecurity related activities from CECIMO national associations

CECIMO National associations are working on awareness-raising activities on this subject by providing short guidelines and recommendations. Such documents help machine tools companies understand threats and implement organisational and technical measures to improve IT security.

Belgium

AGORIA developed a study (Cybersecurity in de maakindustrie) and a white paper (Recommendations for Better Cybersecurity in the Belgian Manufacturing Industry) which aim to help companies to embrace Industry 4.0 in a cyber-secure way. AGORIA Cyber Business Group (Cyber Made in Belgium) is developing a dedicated focus group named CMIB4ICS/OT in order to cover a strategic and uniform way to increase the cyber resilience of the OT industry.

Germany

VDW developed a paper in 2020 (IT-Security of Machine Tools), which identifies the most critical cybersecurity threats in the machine tool sector and suggests different actions to minimise the risks.

Spain

AFM has an active working group that is conducting research on the topic and is highlighting the importance to have dedicated cybersecurity standards and framework for the Machine Tool sector. The Spanish Association has also supported and implemented several activities and projects aimed at assessing the cybersecurity maturity of their companies and helping them to prepare for future attacks through dedicated simulations.

Italy

UCIMU conducts several awareness-raising activities to inform MT manufacturers of the importance of cybersecurity. Furthermore, the associations provide access to tailor-made services on this topic in cooperation with an external company.

6. CECIMO Recommendations for a more cyber-secure Machine Tool sector

Recommendations for policy makers

Public Investments

Public funding is necessary to make adequate progress in terms of readiness of the industry environment and provide a toolbox of provisions, measures, and instruments to significantly reduce vulnerabilities and the costs of responding and recovering from a cyber-attack.

CECIMO calls on the EU policymakers for dedicated funding to help industries, especially SMEs, upgrade and strengthen their IT protection. In particular, public funding should be used to:

- Provide funding to the R&D of solutions for the cybersecurity of existing machinery
- Foster the development of organizational measures (e.g., incident management)
- Develop specialized courses and training for workers
- Invest in projects that would develop cyber secure "digital retrofitting" of existing machines
- Support businesses in the implementation of the NIS 2 Directive

Importance to allow self-assessment

The Cyber Resilience Act will favour a harmonised regulatory framework, covering all the "connected products" via the internet to fulfil cybersecurity requirements and conformity assessment. The latter should be based on the intended use of the product, the related risk assessment, and the self-assessment of a connected product as it is less burdensome, time-consuming, and more agile than a third-party assessment. In this regard, self-assessment may foster Europe's competitiveness as manufacturers know better their products, how to use a software architecture and how to prevent malicious threats.

Therefore, self-assessment can ensure a satisfactory level of cybersecurity, allow companies to develop a skilled workforce (which will be trained to perform such assessment) and overall pay more attention to the company's cybersecurity.

Recommendations for companies

Focus on the interconnections along the value chain

The complex systems of interconnections and meshed networks that are common for industries in the manufacturing sector pose companies at high risk.

Especially, if we consider SMEs, they often lack economic and human resources to safeguard their online and connected devices, making them accessible targets for cyber-threats.

In complex supply chains the multitude of interconnections increases the number of possible entry points for cybercriminals and compromised IT security of their cyber-physical systems can have severe implications.

CECIMO recommends always verifying the cybersecurity level of all the economic actors involved in data sharing practices and paying attention to the following aspects:

- Conduct an inventory of all the entities that have access to the company's data, networks, or systems.
- Develop a strategy for continuous monitoring of network security and data management, if possible, agreed with business partners.
- Organise periodic training sessions for the workforce, especially focusing on common threats such as password management, phishing scams, and others

Increase the level of awareness and training of workers

Employees should be equally involved in the defence process from cyberattacks. In this regard, everyone within an enterprise should be informed and educated to face the cyber threats.

Therefore, there should be a systematic development of skills to increase the workforce's preparedness for cyber-attacks. This can be complemented through professional training programs and constant stimulation of technology development.

For these reasons, industry should always consider adopting provisions that facilitate workers' understanding of cyber threats in their day-to-day activities.

CECIMO recommends developing cyber hygiene guidelines sector-specific checklists and training material aimed at installing good habits in the workforce and reducing the number of incidents.

References:

- OT-Sicherheit an Werkzeugmaschinen – VDW
- IT Security in Machine Tools – VDW

Glossary

EU = European Union

EC = European Commission

NIS Directive = Directive on Security of Network and Information Systems

OES = Operators of Essential Services

DSP = Digital Service Providers

CSA = Cyber Security Act

ENISA = European Agency for Cybersecurity

NIS2 Directive = Directive on measures for a high common level of cybersecurity

CRA = Cyber Resilience Act

MT = Machine Tools

OT = Operational Technology

HMI = Human-Machine Interaction

IT = Information Technology

SQL = Structured Query Language

R&D = Research & Development

SMEs = Small and Medium Enterprises

For more information please contact:

✉ Vincenzo BELLETTI, Director of EU Public Affairs, vincenzo.belletti@cecimo.eu

✉ Gabriele FAVARO, Policy and Projects Officer, gabriele.favaro@cecimo.eu

CECIMO is the European Association of the Machine Tool Industries and related Manufacturing Technologies. We bring together 15 national associations of machine tool builders, which represent approximately 1500 industrial enterprises in Europe (EU + UK+ EFTA + Turkey), over 80% of which are SMEs. CECIMO covers 98% of the total machine tool production in Europe and about 33% worldwide. It accounts for approximately 150,000 employees and a turnover of around 22.5 billion euros in 2021. More than three quarters of CECIMO production is shipped abroad, whereas half of it is exported outside Europe.